DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE USING BLOCKCHAIN TECHNOLOGY

A Thesis

Submitted in partial fulfillment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

in

Computer Application

By

Prikshat Kumar Angra

41800137

Supervised By

Dr. Pritpal Singh

LOVELY PROFESSIONAL UNIVERSITY
PUNJAB
2022

DECLARATION

I, Prikshat Kumar Angra, hereby declare that the work presented herein is a genuine work done originally carried out by me and has not been published or submitted elsewhere for the requirement of the Degree Program. Any literature, data or work done by others and cited within this thesis has been given due acknowledgement and listed in the reference section.

Prikshat Kumar Angra,
Regd. No. 41800137
Date:

CERTIFICATE

This is certified that the thesis entitled "**DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE USING BLOCKCHAIN TECHNOLOGY**" carried out by Mr. Prikshat Kumar Angra S/O Sh. Kuldeep Kumar Angra has been accomplished under my guidance and supervision as registered PhD student of School of Computer Applications, Lovely Professional University, Phagwara. This report is being submitted by him in the partial fulfillment of the requirement for the award of PhD in Computer Applications from Lovely Professional University. His thesis represents his original work and is worthy of consideration for the award of the Degree of PhD (Computer Applications).

Dr. Pritpal Singh

Title: **DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE USING BLOCKCHAIN TECHNOLOGY**

Date:

Abstract

Blockchain technology is the most rapidly evolving revolutionary technology that is being applied in a variety of fields. It is well-known for its capacity to apply this technology to a variety of domains, assisting in the storage of data in domains connected by peer-to-peer networks [1]. This research aims to investigate the existing system that is used in storing and accessing and securing E-healthcare data of tertiary hospitals of Punjab. After detail assessment it had been observed that most of hospitals are using Client/Server architecture in Punjab for making transactions in EHR. The current processing method of transaction in tertiary hospitals of Punjab are having lots of limitation related to data accessibility and data privacy. After analysis, the research continued to solve the limitations of existing system. To accomplish the same, Hyperledger fabric blockchain framework has been used with pluggable PBFT for providing security to healthcare transactions. This research started exploring successful Blockchain Applications. It focused on already existing blockchain applications as proof of concept in different domains was analyzed and the advantages of the technology in different fields were listed.

In implement phase of our study, we used two consensus mechanisms. POW and plugged PBFT in Hyperledger fabric. In a comparative analysis, it has been observed that POW is good but only suitable for cryptocurrency transactions. Another limitation of using POW is, it consumes high power for executing transactions. PBFT is the best approach that we used for secure E-Healthcare data using Hyperledger fabric.

In this research we utilized the Hyperledger caliper tool to evaluate the performance. The proposed scheme when implemented enhanced the performance of blockchain, and the latency also reduced, according to the results. This demonstrates that, like the steam engine and the Internet, Blockchain has the capacity to bring about profound change for humanity's advancement. For setup and initialization with Hyperledger fabric and composer, “Docker” is used. Docker is an operating system container that a developer and/or system administrator can utilise. In the container, it can be used to create, deploy, and run hyperledger-based applications or business networks [27]. It enables the developer to consolidate all dependencies and functionalities into a single container. The hyperledger fabric and composer network can be operated within a container using docker.

The entire framework is arranged into a network during the measurement phase. It displays the installation of the developed or experimental system with hyperledger dependencies on the primary host. The host's job during preparation is to run the EHR system that is linked to the calliper tool hyperledger environments. The calliper framework is used to set up the experiment's primary host during the second phase. The measurement setting is then left to the calliper and hyperledger hosts [122]. During the measurement, all nodes are observed by installing Wireshark, which collects packets with tcp dump and the docker container's synchronised local loopback server. All packet and network visibility is gained by creating a pcap file. The nodes are finished. The Hyperledger fabric is made up of peers and orders as well as the Certificate Authority (CA). Following the completion of the measurement, an experiment is carried out. Caliper and Hyperledger environments have been used in the virtualization of the node utilising Docker. The numerous trials are carried out in the calliper after configuring the pre-measurement script. The measurement collection, which includes all transaction data, is retrieved from the hyperledger calliper. After all of these stages have been completed, the system is evaluated.

Various experiments are described to demonstrate the functionality of the EHR system and provide insights into the Hyperledger Fabric benchmarks for system evaluation. Multiple use cases, including one organization vs. one peer, two organizations vs. one peer, three organizations vs. one peer, two organizations vs. two peers, and three organizations vs. two peers, are simulated in this study. In the network, each organization has a number of ledger peers that carry a copy of the ledger. The formation of blocks is handled by a single ordered host, whereas the workloads are handled by the Caliper host. The result demonstrates a 1.5x reduction in network latency, which aids in improving the EHR system's performance. For a transaction rate of 50, the minimum latency is around 27 seconds, down from 52 seconds. Having 37s for 250 tps, which is also reduced from the 50s. This is a system performance that can be achieved by altering the hyperledger's default network setup.Five rounds of reading/writing the transaction into the network of the ledger with 1000 transactions in each round at few rates of 100, 150, 200, 250,300 transactions per second.In terms of optimization, the system's latency has been reduced by 40%, which is a good outcome for total network performance. The default 250ms block time has a 9s average latency, whereas changing the policy and block time by 2s only has a 4s latency. The default block time for a max tps of 250 is 13s, but with the altered setup, the read latency drops to 6s.

A healthcare system is one of the largest systems that holds many transactions in every moment. Electronic health care is the patient information that stores the health information in a digital format. The patient-centered records allow accessing the data by any authorized user from anywhere and at any time. The electronic health system saves more than $81billion annually [1]. Electronic health care increases the social, health benefit and reduce medical errors. Electronic health record (EHR) is an electronic version of patient's medical records that are conserve using database technologies. Electronic Health Record is electronic patient's health information which is produced by more Care Delivery Organization. The EHR provides the complete record of the patient, which is supported by the different Care Delivery Organization via the interface. Health information like prescriptions, lab reports, patient's medical history etc. With EHRs, patients' healthcare data is accessible in one spot, when and where it is required. Suppliers approach the data they need; at the time they need it to settle on a choice. Solid admittance to finish persistent healthcare data is fundamental for protected and successful consideration. EHRs place exact and complete data about patients' healthcare and clinical history readily available. With EHRs, providers can give the most ideal consideration, at the purpose of care. This can prompt a superior patient encounter and, above all, better patient results. The Healthcare industry is now moving towards a more patient-centric approach with a major focus on delivering affordable treatment and prompt healthcare facilities at all times. Quality healthcare services backed up with the latest technology is the new demand for today. Despite working with gadgets like mobile phones and computers, it is still not possible to collect, analyze, secure, and exchange data seamlessly. To simplify the healthcare system that is smooth, transparent, economically efficient, and easily operable, blockchain technology was implemented in the healthcare industry.

Framework working is bidirectional with the patient side and doctor side. When patients make registration with online with their personal information, this information has all the user details for their login access. In E-healthcare system, this information system is directly sent to data base with some of the command actions, and when patients registration is approved than patients can proceed further in the framework. Where they as the part of system can access their results. After get approved with the registration process electronic healthcare records (EHR) collect approved records and then doctor's process in e healthcare initiate, on patients record when doctor access record and prescribe any lab test or prescription that also this transaction is recorded. Due to all these transactions most of data travelled over network, there are many security challenges and issues generated in e healthcare for data security. The

infrastructure is peer-to-peer, and it works by having both network users (who take part in transactions) and blockchain miners (that facilitate the transactions in a distributed ledger). The ledger is stored in a decentralized network of nodes that are built by all miners in the network using cryptographic techniques. To provide a secure healthcare solution, a blockchain-based E-healthcare system interoperating with a consensus algorithm will be applied to data collected. Blockchain is the next internet that creates immutable and distributed record of data that can be shared with the blocks connected in a peer-to-peer network.

It has been observed with the results with pluggable PBFT consensus mechanism with Hyperledger fabric more reliable for transfer secure data as comparison of PoW consensus of bitcoin. Blockchain has the potential to alter the way we think about healthcare applications by allowing for automated data collection, the elimination of third parties, a trustless system, and data protection. The suggested network does not have to worry about single-point failure because it is a decentralized network. The system architecture for healthcare applications using blockchain has been implemented in our study, along with algorithms for user access control. This thesis also includes the implementation of a blockchain that employs EHR, for which we employed the Hyperledger Fabric blockchain. By integrating blockchain at healthcare, the challenges in the healthcare system can be mitigated.

ACKNOWLEDGEMENT

It is imperative that research work requires a lot of effort and hard work. It requires high concentration and wholehearted support without which it would not have been possible to accomplish the task. The present work is an effort to throw light on "DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE USING BLOCKCHAIN TECHNOLOGY". The work would not have been possible to come to the present shape without proper guidance, supervision, and help provided to me by a number of people.

With a deep sense of gratitude, I acknowledge the encouragement and guidance received from my guide Dr. Pritpal Singh, Associate Professor, Lovely Professional University, Phagwara. I also express my sincere thanks to Mr. Balraj Kumar, Head of Department, Lovely Professional University, for their ongoing support and valuable advice during the periodic assessment of my work. Sincerely thankful to the respected panel members Dr. Neeraj Kumar (Thapar University, Patiala), Dr. Deepak Prashar, Dr. Ranbir Singh Batth, Dr. Amit Sharma, and Dr. Sophiya Sheikh, Lovely Professional University, Phagwara, for their ongoing support and valuable advice during the periodic assessment of my work.

Special thanks to SMO Hoshiarpur, who helped me with the validity checks of the security framework. I am grateful to Mr. Ashwani Kumar, Assistant Professor, Lovely Professional University, Phagwara, and Mr. Vijay Kumar for continuous support and motivation from time to time, I also appreciate the advice of my mother Smt. Kiran Devi, and my father Sh. Kuldeep Kumar Angra for their critical comments, which enabled me to make necessary improvements.

I am also thankful to all the respondents who helped me in the completion of the survey process by spending their valuable time. Last but not least, I can't forget the moral, & psychological support, and motivation received from my wife Mrs. Tanuja Angra, my daughter Prisha Angra and my son Dhananjay Angra during the research work. Most importantly, I offer my significant thanks to the Almighty for all his grace and light which remain as motivation to me all through this work.

Prikshat Kumar Angra

Date –

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF TABLES

LIST OF FIGURES

CHAPTERIZATION

Chapter 1: Introduction

Chapter 2: Review of literature

Chapter 3: Research Methodology

Chapter 4: Data Analysis and Interpretation

Chapter 5: Findings Conclusion and Recommendations

Chapter 1

INTRODUCTION

This research focuses on designing and implement a security framework for E-healthcare using blockchain technology. A healthcare system is one of the largest systems that holds many transactions in every moment. Electronic health care is the patient information that stores the health information in a digital format. The patient-centered records allow accessing the data by any authorized user from anywhere and at any time. The electronic health system saves $81 billion annually [1]. Electronic health care increases the social, health benefit and reduces medical errors. Electronic health record (EHR) is an electronic version of patient's medical records that are conserve using database technologies. Electronic Health Record is electronic patient's health information which is produced by more Care Delivery Organization. The EHR provides the complete record of the patient, which is supported by the different Care Delivery Organization via the interface. Health information like prescriptions, lab reports, patient's medical history etc., With EHRs, patients' healthcare data is accessible in one spot, when and where it is required. Suppliers approach the data they need; at the time they need it to settle on a choice. Solid admittance to finish persistent healthcare data is fundamental for protected and successful consideration [2]. EHRs place exact and complete data about patients' healthcare and clinical history readily available. With EHRs, providers can give the most ideal consideration, for the purpose of care. This can prompt a superior patient encounter and, above all, better patient results. The Healthcare business is presently moving towards a quieter driven approach with significant spotlight on conveying reasonable treatment and brief medical services offices at every one of the times. Quality medical care administrations upheld with most recent innovation is the new interest for now. Notwithstanding working with contraptions like cell phone and PCs, it is as yet impractical to gather, investigate, secure and trade information flawlessly. To work on a medical services framework that is smooth, straightforward, financially proficient, and effectively operable, blockchain innovation was carried out in medical services industry [3].

1.1 Scenario of health Sector in India

The Indian medical services framework likewise offers sharp differentiations, with select metropolitan emergency clinics offering a-list care as an objective for clinical the travel industry [4], while numerous people have helpless admittance to fitting and moderate

consideration. There is a four-level structure of public medicinal services framework in the states of India. This contains Sub Health Centers (SHCs)/dispensaries at the base giving the fundamental human services administrations to a population of 3000-5000 individuals in Punjab. Above it, there is Primary Health Centers (PHC) serving a population of 20000-30000 individuals [5]. Healthcare infrastructure is an umbrella term covering numerous sectors including social, financial and physical capital, that are required for making favorable condition for various segments of people visiting hospitals [6]. Medical care changes began around 2005 through projects pointed toward reinforcing provincial healthcare administrations and giving fractional monetary assurance to medical services to weak families. In India, both public and private division take part in healthcare structure. With 37 states and union territories. Health sector of India has 25778 hospitals in public sector and 45126 hospitals in private sector [7], [8]. Every day lots of transactions done in hospitals. These transactions are recorded manually and sometimes stored automatically in database using e health system. Using manual record keeping of transaction, all data records cannot be maintained in proper way when size of transaction are too much. So, there are many hospitals using EHR, system that is totally using electronic approach to store all transactions in database on its every dynamic action. Super specialty hospitals, trauma centers, tertiary hospitals use EHR.

1.2 Organizational Structure of health Sector in Punjab

In Punjab, both the public and the private division play a vital job in providing medicinal services. It is the Department of Health and Family Welfare under the Public part which is in charge of giving preventive human services benefits in Punjab. It likewise fills in as a referral unit to six sub centers. Above Primary Health Centers there are Community Health Centers (CHC) which serves a population of 80,000 to 1.20 lac and a referral unit to four PHCs. This entire extent of SHCs, PHCs and CHCs goes under essential level healthcare where administrations are constrained (Punjab health statistics report 2016) [9]. To help primary human services administration there are secondary level medicinal services. Secondary medical hospitals are predominantly spread over the locale through common hospitals, sub-divisional medical hospitals and area hospitals. Moreover, regional hospitals work as an optional level for provincial medicinal services and essential level for the urban population. Other than this, there is likewise an enormous system of private hospital segment in the State. In Punjab, general hospital offices have expanded up to mid-1980s primarily due to expanded

portion of assets to the State's hospital segment. After the post-change period, State hospital administrations declined radically [10].

Table 1.1: Broad wise category Health centers during 2020 in Punjab [10]

	Hospitals		**Primary Health center**		**Subsidiary Health center**		**Community Health center**		**Ayurveda Institutions**	
District	1991	2016	1991	2016	1991	2016	1991	2016	1991	2016
Gurdaspur	16	3	47	40	127	120	6	1515	51	52
Amritsar	33	7	49	36	178	98	6	4	43	22
Tarntaran	.	2	-	19		59	-	9	-	22
Kapurthala	7	3	10	13	60	50	5	4	26	26
Jalandhar	25	3	36	28	161	110	6	11	45	32
S.B.S.Nagar	-	2	.	17	-	49	.	3	-	24
Hoshiarpur	16	4	41	32	1 22	93	6	3	57	44
Rupnagar	8	2	23	I1	78	34	5	3	35	22
S.A.S.Nagar	.	2	-	13	.	51	.	5	.	25
Ludhiana	27	5	35	33	1 56	120	6	2	37	36
Firozpur	17	4	38	34	1 00	85	6	8	39	38
Faridkot	17	3	40	8	1 18	20	6	3	26	9
Muktsar	-	3	-	17	.	45	-	s	.	1 1
Moga		I	-	22	.	53	-	5	-	7
Bathinda	I S	4	38	20	1 16	70	6	9	39	27
Mansa	-	2	.	14	.	38	-	4	-	1 2
Sangrur	18	4	41	32	1 17	73	6	6	43	31
Barnala	.	I	.	1 1	.	36	.	4	.	12
Patiala	19	·6	44	28	132	72	6	10	S I	32
Fatehgarh Sahib	.	2	-	14	-	28	-	4	.	1 0
Punjab	203	62	442	444	1473	1308	70	130	493	495

1.3 Organizational Structure of Hospitals in Punjab

Between the period 1991 and 2016, the complete number of hospitals decreased from 219 to 62, number of PHCs stayed stagnant from 442 to 444 out of 2016, the number of dispensaries diminished from 1473 out of 1991 to1308 in 2016. Although the quantity of CHCs rose from 70 to 130 and a marginal growth is seen in other hospital foundations in the State viz. (Ayurvedic, Unani and Homeopathic) yet in total, the development isn't at all extremely tasteful. Region-Wise provisioning of medicinal organizations in Punjab is additionally introduced in Table 1.1. There is a clear proof of interstate variety. There is no expansion in the number of health establishment especially in the rural territories of the State which comprises over 60 percent of the all-out population. Further, these healthcare foundations possessed by the government compared to continually expanding population of the State (Statistical abstract of Punjab 2016 Director, Health and family welfare, Punjab**)**.In 1980, there was short of one bed for a population of 848 people and that proportion increased to 1281 people for every bed during 2016. This demonstrates the powerlessness of Punjab Government to improve the accessibility of beds for indoor treatment in government possessed medicinal organization in the State. Other than this, hospital specialists (specialists, attendants and maternity specialists) engaged with the hospital administrations and population served by them are additionally given in table as population served per specialist and paramedical staff has accelerated in state of Punjab somewhere in the range of, yet a significant contrast in getting to medical consideration is clear from the information accessible. Fatehgarh Sahib has one specialist serving a population of 7,998 individuals and in Moga and Muktsar locale, one specialist covers over 6,000 individuals though the proportion of specialists to the population is 1:533 in Faridkot and 1:578 in Patiala. There is high increase in population served by non-nursing staff with one gynae assistant for 368 individuals in Faridkot contrasted and one maternity specialist for 5,659 people in Fatehgarh Sahib, recently shaped S.A.S. Nagar has one attendant for every 788 individuals. Correspondingly, there is one medical care taker for 444 individuals in Ludhiana contrasted and one discipline for 1,351 individuals in Bhatinda. In S.B.S. Nagar (cut out of Jalandhar and Hoshiarpur and once in the past known as Nawanshahr) which has the most reduced urbanization rate in the three regions, one specialist serves almost 5,000 individuals. Without going into subtleties of the other recently made areas one finds that the population served per specialist is most astounding in the new areas viz. S.B.S. Nagar and S.A.S. Nagar which have been cut from another gathering of the local. Unmistakably the accessibility of hospital

laborers isn't high as the normal numbers show. Punjab has additionally effectively executed the National Rural Health Mission (NHRM 2005-12) in the State which has a prime spotlight on maternal and child hospital. Since maternal and newborn child mortality proportions are higher than what is normal but still `per capita pay was viewed as reason most appropriate for the State to actualize NHRM. Improving institutional conveyances alongside employing an enormous number of helper staff with some medical preparation, for example, Asha works and ANM are correspondence and guides furthermore; utilizing extra assets for interest in innovation are a portion of the backup goals of NHRM. Another region where the State contrasts in its job when contrasted with different States at the national level is underplaying the job of Non-Government Organizations (NGOs). There must be some regulatory for NGO ‘s also. People are making NGO just to collect funds and there is no accountability. One purpose behind this nearness of NGOs in the State is because of the way that the legislature of Punjab sees dynamic nearness of NGOs as an image of neediness. The second reason would be the solid nearness of Gurudwaras, which are to a great extent contributing to a scope of social administrations at State level. Even though they may be diverse in their methodology and extension and may not be a reasonable substitute for NGOs yet they are good enough. Even though, the approach of privatization in medicinal services in Punjab is anything another wonder yet it picked up force in post monetary refunds. As per the (Punjab Human Development Report, (2016), the private hospital part in Punjab has turned into a boss over public sector hospital. There are steep variations in population serviced by paramedical faculty with one birthing assistant for 368 individuals in Faridkot contrasted and one maternity specialist for 5,659 people in Fatehgarh Sahib, recently shaped S.A.S. Nagar has one medical caretaker for every individual. Essentially, there is one medical caretaker for 444 individuals in Ludhiana contrasted and one nurture for 1,351 individuals in Bhatinda. In S.B.S. Nagar (cut out of Jalandhar and Hoshiarpur and once in the past known as Nawanshahr) which has the most reduced urbanization rate in the three regions, one specialist serves almost 5,000 individuals. Without going into subtleties of the other recently made regions one finds that the population served per specialist is most elevated in the new locale viz. S.B.S.

Nagar and S.A.S. Nagar which have been cut from another gathering of regions. Unmistakably the accessibility of hospital laborers isn't extremely high as the normal numbers demonstrate. Punjab has additionally effectively actualized the National Rural Health Mission (NHRM 2005-12, Report) in the State which has a prime spotlight on maternal and kid hospital. Since maternal and baby mortality proportions are higher than what is normal, given

the normal per capita pay, it was viewed as most reasonable for the State to actualize NRHM. Improving institutional conveyances alongside employing countless helper staff with some medical preparing. Even though, the coming of privatization in human services in Punjab is not another wonder yet it picked up pace 1990. As indicated by the Punjab Human Development Report, the private hospital segment in Punjab has turned into a boss wellspring of healthcare consideration covering 90 per cent instances of non-hospitalized care and over 2/3 of hospitalized care. The organization of the un-sorted out the private segment in Punjab ranges from individual practioners, nursing homes, polyhospitals, pathology labs, drug store shops, corporate hospitals (Escorts, Fortis, Ranbaxy and so forth.). Even though, very less data is accessible on private hospital segment working in Punjab yet a couple of highlights might be featured. For instance, the private hospital division works without adhering to guidelines and is frequently an obstacle to making healthcare open to all. Private specialists don't falter to complete sex determination tests on pregnant moms. These specialists running small nursing homes may regularly be eager to end pregnancies on the off chance that the hatchling is observed to be female. Presumably that, private area medical hospitals are regularly furnished with most recent hardware and innovation. Yet, the majority of the occasions, these hospitals have the untrained paramedical staff to convey healthcare administrations.

Private medical hospitals utilize authorities on contract premise. Patient's rights are frequently not successfully served in the private hospital segment. The larger part of such hospital suppliers gives healthcare consideration to benefit. It is important to note here that private medical services in Punjab are very costly yet even poor people are going to private hospital administration. Not just this, legislature of Punjab decently mentions in its report that "Punjab has a huge private medicinal services establishments and experts, yet regardless of playing such a significant job, no data with regards to the genuine number of private hospital are accessible with the Government of Punjab, as there is no arrangement for it. Enlistment isn't required for beginning a hospital, a nursing home, or private practice. It merits referencing here that a couple of studies, including three national reviews which have been led to inspect the health looking for conduct and usage example of the overall population in Punjab to see how far the private part has won the fight in giving healthcare benefits in the State. These investigations demonstrate that individuals in Punjab are to a great extent for private hospital suppliers in the use of hospital administrations for both in-tolerant just as out-understanding considerations. Punjab have embraced about 76.1 per cent of the all-out human services spending from their

sources, while open spending is just 18 per cent, and every single other source like non-governmental associations, magnanimous trusts, and so forth, contribute just 5.9 per cent of aggregate hospital expenditure [12]. Demonstrates the degree to which family units in Punjab are reliant on Out-of-Pocket use (OOP) because of low government area spending on medicinal services coming about in overdependence on private division for getting healthcare consideration administrations. It is additionally significant here to underline the job of Punjab government in privatizing human services which is obvious from the way that administration gives charge advantages, endowments and concessions to private hospitals and medical experts for setting-up of hospitals and doing private practices. The presentation of client expense for all sort of administrations in hospitals adds up to privatization. Likewise, the administration of Punjab is offering backing to the corporate division by giving them the grounds at a financed rate in the Punjab Urban Development Specialist (PUDA) created states. It demonstrates that the Punjab government someplace down the line is compelling individuals to look forever costly private medicinal care knowing completely well that over the long haul this sort of option won't work given the profoundly unacceptable, exploitative and unregulated medicinal services that the open division gives to by far most of the general population of State. This uncovers a noteworthy breakdown of general hospital administrations in the Punjab State. The private segment isn't the only one to fault as it would be welcome if it develops to oblige all segments that can pay for private consideration.

1.3.1 Electronic Medical Records vs. Electronic Health Records

Dr. Henry Plummer presented the Electronic Medical Record (EMR) in 1880, focusing on patient-specific information. Late 1960's Dr. Larry Weed changed the focus from the patient-oriented record to the patient’s record issue, apparent signs, and side effects diagnostic report and plan. During EMR every information of patients recorded manually than these are published in database. The electronic medical record is a digital replication of paper records. Quickly share the medical information among doctors and other staff of hospital. The main objective is exchanging medical information between different physicians. Various stakeholders like out of patients, medical service suppliers, insurers, including the government.

1.3.2 Electronic Health Records

Electronic Health Record (EHR) is electronic patient's healthcare data which is created by more Care Delivery Organization. The EHR gives the total record of the patient, which is upheld by the distinctive Care Delivery Organization through the interface. This interface having many pathways to get data. Health information like patient registration, approval of their appointments, medical history of patient, doctor's prescription, and progress notes etc. stored directly into data base from different GUI (Graphical User Interfaces). The Electronic Health Record (EHR) with patient's data is viewed as exceptionally delicate in healthcare association. Delicate data to patients in medical services must be overseen with the end goal that it is free from any and all harm from unapproved access [13]. Electronic Health Record is electronic patient prosperity information gives the absolute record of the patient, which is maintained by the unmistakable Care Delivery Organization through the interface. The National Alliance connects the sharing of electronic health records between different providers for health Information Technology discussed the comparison of EMR vs. EHR, as explained in Table 1.2.

Table 1.2 EHR vs. EMR [13]

	Electronic Medical Records	**Electronic Health Records**
Definition	Medical record offering inside the hospitals	The Subset of EMR from 1 or more data gathering constraints where a patient received clinical services
Owner	Owned by organization	Owned by stakeholders
Scope	Companies supply systems installed by hospitals and clinics	Systems run by a community, state or regional emergency or nationwide emergency organizations
Right	The patient has the option to get to the EMR data dependent on the advantage given by the EMR proprietor.	The patient gave is intuitive access just as the capacity to affix data.
Interoperability	Each EMR contains a patient's encounter in a single organization. It	Sharing records amongst a couple of CDOs, related by way of

	does not include other organization data	National Health Information Network (NHIN)

1.4 Common security concern in E healthcare

The trouble in the growing usage of IT foundations in e-medical services is apparently stressed over security when frameworks are trustworthy with medical care data. For the far-reaching reception of e-medical services by clinics, it is fundamental to play out a definite assessment of security issues, to make way for the normalization of different segments for the appropriate execution of e-medical services. A typical e-healthcare framework can comprise of a large number and subsystems, such as appointment and scheduling, prescription records, patient history, routine clinic reports, etc. Each of these subsystems is vulnerable to security threats [14],[15],[16].

1.4.1 Security

It is the property of a framework that is protected to ponder assaults and control from outside of the structure. The framework joins the piece of data security. Mention the common security issues in the health care system, such as confidentiality, authorization, and integrity [17].

1.4.2 Confidentiality

Healthcare information is very sensitive information need to protect from unauthorized users. The electronic health records (EHR) are accessed by many users simultaneously that's why privacy is one of the core responsibilities of e-healthcare. System allows the authorized user to access electronic health records [17].

1.4.3 Authorization

EHR framework concurs with the specialists to get to the record and store, improving the chronicle measure for an approved client. The clinical administrations affiliations endeavor to ease these dangers, and they need to accept accountability for their approval. The approval cycle limited to outer clients, and it is basic to specify the entrance control component to

guarantee the patient's security. It is a cycle; the framework ought to determine the entrance advantages for getting to the e-Health information [18].

1.4.4 Integrity

Keeping up the respectability of the e Healthcare record is fundamental since it is utilized to perceive and follow patients as they move starting with one provider then onto the next provider. The integrity of medical information is necessary to decide on patient care. It maintains the health care which should be accurate and unchanged over entire life cycle. Data is implement independently where it is required in electronic health records (EHR). For any purpose, data accessed and used for any transaction in e-health records, this is sure that we are using true data for the transactions [19].

1.4.5 Privacy

These security rules of the medical services framework ought to indicate who needs to share the information and how to utilize healthcare data. There are many rights in the database according to which we can access the data from the database. The user is responsible for all the activities he/ she performs through transactions. Many times, rights are individually given to the user those are permanently private for all the instances through each and every transaction that happens in the database. These security rules of the clinical administration's structure should demonstrate who needs to share the data and how to use prosperity information.

Table 1.3 Security Requirements in E healthcare

S. No.	Security concept	Requirements
1	Ownership of medical data in E healthcare	As per many transactions done on healthcare data, it is required to characterize the creators, supervisor, and administrator
2	Data Integrity	E-healthcare consists of different types of data, System will protect the precision and consistency of information

3	Updating	In E-healthcare, the system will update and re-establish the information without any loss of data.
4	Data Access	It is also a system requirement to keep user access secure while making transactions with the database over the network
5	Attacks detection	Electronic health records (EHR) are systematized collection of digital records, it is requisite in e healthcare security to work on the attacks detection and trigger all these unspecified actions
6	Patient's access	The framework will empower the patient to give rights over their data to different clients if requires.
7	Confidentially	System guarantees that all the information from data base transactions is available to an authorized user only.
8	Doctors access	Electronic health records (EHR) are a synchronized system with patients records and doctor records, it is vital to act to provide security to the doctor access panel through the transactions.

Privacy is essential for the E-healthcare system. Problems in the system security in electronic health records (EHR) focus on integrity, authorization, confidentiality, availability, access control, detection and prevention of attacks, and so on.

1.5 Security issues related to users in e healthcare

Electronic health records framework facing many users related security issues. Different types of organization and outside people access information in e healthcare. Doctors, patients, insurance companies, medical lab, pharmaceuticals etc. are main users, who are responsible for generate data and making transactions in e healthcare [20]. Throughout the e healthcare

scheme extensive activities done by users of different types. The tasks that can be performed by patients are:

1. Registration.
2. An entrance ticket will be acquired by the patient to keep personality hidden.
3. Begin mysterious utilization of administrations.

Table 1.4 Users Security Requirements in E Healthcare

S. No.	Security concept	Requirements
1	Registration	Verify the authenticity of user
2	Non-repudiation of user action	It is required in e-healthcare that verification one user transaction never deny other user's transaction
3	Non-repudiation of emergency access	E healthcare gives emergency access to users (doctors, patient), due to provide security to one side transaction other transaction not denied
4	Verify user actions	It accesses user's identity and allowed access
5	Access in transactions	To check the privileges only to the authorized users, allow users to make transactions to the system.

1.5.1 Registration

Enlistment is a cycle by which a patient's name and personality are selected into the records of the medical clinic. This is needed to offer types of assistance of the clinic to the patient and to monitor different administrations that are profited by every patient. This is moreover the prime step to enter into the e healthcare system. This process involved following objective: -

1. To gather fundamental subtleties of patients identified with identity, contacts, and demography

2. To make an extraordinary distinguishing proof number for every single patient
3. To enter patient's name in the medical clinic's framework
4. To create a record of the patient for archiving further cycles identified with him/her

Each and every data entered in the registration process, in electronic health record (EHR) verification and authentication is a prime requirement in security.

1.5.2 Non-repudiation of a user action

It is one of the security components; somebody can't prevent the authenticity from guaranteeing something. Non-denial is a legitimate thought that is normally used in data security and alludes to the administrations, which offer affirmation of the starting purpose of data and the dependability of the information, in electronic health record (EHR) every transaction that is performed by user never break access of other transactions required.

1.5.3 Non-repudiation of emergency access

Protection and security one significant test for medical services suppliers to keep up with expanding security penetrates. Client verification is a fundamental factor to actualize in Electronic Health Records (EHRs) to secure patient information and keep noxious clients from accessing the clinical worker [21]. Emergency access is provided to doctors and patients, is required to secure each transaction without any denial in other transactions.

1.5.4 Verify user actions

In Electronic health records (EHR) system many users connect to database. It is required to check user identity and identify the users. Client Identity Verification is a safety effort that checks that all solicitations produced using inside your application or Web Chat gadget are coming from valid end-clients. When User Identity Verification is set, users can only contact the support team once their identity has been validated. When the system recognizes that a valid token was provided in the login request, the user is considered validated. After this process user allow to perform required action in e healthcare system.

1.5.5 Access in transaction

Numerous activities performed in electronic health records (EHR) that affects data. Distinct users access EHR through their own credentials, check the privileges only to the authorized users and allow user to make transactions. This is also a challenge to secure database transactions accessed by multiple users.

1.6 E-Healthcare Security Requirements

The security, privacy, and confidentiality problems posed by E-Healthcare data necessitate a re-examination of traditional information security principles and procedures. Individual permission, confidentiality, and privacy are the major criteria in adopting and successfully using e-Healthcare information because of the importance of security and privacy.

1.6.1 Manage and control the access to EMR data in the EHR

The security, protection, and classification difficulties posed by e-Healthcare data necessitate a rethinking of traditional data security concepts and methods. Individual consent, confidentiality, and privacy, which are the primary factors in accepting and successfully using e-Healthcare information, have been raised as a result of the importance of security and privacy in e-Healthcare information. The current state of E-Healthcare data trends the board emphasizes the need for comprehensive integration of security, protection, and privacy shields inside the executive's structures and approaches to e-Healthcare data. This raises significant difficulties that request all-encompassing methodologies traversing a wide assortment of lawful, moral, mental, data and security designing. The laws were at that point guaranteed to ensure clinical data. EMR contains a few clinical information, which is gotten to by the patient or with the relatives. The patient gets a notice if the clinical information was gotten to by unapproved clients.

EHR innovation is the focal point of progress in medical services advancement. Electronic Healthcare records (EHR) will develop to be a suitable escort for medical clinics. EHR innovation is the focal point of progress in medical services advancement. Electronic healthcare record will develop to be a suitable escort for medical clinics. For execution of electronic

healthcare record brief incitement will help occupy up an adequate fragment of the innovation ventures. Endurance in serious market will be difficult to remain. Electronic health records consist of patients, doctors information that consists of different transactions, in which huge amount of data is generated. Degree and more extensive range of EHR, including the trading of patient data, solidly to improve the quality consideration, proficiency and profitability, and facilitate a superior interoperability of patient data across the hospitals. Brought together completely acknowledged EHRs record having which incorporates the patient's healthcare data: which is outright, defended and exact. It will improve the arrival of venture and thus expanded appropriation pace of EHR. Generally speaking, motivation of EHR is, the capacity to rapidly give care and to use sound judgment. With EHR selection all advantages will achieve all partners in the country, including, doctor, sellers, patients and society all in all. System has sensitive information about doctors, patients and society requisite to secure transactions performed in EHR. Because data travelled in number of nodes, from one block to other block data travelled and security constrains are required to apply, that’s why a secure framework is provide to e healthcare system that secure records of EHR.

1.6.2 Privacy access to EHR

To provide privacy access to e healthcare is an essential part of the system. When multiple user are connected to e healthcare system. Then basic requirement for each and every user is to provide privacy and secure access for their transactions. The security and security of healthcare data have been ensured said the Health Protection Portability and Accountability Act (HIPAA). These protection rules permit family individuals to get to healthcare data. Here and there the patient would not like to uncover touchy healthcare data to relatives or some medical care suppliers. Protection conservation needs to address in the proposed framework. User can access their own information with their access privileges. Only authorized user can access the data and become part of the system. Despite the fact that emergency clinics utilize electronic clinical records framework in their everyday administrations, the experience of the medical care experts makes them not completely trust the framework. Electronic Health Records (EHR) holds multiple user’s data at one time, it is a challenge in EHR if direct access to the record is given, so privacy access required to access EHR [22].

1.6.3 EHR data authentication

There is subsequently an incredible interest in moving from paper-based healthcare records to electronic healthcare records (EHRs). These endeavors are mainly being made by autonomous associations. Notwithstanding, ongoing proposition recommend that coordinated healthcare records give numerous advantages. The respectability of healthcare data should hence be secured to guarantee tolerant security, and one significant part of this insurance is that of guaranteeing that the data's whole life cycle is completely auditable [23]. Accessibility refers to the "property of being open and useable upon request by an approved substance". The accessibility of healthcare data is likewise basic to viable medical services conveyance. Healthcare informatics frameworks should stay operational even with cataclysmic events, framework disappointments, and disavowal of administration assaults. Security additionally includes responsibility, which alludes to individuals' entitlement to censure or inquire why something has happened. Healthcare data is additionally viewed by numerous individuals as being among the most private of a wide range of individual data. Securing this secrecy is along these lines fundamental if the protection of subjects of care is to be kept up.

In any case, this opens new security dangers. There is a genuine worry about both individual's and substances' entrance levels to patients' EHRs. A patient's EHR may be divided and available from a few destinations (by visiting various specialists' workplaces, medical clinics, suppliers, and so forth). Security surrenders in a portion of these frameworks could cause the exposure of data to unapproved people or organizations and healthcare information, in this way, need assurance against controls, unapproved gets to and manhandles, which incorporates considering protection, dependability, confirmation, obligation, and accessibility issues.

Information validation is the way toward affirming the beginning and respectability of information. The term is commonly identified with correspondence, informing, and reconciliation. Authenticate user can access data and perform transactions in e healthcare, with user's own privileges user can access their own existing records, also create new ones.

1.7 Important concerns for E-healthcare services in Punjab

As inspected, there has been no development in the overall medical care organizations particularly during the post-progression time frame in Punjab. Due to lessen government

spending and changing requirements under the helper change program of World Bank, general medical care organizations, particularly ign Punjab, have endured parcel. Punjab government furthermore saw the way that nearly11 % of CHCs, 51 %of PHCs, 74 % of the SHCs, and 50 per cent of sub-focuses in the state was without legitimate structure as per the book of the 12"' multi-year plan (2012-17). Distinctive more limited size level examinations have moreover assumed that there is gigantic issue in designs, device, machines, private settlement and medical services staff, etc., at all levels in the overall medical services foundations in the State. In an audit coordinated by the International Institute for Population Sciences studied the significant offices at the discretionary and tertiary therapeutic administrations level are still less (statistical abstract of Punjab, 2016). On the off chance that there ought to be an event of emergency care, none of the CHCs had Intensive Care Units (ICUs). Despite the fact that ICUs have been available in sub-divisional clinics yet none of them was cooled. Those cooled either don't have a proper back-up office in light of inconsistent force supply or were viewed as, non-useful. To the degree availability of drug was concerned, restorative store the board was not seen as effective. Essential and life-saving drugs were not open in for all intents and purposes all of the medical clinics. Further adding to alert, buying of medicine was for the most part done from customer charges resources in all clinics. All of the emergency clinics has all around described reference systems anyway it isn't continued in real practice. None of the clinical emergency clinics was giving standard eating routine to their patients.

Clinical emergency clinics didn't have authentic spots, latrines, and kitchen workplaces for the relatives of the patients. Maternity and emergency organizations were viewed as most really terrible impacted in CHCs and sub-divisional medical clinics. The basic clarification was the non-openness of experts relentless for maternity and emergency organizations. To the extent sorts of stuff, the audit found that equipment was either out of solicitation or not being utilized. The patients needed to go outside to get the test or X-bar done. The medical services record room was not fittingly organized and figured out. There was a the same unit of specialists as a result of which particularly in the sub-divisional clinic and in CHCs master were doing plan night additionally, emergency commitments and as such were not open for standard OPD. The survey also found that a lot of time was wasted by trained professionals, including specialists to perform various commitments like going to lawful questions, VIP visits, and other principal therapeutic administrations commitments like medical services fairs. Another progressing study drove by the International Institute for Population Sciences (2016) for getting to the medical services office breaking point and preparation in the midst of structure at fundamental

restorative administrations level in all district of Punjab revealed dazzling real factors for utilization of private area in medical care.

As demonstrated by the outline, Punjab is perhaps the most incredibly horrible performing states similar to availability of fundamental meds. In Punjab, only 26 percent of PHCs had private quarters for clinical authorities however 55 percent of PHCs at a public level have private quarters. West Bengal, Maharashtra, and Assam are far in front of the public typical. To the degree, 24 hours working of PHCs is concerned only 17 percent of PHCs are laboring for 24 hours through the public ordinary is 53 percent. West Bengal, Maharashtra, and Assam are far in front of the public typical. To the degree, 24 hours working of PHCs is concerned only 17 percent of PHCs are laboring for 24 hours through the public ordinary is 53 percent. CHCs are irrelevantly over the public ordinary to the extent openness of master, aside from anesthetists and medical care administrators. This shows fundamentally after use of NHRM (2005-12) in Punjab State, the fundamental medical services workplaces and establishment for country people is really inadequate.

E healthcare services play an important role in tertiary hospitals of Punjab, reason behind this statement is that these hospitals come under category of super specialty hospitals or trauma care centers, these all centers receive 80% information using online platforms, maximum data base transactions done in online manner. Current scenario of Punjab in healthcare as a service access database online, multiple users are part of the system whether they are patients, doctors, lab in charge, insurance persons etc. E healthcare provided a platform that is used to make transactions and store each and every activity in data base, tertiary hospitals of Punjab differentiate transactions in different levels, one of them are on the patient’s side and other is on the doctor side. This is an important concern in e healthcare service to secure transaction that are occurred in each second and generate thousands of results.

1.8 Number of Doctors registered in State Healthcare alliances In India

Through a composed answer to address in Rajya sabha, Minister of state Smt Anupriya Patel educated in 2018 that there are 1041395 specialists enlisted in state clinical council.as on 30th September 2017,details of specialists enrolled with each state clinical board is referenced in beneath table. Top five states out and out adds to 52.07 percent strength of specialists in India

for example Maharashtra, Tamil Nadu,Karnatka,Andhra Pradesh and Uttar Pradesh with 542315 specialists .Assuming accessibility up to 80 percent 8.33 lakh specialists are really accessible for effectively offering support to individuals It gives a specialist to populace proportion at 1:1596 against WHO suggested 1:1000. A greatest number of enrolled specialists is with Maharashtra for example 153513 followed by Tamil Nadu and Karnataka with specialists enlisted around 1 lakh. Punjab is having 44682 specialists' registers in Punjab clinical board and around 10000 specialists running their own in excess of 50 bed super claim to fame clinics. As indicated by news distributed in the tribune day by day for April 18, 2019, just Jalandhar locale in Punjab is having around 800 superspeciality and multi-strength clinics and arising as one of the greatest government health care center point in Asia. When contrasted with private medical care area number of public area clinics are not many in number in Jalandhar with just 3 clinics as locale common clinics and just 11 local area healthcare focuses .So government should outline some approach to regularize extension of private medical services area and administrations given by them a talked about in this part prior there is less expansion in number of public area medical clinics of Punjab because of less Government spending and changing needs of strategy producers after 1991. Practically all private portion clinical emergency clinics are routinely outfitted with latest contraption and innovation. However, these facilities have the undeveloped clinical and paramedical staff to offer therapeutic types of assistance. Private facilities use additionally specialists on an agreement premise. It is intriguing to note here that private clinical emergency clinics in Punjab are particularly expensive yet even destitute individuals are going to private prosperity organization. Nonappearance of care among poor, choice heading and deficient directing framework in the state are the huge detours for the poor in getting free treatment from private clinics. Moreover, there is essentially no provisioning of health care coverage for the poor in the State. A few NGOs in the State and Punjab government have started diverse clinical inclusion plans for destitute individuals yet the results are far from being seen.

Table 1.5: Number of doctors registered in state Healthcare alliances (Councils) [24]

Maharashtra Healthcare alliances	153513
Tamil Nadu Healthcare alliances	126399
Karnataka Healthcare alliances	104794
Andhra Pradesh Healthcare alliances	86129

Uttar Pradesh Healthcare alliances	71480
West Bengal Healthcare alliances	66974
Travancore Healthcare alliances	55251
Gujarat Healthcare alliances	53954
Healthcare alliances of India	52666
Punjab Healthcare alliances	44682
Rajasthan Healthcare alliances	40559
Bihar Healthcare alliances	40043
Madhya Pradesh Healthcare alliances	34347
Assam Healthcare alliances	22532
Orissa Healthcare alliances	21681
Delhi Healthcare alliances	16176
Jammu and Kashmir Healthcare alliances	14326
Uttarakhand Healthcare alliances	7060
Chhattisgarh Healthcare alliances	6915
Haryana Healthcare alliances	5717
Jharkhand Healthcare alliances	5093
Goa Healthcare alliances	3367
Himachal Pradesh Healthcare alliances	2849
Telangana Healthcare alliances	2354
Sikkim Healthcare alliances	893
Arunachal Pradesh Healthcare alliances	840
Nagaland Healthcare alliances	801
Tripura Healthcare alliances	0
Total	1041395

Table 1.6: Top 5 States with share of registered doctors

Maharashtra Healthcare alliances	153513
Tamil Nadu Healthcare alliances	126399
Karnataka Healthcare alliances	104794

Andhra Pradesh Healthcare alliances	86129
Uttar Pradesh Healthcare alliances	71480
Total	542315

1.9 Need for study

Medical services as an industry has novel prerequisites related with security and protection because of extra legitimate necessities to ensure patients' clinical data. The point of this examination is to distinguish and dissect the security dangers that exist for the Electronic Health Records medical care framework.

The principal objective of Information innovation has been utilized in medical services to improve and upgrade clinical administrations and to diminish costs. The worldwide admittance to clinical information is permitted in the e Healthcare framework, yet security and protection is a difficult issue.

The latest advancement underpins the nature of medical care administrations to the advantage of the two patients and emergency clinics. The clinical information dispersed across different systems; the basic data isn't open as expected, and furthermore suppliers are most certainly not permitted to get to the healthcare information.

The latest advancement underpins the nature of medical care administrations to the advantage of the two patients and emergency clinics. The clinical information dispersed across different Systems; the basic data isn't open as expected, and furthermore suppliers are most certainly not Permitted to get to the healthcare information.

There are various sorts of individuals who access healthcare data in a solitary association like the specialist, nurture, insurance agencies, and so on electronic healthcare records (EHR) contain a gigantic measure of information inclusion and updating in everyday practice. So it is vital to make sure about EHR. Trillions of transactions processed in e healthcare system every hour. Only authenticate persons responsible for every transaction, data generated in every transaction stored in database, patient’s data accessed by doctors and doctors’ data is only visible to the patients same way when other become part of the system they as the part of system

can make transactions. Hospitals store batch of transactions and challenge is to secure data that is part of each transaction whether it occurs on patient's side, doctor side.

The motivation of the research is to investigate the existing techniques for securing the e Healthcare record in which most of hospitals in Punjab using client server security architecture. In which we are data is stored on server and data first generated in e healthcare, there are many pathways through which data is passed and generated.

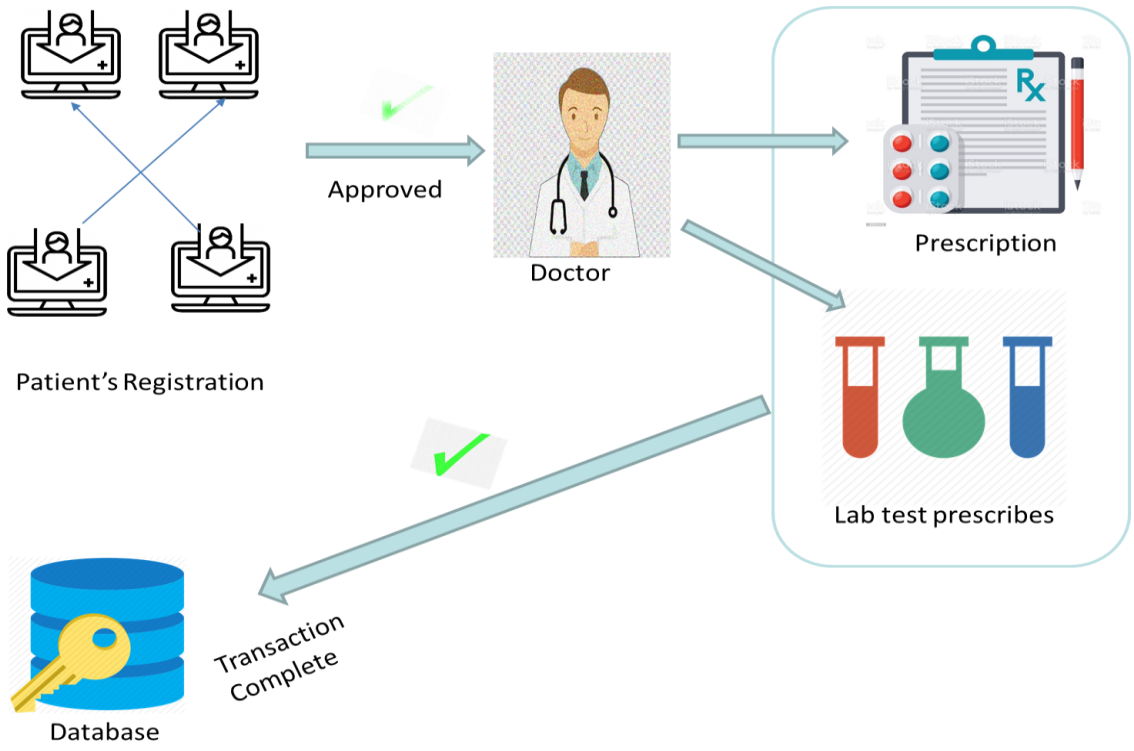


Fig 1.1: Existing E-healthcare Model

Framework working is bidirectional with the patient side and doctor side. When patients make registration with online with their personal information, this information has all the user details for their login access. In e healthcare system, this information system is directly send to data base with some of the command actions, and when patients registration is approved than patients can proceed further in the framework. Where they as the part of system can access their results. After get approved with the registration process electronic healthcare records (EHR) collect approved records and then doctor's process in e healthcare initiate, on patients

record when doctor access record and prescribe any lab test or prescription that also this transaction is recorded. Due to all these transactions most of data travelled over network, there are many security challenges and issues generated in e healthcare for data security. The infrastructure is peer-to-peer, and it works by having both network users (who take part in transactions) and blockchain miners (that facilitate the transactions in a distributed ledger). The ledger is stored in a decentralised network of nodes that are built by all miners in the network using cryptographic techniques [25]. To provide a secure healthcare solution, a block chain-based E-healthcare system interoperating with consensus algorithm will be applied on data collected. Blockchain is a powerful innovation that makes permanent and conveyed record of information that can be imparted to the squares associated in shared network. By incorporating blockchain at medical care, the difficulties in the medical care framework can be relieved and it fills in as a shelter to the patients, specialists, clinical workers and the backup plan. Osiz advances is a prevalent blockchain improvement organization, who foster custom blockchain applications for medical care area to do the operations from keeping up with patient's very own record to symptomatic reports and specialist's solution.

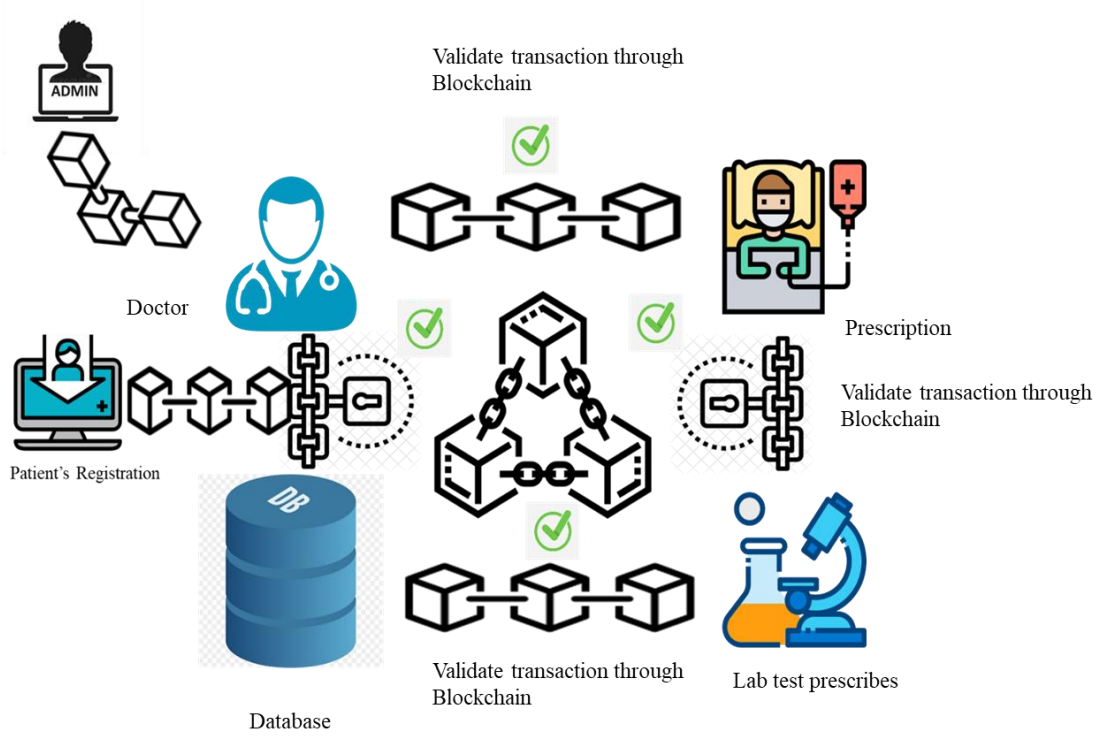


Fig 1.2: Proposed E-healthcare Model

In the proposed model, healthcare transactions are done through distributed ledger using blockchain technology. Numerous transactions execute on different nodes demonstrate in fig 1.2, Admin generate a transaction over the network and directly connected to the doctor through a proper validation process, using blockchain network doctor linked with patient registration and prescription. Lab prescription detail of patient connected to patient prescription. All the transactions validated through blockchain in the proposed model. The flow of transactions from one peer to another peer is secured using blockchain, data from admin, doctor, and patient used a secured blockchain security for e healthcare. The proposed model also secure transactions from prescription and lab test prescription data that travel from doctor and patient's registration model.

In implement phase of our study, we used two consensus mechanisms. POW and plugged PBFT in Hyperledger fabric. In a comparative analysis, it has been observed that POW is good but only suitable for cryptocurrency transactions. Another limitation of using POW is, it consumes high power for executing transactions. PBFT is the best approach that we used for secure E-Healthcare data using Hyperledger fabric. Hyperledger calliper tool used to evaluate the performance. The proposed scheme enhances the performance of blockchain with the proposed algorithm , and the latency may also be reduced using the proposed technique, according to the results. This demonstrates that, like the steam engine and the Internet, Blockchain has the capacity to bring about profound change for humanity's advancement.

Proposed mode designed and implement using blockchain technology because it is transparent, a blockchain is a mechanism for storing and exchanging information that is secure. Due to the dual nature of each block in the chain—as both an autonomous unit with its own information and a dependent link in the overall chain—a network controlled by members who store and share the information, as opposed to a third party, is created.

1.10 Blockchain in healthcare

The development of smart contract innovation has over forty years of history. It is re-birth with the advancement of block chain innovation. It is the fundamental innovation of the most mainstream digital money of the world "Bitcoin" proposed in the white paper of an obscure individual called "Satoshi Nakamoto". Blockchain is the most addressable innovation, which grabbed the eye of various social orders like organizations, instruction enterprises and

scientists, and so on. Blockchain innovation is most basically characterized as a decentralized, conveyed record that records the provenance of a computerized resource. Using decentralization and cryptographic hashing, Blockchain, also known as Distributed Ledger Technology (DLT) [26], renders the historical background of any computerized resource unalterable and easy.

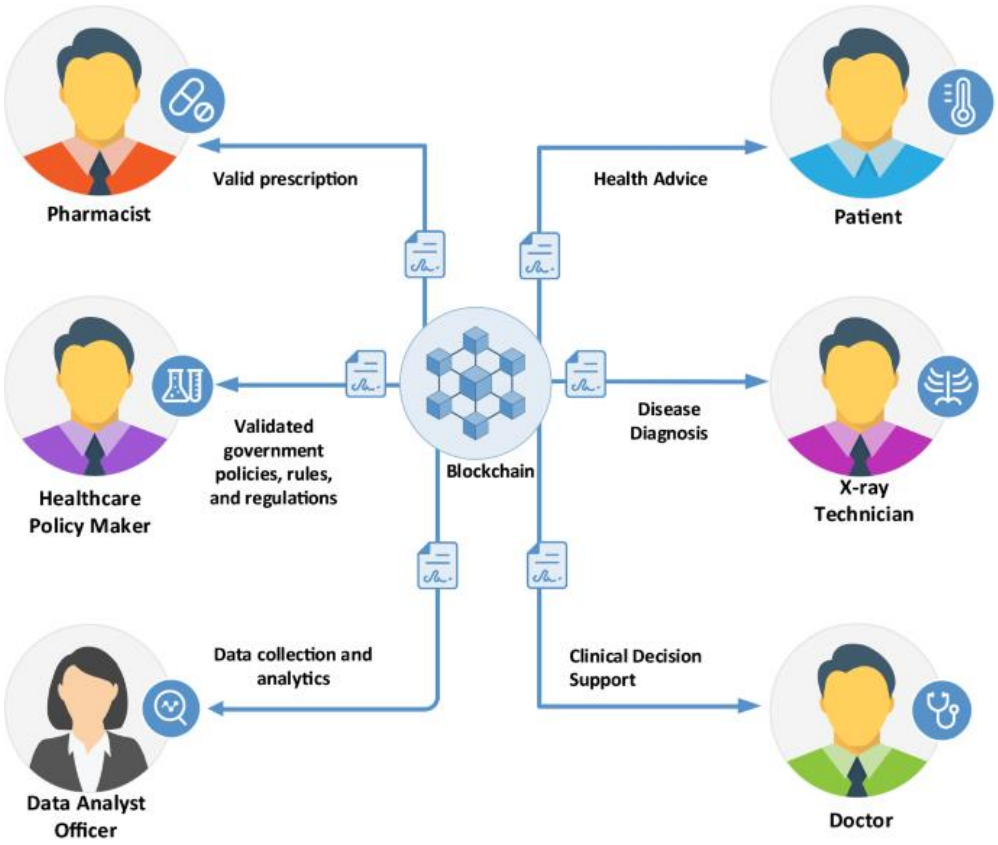


Fig 1.3: Blockchain Structure

1.10.1 Public vs. Private Blockchain

As a shared organization, joined with a conveyed time-stepping worker, public blockchain records can be overseen self-governing to trade data between parties. There's no requirement for a manager. In actuality, the blockchain clients are the manager. All the request nodes for the most part connected to public blockchain.

A second type of blockchain, known as private or permissioned blockchain, permits organizations to make and halfway control their own conditional organizations that can be utilized between or intra-organization with accomplices.

1.11 Advantages of Blockchain

1.11.1 Precision of the Chain

Trades on the blockchain network are supported by an association of thousands of PCs. This wipes out basically all human consideration in the really look at communication, achieving less human screw up and a precise record of information. Whether or not a PC on the association were to submit a computational blunder, the misstep would simply be made to one copy of the blockchain. All together for that slip-up to spread to the rest of the blockchain, it would ought to be made by in any occasion 51% of the association's PCs-a near incomprehensibility for a gigantic and creating association the size of Bitcoin's [27],[28].

1.11.2 Cost Reductions

Ordinarily, purchasers pay a bank to really look at a trade, a legitimate authority to sign a document, or a minister to play out a marriage. Blockchain kills the prerequisite for untouchable check and, with it, their connected costs. Business visionaries causes a little cost whenever they recognize portions using charge cards, for example, since banks and portion getting ready associations need to deal with those trades. Bitcoin, of course, doesn't have a central position and has limited trade costs.

1.11.3Decentralization

Blockchain doesn't store any of its information in a central region. In light of everything, the blockchain is reproduced and spread across an association of PCs. Whenever one more square is added to the blockchain, every PC on the association revives its blockchain to reflect the change. By spreading that information across an association, rather than taking care of it in one central informational collection, blockchain ends up being more enthusiastically to screw with. If a copy of the blockchain fell heavily influenced by a developer, simply a singular copy of the information, instead of the entire association, would be subverted.

1.12 Blockchain Consensus algorithm

The blockchain agreement calculation is that it is a methodology by means of which all the companions of a Blockchain network arrives at a typical acknowledgment or agreement about the ongoing condition of the dispersed record.
An agreement system empowers the blockchain organization to accomplish dependability and fabricate a degree of trust between various hubs while guaranteeing security in the climate. This is the motivation behind why it is one of the crucial pieces of each Blockchain application advancement in the appropriated record climate.

1.13 Objectives of Blockchain Consensus Technique

1.13.1 Bind Agreement

One of the superb goals of agreement instruments is achieving bind agreement. Dissimilar to concentrated frameworks where having trust in the authority is essential, clients can work even without building trust in one another in a decentralized way. The conventions inserted in the Distributed blockchain network guarantees that the information associated with the cycle is valid and precise, and the status of the the public record is forward-thinking.

1.13.2 Forestall Paired Spending

Agreement measures work dependent on specific calculations to guarantee that the public record just contains certain exchanges that are checked and genuine. This tackles the conventional twofold spending issue, for example the issue of twice spending advanced money.

1.13.3Safety

All hubs are fit for producing results that are valid as per convention rules in a decent agreement framework.

1.13.4 Comprehensive

An effective agreement component guarantees that each organization hub is dynamic in the democratic cycle.

1.14 Research Contribution

Developing interest for medical care benefits and coordinated consideration conveyance, combined with an expanded spotlight on part healthcare executives, emphasizes the requirement for a data innovation framework that can eliminate reliance on agents. Blockchain can help beat most, if not all, of these difficulties. A framework based on circulated engineering, blockchain doesn't need different degrees of verification and simultaneously gives total, on-request admittance to sequentially organized information. It is a hearty innovation that can drive medical care industry execution, improve the nature of care and lower the expense of conveyance.

Quite possibly the main part of a medical services framework is the manner in which its information is shared across substances in the worth chain. Blockchain upholds consistent data sharing that can take out the duplication, blunders, and irregularities that can emerge with customary, brought-together information stockpiling. The savvy contracts application takes out the requirement for delegates to oversee and execute the part/tolerant agreements.

Blockchain innovation has expected applications to a portion of the difficulties looked at by the medical services industry. The most grounded capability of blockchain innovation in the medical services field is its vigorously explored applications, specifically: security, trustworthiness, decentralized nature, accessibility, and validation standards because of the overall record and square related framework. The medical services industry is confronting issues adjusting to a developing mechanical foundation zeroed in on Internet-empowered gadgets, IoT, keen gadgets, and detecting gadgets. As such advancements empower the medical care industry to all the more likely serve its patients in an always developing interconnected world, malignant entertainers can likewise misuse weaknesses in these innovations (just as cycles and clients) to access and copy the information, making it harder to divide records

among clinics. This can bring about obsolete information, and thus medical issues or misdiagnosis, and an issue checking a patient's identity.

Plainly blockchain has numerous advantages, which can be applied to the medical care industry To tackle various issues in record sharing and security. Notwithstanding, blockchain isn't an answer that can be constrained into any circumstance. All things considered, cautious assessment of explicit blockchain issues and how they impact the medical services industry should be assessed. Issues, for example, mining motivating forces, which are a center instrument of blockchain have not been completely viewed as in the medical care industry, just as explicit blockchain assaults that can end the whole framework [29].

While numerous scientists researched the utilization of blockchain for medical services information the executives, anyway as far as anyone is concerned there is no assessment of this new worldview with the customary customer/worker model. The customer/worker model experiences the issue of information stewardship, information fracture, weakness, security and protection.

The final involvements of this thesis work illustrated as given below.

1. To study and analyze security issues in electronic healthcare system.
2. To propose a new security framework, to secure e healthcare system through block chain consensus mechanism.
3. To ensure the integrity of e healthcare record
4. To compare proposed security framework with existing system.

1.15 Structure of the Thesis

The thesis is organized into five sections and the workflow of the thesis is shown in Fig. 1.4. The research work nucleus on securing E-healthcare using blockchain technology through a consensus mechanism.

Chapter 1 start with an introduction to Blockchain, then Types of blockchain, Structure of blockchain, Security issues in the healthcare system, research motivation, objectives, the contribution involved, and a detailed outline of the research work.

Chapter 2 identified the research gaps based on the review of the literature. The detailed review of literature based on the electronic health records (EHR), blockchain security and various consensus algorithm that are used to provide security using blockchain domain of authentication, data integrity, and confidentiality in the healthcare blockchain system.

Chapter 3 elaborates on the proposed framework to secure the eHealth system through blockchain consensus algorithm. The primary goal of the proposed system is to provide a secure platform to the eHealth record between providers with the help of consensus mechanism of blockchain.

Chapter 4 explore results from data analysis and interpretation results according to the proposed and existing system. Comparing all activities including the framework for providing security in e healthcare. Finally, **Chapter 5** concludes the thesis with finding conclusion and recommendations of the research contribution and future extension of the work.

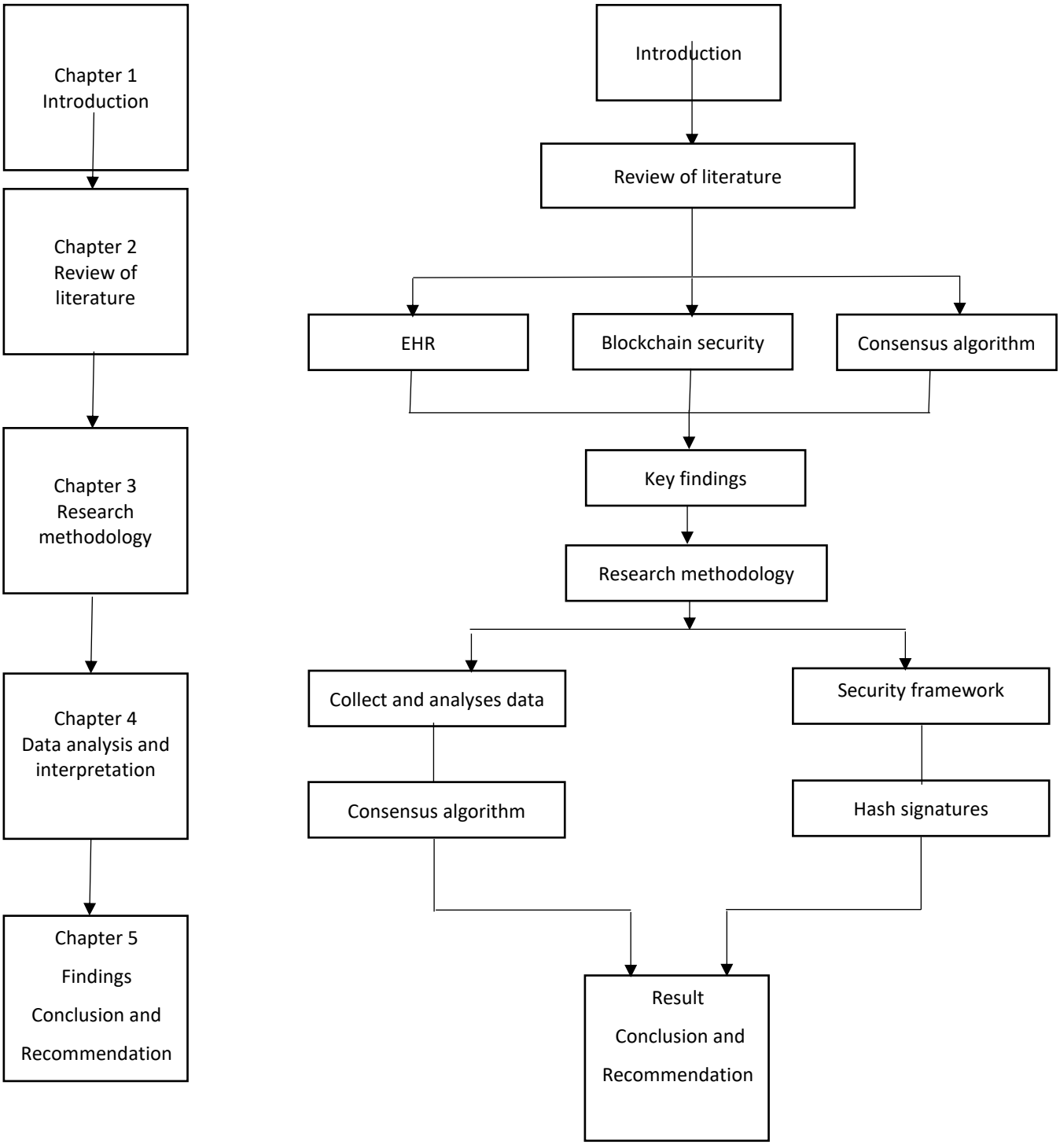


Fig. 1.4: Structure of the thesis

1.16 Phases in Research

Research work is divided into three different phases that shown in Fig. 1.4. Include each organized way to solve problems that identified.

Phase 1 contains literature survey in blockchain security, electronic health records (EHR) and consensus algorithms used to promise security using blockchain.

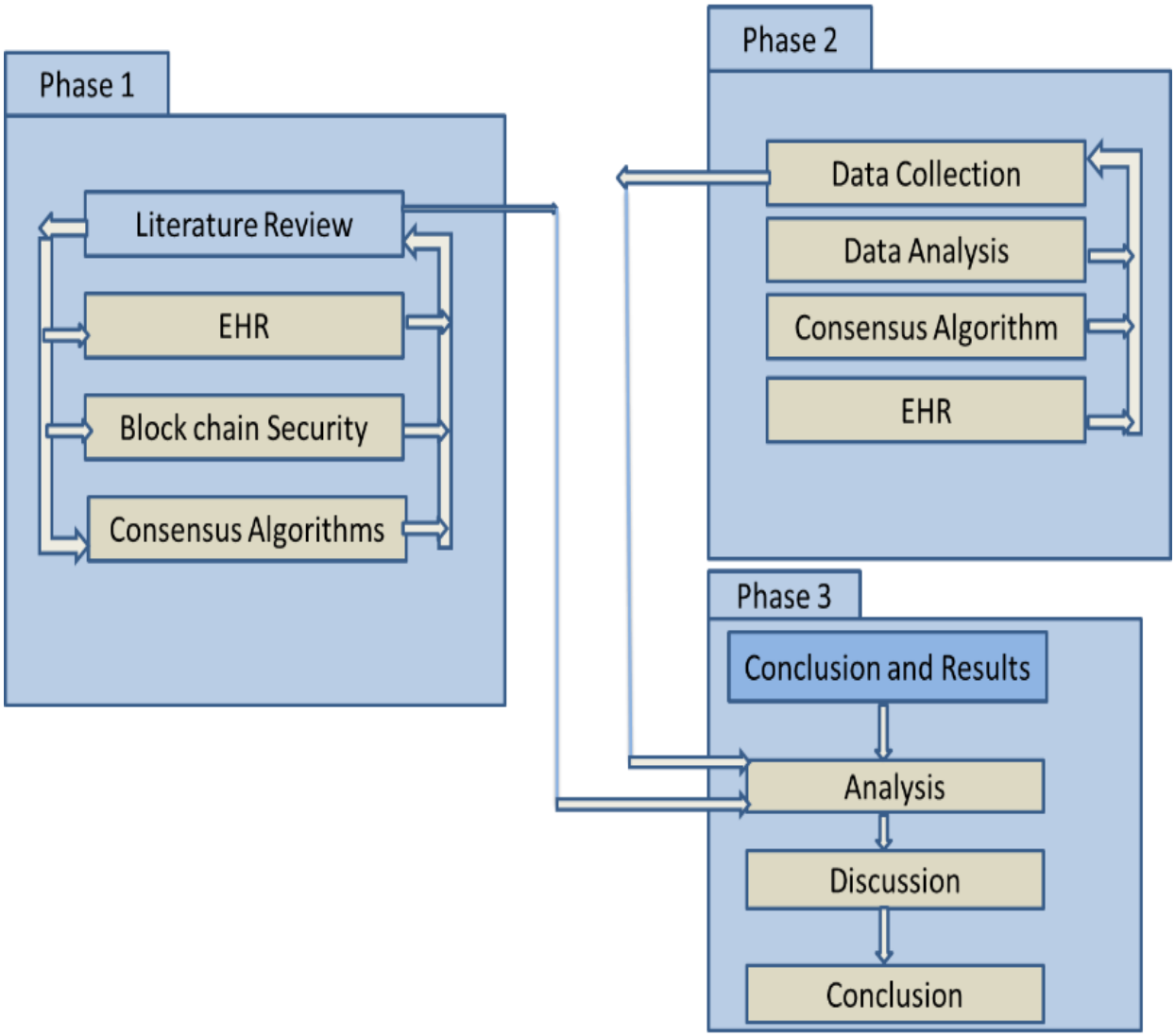


Fig. 1.5: Study Phases

Phase 2 coordinates control data collection from healthcare systems, analyses data. Design and implementation of security framework in e healthcare system using blockchain. Electronic health records (EHR) provide information after implementing security framework.

Phase 3 exhibit results from research for analysis and discussion on major aspects. This phase set forth conclusion on the proposed mode and comparing with the existing model.

CHAPTER 2

REVIEW OF LITERATURE

Electronic healthcare record was scatted across the various clinics and never intended to deal with that information by a solitary supplier. One supplier keeps up every medical clinic patient's information, and it is hard to see the past healthcare information by different suppliers [29]. Every association keeps an alternate access control framework, which chooses to permit or deny. The single substance deals with the entrance control list and organization. Two fundamental downsides in the concentrated methodology are a solitary purpose of disappointment and focal position. A solitary purpose of disappointment implies the concentrated admittance control falls flat; by then, it's not possible for anyone to get to the whole framework. All the exchanges are affirmed by the focal power, which prompts security and execution issues. As per the HIPAA protection rule, for the patient solicitation, the supplier can take 60 days to react to refreshing the record [30].

2.1 Studies on Indian Health Scenario

In this we analyzed the healthcare changes in India with time arrangement study. The investigation set out that the advancement in the Indian clinic zone was the delayed consequence of the asset given by the International Monetary Fund and World Bank on India to accept Structural Adjustment Policies. It was found that the medical clinic changes brought two sorts of changes (1) Decline in the organization assignments to the medical clinic portion and (2) Increased improvement of the private medical clinic part. The administrations' structure and the investigation which was being done by Indian Council of Medical Research suffered seriously on account of the lessened general emergency clinic spending. It was prescribed that to beat this issue decentralization should be done in the medical clinic section wherein the powers should be moved to the local governments or Panchayati Raj Institutions. The development in the organization's medical clinic use was recommended up to 2-3 percent of GDP. The level of government emergency clinic utilization made by the states and its association with the installment of each state. The data was removed for 14 states from various reports dispersed by the assembly. The time course of action investigation of data was made and the results revealed that the rate increase in the Gross State Domestic Product was exceptionally high when stood out from the development in state medical clinic utilization. On a typical, each state was seen to spend simply 0.43 percent of GSDP on broad medical clinic

[31]. Without palatable budgetary resources in the organization medical clinic zone, everybody has started inclining toward the private human administration's organizations. It was exhibited that the public goal of extending general clinic utilization to 2-3 percent of GDP was difficult to achieve without the rising in medical clinic appropriations by states. The requirement for growing the emergency clinic utilization and utilizing it successfully was highlighted. Beside this, the genuinely essential clinic changes creators moreover suggested both in everybody and private medical clinic zone.

It was prescribed that to beat this issue decentralization should be done in the clinic section wherein the powers should be moved to the local governments or Panchayati Raj Institutions. The extension in the organization medical clinic use was recommended up to 2-3 percent of GDP. The level of government emergency clinic utilization made by the states and its association with the installment of each state. The data was removed for 14 states from various reports circulated by the governing body. The time plan investigation of data was made and the results revealed that the rate increase in the Gross State Domestic Product was extremely high when stood out from the extension in state medical clinic utilization. On an ordinary, each state was seen to spend simply 0.43 percent of GSDP on broad emergency clinic. Without agreeable budgetary resources in the organization emergency clinic territory, everyone has started inclining toward the private human administration's organizations. It was shown that the public target of extending general medical clinic utilization to 2-3 percent of GDP was difficult to achieve without the climb in clinic dispersions by states. The requirement for extending the medical clinic utilization and utilizing it successfully was included. Beside this, the genuinely fundamental medical clinic changes creators also suggested both in everybody and private medical clinic zone [33].

The clinic markers exhibited an alarming picture of the Indian emergency clinic part with the infant kid demise rate and maternal passing rate significantly higher than foreseen. It was seen that without authentic government emergency clinic workplaces, the average compressed the organization to empower the private players to enter the emergency clinic division. The investigation found that the emergency clinic changes brought subsequent to accepting Structural Adjustment Policies (SAP) moreover fail to improve the medical clinic organizations. People saw to be progressively arranged towards the private clinic organizations as they believed them to be progressively productive. It was seen that the creator of the non-treatment case extending among the down and out people on account of their powerlessness to

pay the over-the-top expense charged by the private fragment. The maker suggested that the overall emergency clinic hypothesis should be extended and the rule segment should be delivered for the private emergency clinic region. The specialist register of the American Medical Association was in like manner used to get the quantity of experts who emigrated from India. The idea of clinical getting ready given by different schools was assessed dependent on pointers like the accreditation assessments given by the Healthcare alliances of India, examination by understudies. The results showed that the resettlement rate to the US was high if there ought to emerge an event of the highest medical care colleges of India and it was a creator in case of low situated schools. Comparable results creators represented concerning movement of Indian experts to the UK. The low idea of medical services planning in India, when stood out from made countries like the USA and UK, has been appeared as one explanation behind the high removal rate. The researcher further focused that the deficiency of clinic work can't be met just by extending the amount of private clinical schools on the grounds that not a lot of colleges have adequate workplaces to get ready and develop best emergency clinic pioneers in the country [34].

Author investigated the major issues looked at by broad medical services providers in India and prescribed clinical measures to beat them. On the reason various reports and existing composing, the going with five essential issues creators highlighted by the author. (1) Shortage of medical clinic system (2) Shortage of medical clinic work, (3) High family use on the clinic, (4) forbidden nature of medical clinic organizations (5) Low thickness of subject matter experts. The examination suggested that the inadequacy of the medical clinic laborers could be overpowered by improving day to day environments around the open emergency clinics in rustic areas. In this manner, the inadequacy of establishment could be overpowered by making effective usage of the current outpatient workplaces by starting night moves notwithstanding the morning timings [35].

Author broke down the condition of government and private medical clinic part in India. The clarifications behind the mistake of government clinic organizations' creators were revealed in the examination. The emergency clinic part gives creators inspected by segregating the medical clinic organizations into two classes, to be explicit, (1) Preventive and promotive and (2) Curative medical care. It was found that the adaptable diseases for the most part regular in the destitute people coauthored the activities impelled to control these ailments creator focusing on both poor and rich correspondingly. On the off chance that there ought to emerge an event

of healing organizations the difficult issues which creator found in the Primary emergency clinic centers approve the lack of medical clinic staff, the nonattendance of emergency clinic workers from emergency clinic office, unseemly and undeveloped staff and nonappearance of cheerfulness towards the patients. The shortfall of obligation was seen to be the principle thought for the failure of the organization emergency clinic organizations. It was prescribed that the methodology makers should unravel the necessities of the patients into plans and the medical services providers should be offered persuading powers to give better emergency clinic organizations.

Researcher assessed the availability and transport of the clinic staff transversely over various states in India and the impact of awkward nature in medical clinic workers scattering on the clinic results. The data concerning the openness of three kinds of healthcare labor force, specifically, trained professionals, dental subject matter experts and clinical chaperons' creator obtained from the Report healthcare and Family Author toll circulated by the Ministry of Statistics and Program Implementation [36]. Direct backslide was associated with assess the association be authored the thickness of clinic workers and the key emergency clinic results like infant mortality and maternal mortality. The results uncovered that their creators' monstrous intrastate abnormalities in the openness of clinic workers. The availability of experts per 1000 populace was seen to agree to less and there was an extraordinary lack of experts in specific states like Uttarakhand, Uttar Pradesh, Bihar, etc. It was sawed that the higher thickness of experts in a state prompts creator infant youngster mortality and maternal mortality thusly setting up an association be composed the amount of emergency clinic labor force and emergency clinic result.

In examination zeroed in on the situation with general clinic utilization in a bit of the Indian states with low Gross State Domestic Product (GSDP). The data was taken from various state government and central government appropriated reports. The investigation revealed that the states with a low compensation like Bihar, Orissa, Assam and Rajasthan had creator status and as a result of their low compensation they are not capable of growing the financial tasks to the emergency clinic fragment. These states going up against the most outrageous absence of medical clinic resources [37]. It was seen that as a result of the immense size of these states, they gigantically influenced the overall emergency clinic circumstance of India. The maker suggested that the central government while making clinic utilization should zero in on the

destitute states with the objective that the highway distortions in the medical clinics can be endure.

Author investigated the association between high cash-based utilization on clinic and extending dejection. The data was taken for 16 states from the 50th cycle (1993-94) and 61st cycle (2004-05) reports of the National Sample Survey and connection was put aside a couple of moment's ranges to measure the change in the components more than 10 years.

The results showed that there was a sharp addition in the cash-based utilization be writing two data centers. Due to the absence of government emergency clinic structure, there has been a development in the use of private emergency clinic organizations which has also come to fruition into more vital Out of pocket (OOP) utilization. In any case, unmistakable assortments creators watched concerning the change in OOP use be wrote the states. The examination exhibited that the new methodologies which exceptional the private parts in the medical clinic region provoked an important augmentation in the desperation levels of the country. A more noticeable level of person's creator pushed underneath the destitution line due to extended OOP portions in 2004-05 in by far most of the states.

Author investigated the issues in the Indian clinic territory unequivocally the receptiveness and the idea of emergency clinic organizations in India. The data creator took from various reports conveyed by the Indian Ministry of Health and Family. Despite the discretionary data, fundamental data creators in like manner assembled from the 352 families (300 commonplace and 52 metropolitans) of Muktsar District in Punjab. It was considered to be against the development when all is said in done medical clinic utilization from 1950 to 1990, there was a fast reduction in the comparable during the decade following the progression changes. The audit found that people creators progressively arranged to private medical care organizations. This over-reliance on private medical clinic fragments has provoked gigantic metropolitan commonplace varieties in the plan of clinic organizations. Due to lacking government thought towards the overall clinic division, the idea of its clinic organizations has rotted.

Researcher investigated the accomplishment of two essential emergency clinic ventures to control the adaptable diseases, specifically, the National Leprosy Eradication Program (NLEP) and the National Anti-Malaria Program (NAMP). It moreover intended to separate the example

in the event of lifestyle contaminations. The examination was done dependent on various clinic reports dispersed by the Ministry of Health and Family Author admission.

The results uncovered that the NLEP has been powerful in getting a diminishing the messiness cases. Despite the fact that the NAMP has expected a basic occupation in the control of Malaria coauthored the contamination has not yet been abstained from. The examination suggested that it very well may be possible just by taking genuine disinfection measures. On account of the move in the lifestyle of everybody of India, they have ended up being logically introduced to the non-adaptable sicknesses like Diabetes and Cancer. It was suggested that strong political will is required to battle with existing illnesses and various issues in the Indian clinic part. in their investigation dissected the association be written diverse emergency clinic markers and the money related status of everybody. The investigation was done using board data for 14 states from the year 1970-71 to 2000-01. The relationship is written the Life Expectancy during labor (LEB), Infant Mortality Rate (IMR), and various pointers were resolved with the per capita Net State Domestic Product (NSDP). The investigators set up that a two-way association is created these segments i.e better emergency clinic prompts higher per capita pay and more significant salary prompts better emergency clinic. In spite of what may be normal, a negative association was found among desperation and LEB. The IMR was seen to be oppositely identified with the per capita NSDP as the IMR extended with decreased compensation level [42]. The examination also revealed that the state with more conspicuous advancement in the thirty years had more prominent improvement in the LEB. Likewise, the open utilization on the emergency clinic was found to straightforwardly influence the emergency clinic pointers. Thusly, it was recommended that to construct the speed of money related improvement, a bigger measure of theory on the medical clinic region is required.

SECTION I

2.2 Studies on Punjab Health Scenario

Author researched the practicality and execution of the human administration’s benefits in the different districts of Punjab. The helper data was assembled from various circulated reports and the examination was made with the help of the stochastic edge’s strategy (efficiency examination). The future during labor was used as the yield pointer to test the efficiency of

emergency clinic organizations. Out of the significant number of locales of Punjab, Ludhiana was found to have the most efficient medical care workplaces. The higher life trust in Ludhiana was credited to the more important openness of subject matter experts and clinical orderlies nearby. The results exhibited that the creator viability of certain regions was not because of the shortfall of medical clinic establishment but because of the absence of various resources for run these workplaces. Further, it was represented that the abatement in clinic lopsided characteristics be written the areas of Punjab could provoke progressively efficient emergency clinic organizations. So, the expert suggested that the Punjab government should focus on the helpless performing areas [38].

The examination revealed that despite the fact that there was a development in state government medical clinic spending in authentic terms coauthored the bit of emergency clinic spending altogether out government utilize lessened in relative terms since the use of financial changes. Insignificant improvement was found in the populace served per bed from 1980 to 2004 showing stagnation in the organization's emergency clinic system. The results found that the bed inhabitance extent was incredibly low in the open clinical clinics achieving low utilization of general medical clinic establishment generally considering the bad quality of emergency clinic organizations. Lack of the emergency clinic labor force was represented as another significant issue in the emergency clinic division of Punjab. It was included that most of the medical clinic posts creators lying void due to lack of resources with the state. It was suggested that the state government should figure out how to improve the condition of general emergency clinic organizations by (1) encompassing state clinic approach (2) network help; and (3) growing general medical clinic hypothesis.

Author evaluated the presentation of the emergency clinic division in Punjab during the primary half-season of the 11th multi-year plan. The examination declared that the degree of budgetary allocation to a therapeutic and general medical clinic out of the total government use in the 11th plan was more creator than the 10th course of action [39]. The organization at first apportioned Rs 10, 321.5 lacs for the clinic region for the principal year of plan coauthored later it was lessened to half as a result of inability to start the new emergency clinic programs as organized. Further, it was found that out of the total medical clinic cost for the 11th course of action, only 5% was spent during the underlying two years. The deferral in support and course of action of the money was the huge clarification behind low utilization of the resources. The emergency clinic plans financed by the central government performed better than those

pushed by the state government during the hour of the examination. Rashtriya Swastha Bima Yojana and Punjab Nirogi Yojana creator and composed to be productive in achieving the ideal objectives. High maternal mortality in Punjab was included to be the most essential issue in the clinic region of Punjab. It was suggested that the law-making body should figure out how to encourage institutional transports to the maternal demise rate. Further, it focused that state medical clinic course of action should be enclosed as demonstrated by the medical clinic needs of Punjab [40].

Took apart the circumstance of the organization medical clinic division in Punjab and the impact of the plan of Punjab Health System Corporation (PHSC). The data creators took from various state government and central government reports. Rate procedure was used to see the example in the medical clinic markers. The results found that the amount of government guaranteed clinic associations lessened after the headway changes. It was highlighted in the investigation that even after the advancement of PHSC there was exceptionally little improvement in the vast majority of the clinic markers [41]. Despite the fact that the future in the state extended in the post-movement period coauthored the speed of addition was not actually the pre-progression period. The experts uncovered the helpless condition of the overall clinic organizations as the reason for the lessening in the quantity of patients treated each year. Further, it was suggested that the overall emergency clinic utilization should be extended by the state government to improve the medical clinic establishment.

Author assessed the course of action of emergency clinic organizations to the down and out people of India, particularly in Punjab. The data creators accumulated from both discretionary and fundamental sources. The helper sources fused the circulated reports at the state and central level. An illustration of 100 respondents was browsed the most insignificant financial social occasion of Ropar zone for a wise fundamental outline. The data study was done with the help of rate and ordinary methodologies. The results revealed that the reduction in monetary allotments to the overall clinic division provoked the breaking down of the organization healthcare administrations.

Appropriately, everyone creators left with no decision than to use the costly private emergency clinic organizations. Further, it was seen that the most un-blessed portion of the overall population was fiscally grieved by the enlivened advancement of unregulated private part. There was a shortfall of care among the dejected people with respect to the organization game

plans like the exemption of customer cost through yellow cards. Furthermore, there was no framework to screen the presence of private players related with open private associations. The examination suggested that the organization utilization in the clinic division should be extended and destitute people should be given information about the current medical clinic approaches which can financially help them.

Punjab Human Development Report (2004) exhibited that despite the fact that there was an improvement in the emergency clinic markers of the state yet simultaneously a ton of inefficient perspectives existed in the clinic structure. The organization task to the clinic region was seen to be bigger than other social divisions which have low thought towards the overall emergency clinic. The report likewise enlightened the mushrooming improvement of the unregulated private clinic care suppliers. It was revealed that preventive medical care was for the most part given by the public emergency clinic division while the private section obliged the medicinal human assistance's requirements.

Author enlightened the issues related to the privatization of human administrations with the help of cash related assistance from the World Bank. It was seen that the plan of restorative administrations organizations was made business activity by World Bank, in this way diminishing the organization's commitment to give essential emergency clinic organizations to its kinfolk. The yellow card plan pushed by Punjab Health System Corporation (PHSC) to give budgetary admission to the poor didn't perform creator. A large portion of the helpless person's creators were uninformed of this arrangement and the people who realized felt that it was difficult to obtain the card and after that reestablish it. A huge number of degradation cases creators in like manner found under the World Bank helped the undertaking of PHSC. Further PHSC was viewed as an equal system to the current clinic structure in Punjab. Additionally, it was directed by comparable people related to the state medical clinic structure. The investigation furthermore saw that the World Bank credit had extended the commitment authority of the state.

Author examined the issues facing the open private affiliation exercises in clinic division, particularly in the area of Punjab. It was revealed that the Punjab government gave distinctive persuading powers to the private region human administrations providers to hold hands with the council to set up a specialty clinical clinic. Punjab Urban Development Authority (PUDA) offered land with appointments up to 60 percent to attract more candidates. Regardless of such

offers, not a lot of bidders turned up and the plan didn't insight [40, 41]. The investigation coauthored that the shortfall of the real course of action improvement and the standards concerning the joint experience was the fundamental reason for the public authority's inability to convince the private part. It was suggested that prior to starting the open private associations, the Punjab Government should develop an instrument to screen whether the private accomplices follow the fundamental conditions or not. Other than this, proper methodologies should be shaped characterizing the work of the private division and the council in such errand.

SECTION II

2.3 Studies on Electronic Health Record

In this paper, author presented a framework plan where blockchain innovation is proposed to be utilized in the medical care framework, where the crucial data with respect to the clinical examinations are divided among emergency clinics, clinical centers, and research foundations dependent on access strategies characterized by the patients. To secure classified information, our answer includes the utilization of two kinds of chains: a private one, the side chain, which keeps data about the genuine ID of the patients, and a public one, the main chain, which stores data about patients' healthcare information set apart with a transitory ID. To test it, author build up the plan utilizing Hyper ledger Fabric structure [43].

In this paper, the author addressed the difficulties of information interoperability and administrative consistency when planning and sending medical care applications in a heterogeneous home-edge-cloud climate [44]. Author proposed the ChainSDI structure that influences the blockchain procedure alongside bountiful edge processing assets to oversee secure information sharing and figuring on delicate patient information. Author proposed programmable ChainSDI application programming interfaces to encourage the determination of locally situated medical services administrations running on a product characterized foundation (SDI).

As Internet of Things (IoT) devices and other remote patient monitoring systems become more common, security concerns concerning data sharing and logging are becoming more prevalent. Author proposed employing blockchain-based brilliant agreements to encourage secure

examination and the CEOs of clinical sensors to deal with the protected health data (PHI) created by these devices. This clever contract architecture would ensure continuous patient monitoring and clinical mediations by sending alerts to patients and clinical professionals, as well as keeping a secure record of who started these activities. This would resolve numerous security weaknesses related to distant patient checking and computerize the conveyance of notices to all included gatherings in a HIPAA consistent way [45],[46].

In this paper, author proposed plan and actualize a portable medical services framework for individual healthcare information assortment, sharing, and cooperation among people and medical care suppliers, just as insurance agencies. The framework can likewise be stretched out to oblige the utilization of healthcare information for research purposes. By embracing blockchain innovation, the framework is executed in a disseminated and trustless way [47].

In this paper, author proposed have proposed a lightweight blockchain design for medical services information the board that has low computational and correspondence overhead when contrasted with the Bitcoin organization [49]. Author proposed supplanted the energy-devouring mining agreement convention of the Bitcoin network with a versatile furthermore, an energy-proficient agreement convention. Additionally, our engineering isolates the hubs into groups, with each bunch having a chief that keeps up the record when contrasted with the Bitcoin network where all the hubs keep up the ledger. Our design utilizes an HBCM which produces the squares (repeated on the other BCMs) and requests the exchanges.

Electronic healthcare record sharing can assist with improving the precision of finding, where security and protection conservation are basic issues in the frameworks. In This Paper, author proposed blockchain-based secure and protection saving PHI sharing (BSPP) plot for determination enhancements in e-Health frameworks [50]. The private blockchain is answerable for putting away the PHI while the consortium blockchain tracks the protected files of the PHI. To accomplish information security, access control, protection conservation, and secure hunt, all the information including the PHI, catchphrases, and the patients' character are public-key encoded with a watchword search.

Existing IoT frameworks are powerless against a solitary purpose of disappointment and pernicious assaults, which can't offer stable types of assistance. Blockchain consumes more power if working on POW, which are not reasonable for power-compelled IoT gadgets. To

handle these difficulties, the author presented a blockchain framework with a credit-based agreement instrument for IoT. In this instrument, author proposed a credit-based proof-of-work (PoW) the component for IoT gadgets, which can ensure framework security and exchange proficiency at the same time. To ensure touchy information secrecy, they plan an information authority the board technique to manage the admittance to sensor information.

In this paper, author proposed talk about the idea of blockchain innovation and the obstacles in its selection in the medical care area. Besides, an audit is led on the most recent executions of blockchain innovation in medical care. At long last, another contextual investigation of a blockchain-based medical services stage is introduced tending to the disadvantages of ebb and flow plans, trailed by proposals for future blockchain analysts and designers [51].

In this paper, author proposed an insignificant blockchain-based medical care stage and look at its execution time and measure of information moved with the customer/worker framework model for healthcare records update and inquiry. This is with an expanding number of records and emergency clinics [52].

In this paper, author proposed a Blockchain Decentralized Interoperable Trust structure (DIT) for IoT zones where a brilliant agreement ensures validation of spending plans and an Indirect Trust Inference System (ITIS) diminishes semantic holes and improves reliable factor (TF) assessment by means of the organization hubs and edges. Our DIT IoHT utilizes a private Blockchain swell chain to build up reliable correspondence by approving hubs dependent on their between operable structure so that controlled correspondence needed to address combination and mix issues are encouraged by means of various zones of the IoHT framework [53].

SECTION III

2.4 Studies on Blockchain Security

2.4.1 Cryptography Techniques

Cryptography is a strategy that is utilized to get correspondence within the sight of outsiders. It is the way toward changing over the plaintext into ciphertext.

1. Public-key cryptography

The Ciphertext is encoded, it contains plaintext however unclear by a human or PC without legitimate code to decode. It expands the security of the message. There are two kinds of cryptosystem accessible, one is symmetric, and another is unbalanced cryptography. It is a cryptographic method, and it includes key sets, call it a deviated key pair, where one key utilized for encryption and another key is utilized for decryption [55].

2. Symmetric Encryption

Two gatherings utilize a similar key for both encryption and decoding. The symmetric structure is quicker contrasted with deviated as far as information control, and execution is likewise fantastic. The fundamental issue with these methods is to talk about subtly with somebody, should attempt to meet truly and concur on the mysterious key [56].

3. Asymmetric Cryptography

In asymmetric cryptography, two keys are used for encryption and decryption. The key pair is created for every client to move the record safely. Private keys should keep it mysterious and public key circulated unreservedly between parties. Anybody can encode the information utilizing the public keys, and the recipient gets the document and decode with the assistance of a private key. The message encoded with the client's public key and unscrambled with the mysterious key, and it builds the security of correspondence. Process demonstrated in fig 2.1.

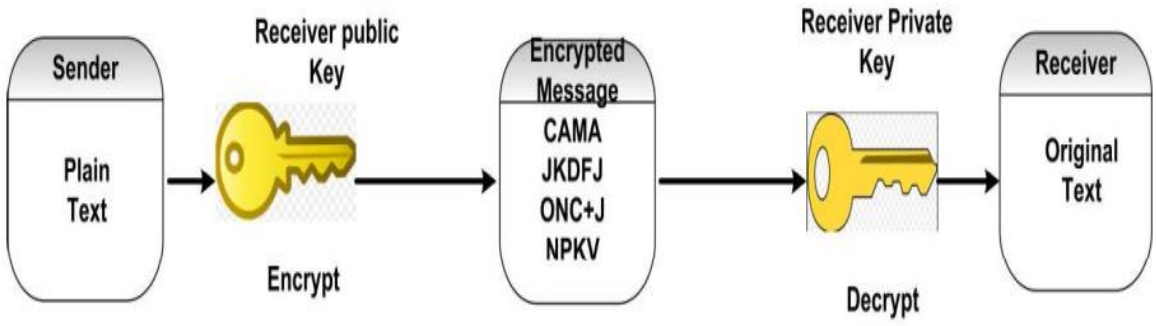


Fig. 2.1: Asymmetric Key Cryptography

4. Hashing

The way toward taking data and applying a hash work is called hashing. The hashing calculation thinks about the information as information, and produces a fixed-length as yield. In the block chain, the exchange solidified, and a hash is prepared. A Secure Hashing Algorithm (SHA) is used to make the hash [56]. The hashing is confined to a single direction work and not ready to adjust the interaction, and it is significantly unrealistic to utilize the respect sort out what the data was. A Secure Hashing Algorithm (SHA) is used to make the hash. The hashing is confined to a single direction work and not ready to adjust the interaction, and it is significantly unrealistic to utilize the respect to sort out what the data was. Hashing process is shown in Fig. 2.2.

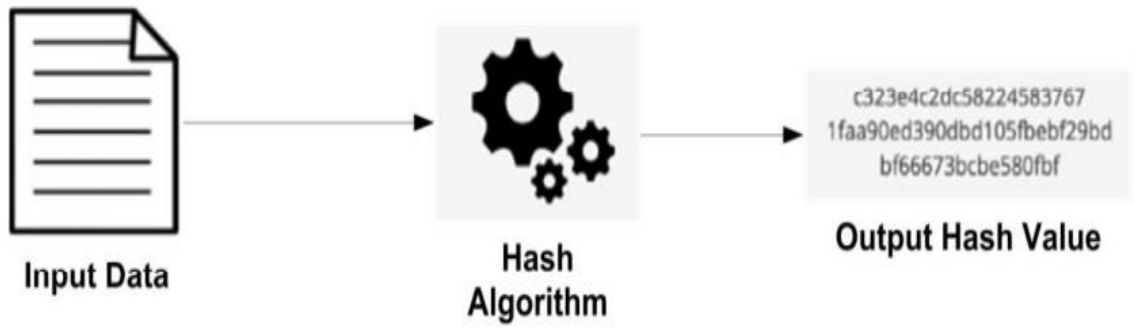


Fig. 2.2: Hashing Process

5. Digital Signature

A computerized mark is a mathematical technique used to check the realness and the uprightness of a message appears in Fig. 2.3. An advanced mark is identical to a manually written mark, it offers high security, and it is required to deal with the issue of modifying and confirmation in electronic trades. All clients claims a group of private keys and public keys. The private key that will be kept in classification is utilized to sign the exchanges. The carefully marked exchanges are communicated all through the entire organization. The run-of-the-mill advanced mark is engaged with two stages: the marking stage and the confirmation stage [59]. For example, a client Alice needs to pass another client Bob a message. (1) In the noticing stage, Alice encodes her information with her private key and sends Bob the encoded result and unique information. (2) In the confirmation stage, Sway approves the incentive with Alice's public key. In that manner, Bounce could undoubtedly check if the information has been messed with or not. The run of the mill computerized signature calculation utilized in the blockchain is the elliptic bend computerized signature calculation (ECDSA).

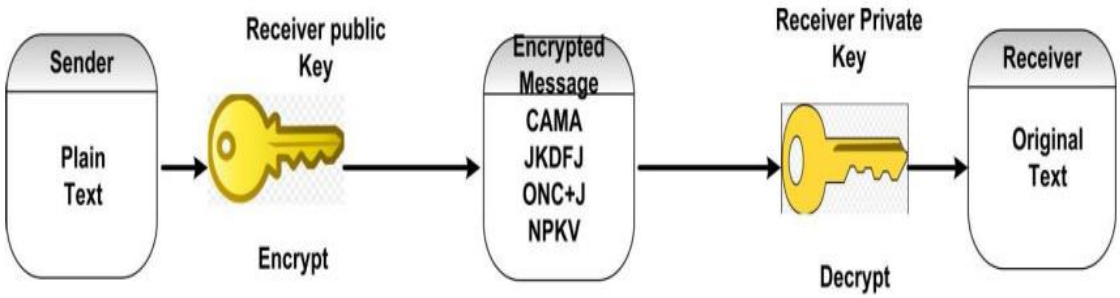


Fig. 2.3: Digital Signature Process

2.4.2 Cryptography in healthcare

Security and privacy are essential factors in the healthcare system. The extraordinary existing cryptography security arrangements like Identity-based encryption, the accompanying encryption procedure goes under open key encryption.

2.4.2.1 Identity-based Encryption

The specialist creates the patient healthcare data and it’s encoded with the public key of the patient. The public key is created dependent on the remarkable data of the client like email address, etc. Presently the patient needs to get to the healthcare record, and the private key generator validates the client at that point making the private key dependent on general society key of the patient. This key is just utilized for a specific healthcare record [61].

2.4.2.2 Attribute-based Encryption

The arrangement of qualities utilized for encryption and decoding measure. The key expert makes a public key and master key for the client. Every private key is related to an entrance structure over properties. During the decoding interaction specialist permits unscrambling the information utilizing the private key; likewise, it ought to fulfill the entrance strategy. The attribute-based encryption measure keeps up the monotonic access structure like AND, OR, etc.

2.4.2.3 Key-Policy Attribute-based Encryption

Key-Policy attribute-based encryption methods permit non-monotonic access structures. The healthcare record is scrambled, and it is related to a bunch of attributes, every private key related to the entrance construction of the ascribes. The specialist attempts to get to the encoded healthcare record, and it is permitted just for the ciphertext is related with ascribes and ought to fulfill the entrance structure, which is related with a private key [62]. The disadvantage is that the encryptor cannot decide who can decrypt the data, and also the data owner has to trust the key issuer. These issues addressed by Ciphertext attribute-based encryption.

2.4.2.4 Ciphertext-Policy Attribute-based Encryption

The fine-grained encryption procedure is used to encode the prosperity record, and each prosperity record keeps up its passageway plans. In ciphertext characteristic based encryption, a customer's private key is related to the game plan of attributes, and ciphertext is related to get getting approaches over credits [63]. For example, specialist or patient attempts to get to the

healthcare record, access authorization is given if and just if the characteristic of a specialist fulfills the entrance strategy of the ciphertext, at that point the specialist can unscramble the ciphertext.

By following the above methods, healthcare records are encoded and put away in the cloud. The cloud workers are an untrusted substance; it is each individual obligation to save the medical services data securely in the cloud. Since the patient keeps the private data in the cloud, it has been vital to keeping data free from any danger by the cloud advantage provider. Despite the fact that the patient information is achieved by techniques for applying distinctive encryption and storing that information into a cloud [64].

In a concentrated network, the one focal hub does the main piece of the work. In any case, it is deficient to get eHealth information in the cloud, on the grounds that the need to confide in the outsider and furthermore a solitary purpose of disappointment is in the cloud. In the E-healthcare framework distributed nodes and secure distributed nodes is not providing the level of security to data from the transaction in the electronic health records (EHR), the trustworthiness of e medical services records isn't kept up in the cloud, and it accomplishes by blockchain.

2.5 Types of blockchain

The three varieties of blockchain are public blockchain, private blockchain, and Consortium Blockchain as shown in Fig. 2.6.

2.5.1 Public Blockchain

The public blockchain is isolated into consent and permissionless. In Public permissionless, anybody can take an interest in perusing, composing, in the blockchain. Anybody can approve the exchange at a given time, and it is accessible to all. Anybody in the organization can confirm the exchanges by utilizing proof of work components (PoW). Every hub or framework in a decentralized organization will go about as excavators. The digger approves the exchanges, and all the diggers offer a similar response, at that point the square is put away in the blockchain. In the Public permissioned blockchain, anybody can peruse the information, however, as it where a predefined client can approve the value-based information [65].

2.5.2 Private Blockchain

In private permissionless blockchain just approved clients reserve the privilege to see the information. The information is not freely accessible and is put away in the private blockchain. The exchange is approved by the approved client like a senior representative, government, authority, establishment, etc., yet at the same time, delicate data can be ensured. In a controlled climate, high energy utilization, and low exchange throughput because of verification of work. Square has no exchanges; digger mine the square at regular intervals, recurrence of adding blockchain is sporadic. The advanced mark improved on measure used to confirm the personality. The administering party has no power over to guarantee the unchanging nature of the record. For, e.g., Healthcare information would prefer not to share freely, and it is noticeable to certain gatherings like a specialist, relatives, etc. In the present circumstance, the private consent blockchain utilized. The lone distinction is that the information isn't accessible freely [66].

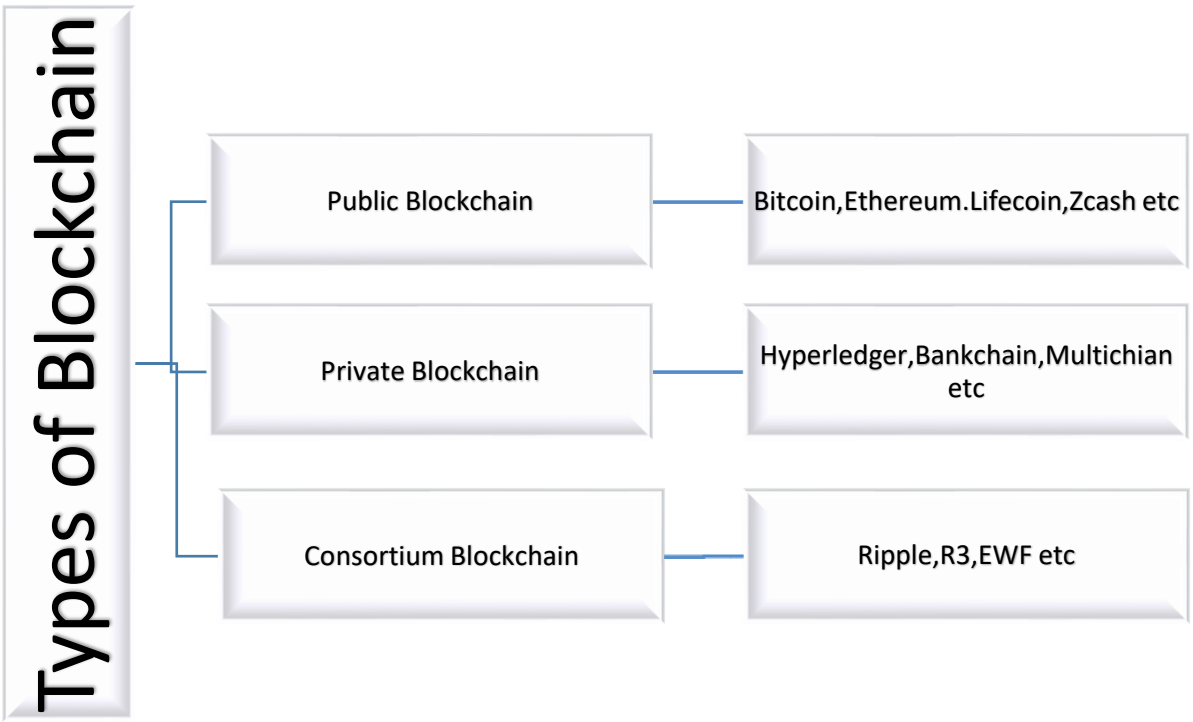


Fig. 2.4: Types of Blockchain

2.5.3 Consortium Blockchain

Consortium blockchain lies between open blockchain and private blockchain, which is reasonable for big business; the public authority empowers the adaptability and control of the information, which is put away in private and shared on the public record. The consortium blockchain ought to keep up more than one control, as opposed to a solitary control. The parties of the affiliations or agent individuals get together and make decisions for the best benefit of the entire system.

Table 2.1: List of the various blockchain that has been explained.

	Bitcoin (Nakamoto, 2008)	Ethereum (Wood, 2014)	Hyperledger (Cachin, 2016)	Cardano (Kiayias, 2017)
Founder	Satoshi Nakamoto	Vitalik Buterin	Brian Behlendorf	Charles Hoskinson
Governance	Bitcoin Developers	Ethereum Developers	Linux Foundation	Cardano Foundation
Transaction/second	7	20	3.5k-110k/sec	257
Avg Transaction fees	1.7USD	0.19USD	0	0.15USD
Open Source	Yes	Yes	Yes	Yes
Exchange Price	9000	700	-	.368
Programming tool	C++	Solidity	Go or Java	Plutus

2.6 Structure of blockchain

Each square which contains a rundown of exchange and square header. Fig 2.7 clarifies the design of the blockchain. The segment of the blockchain clarified beneath.

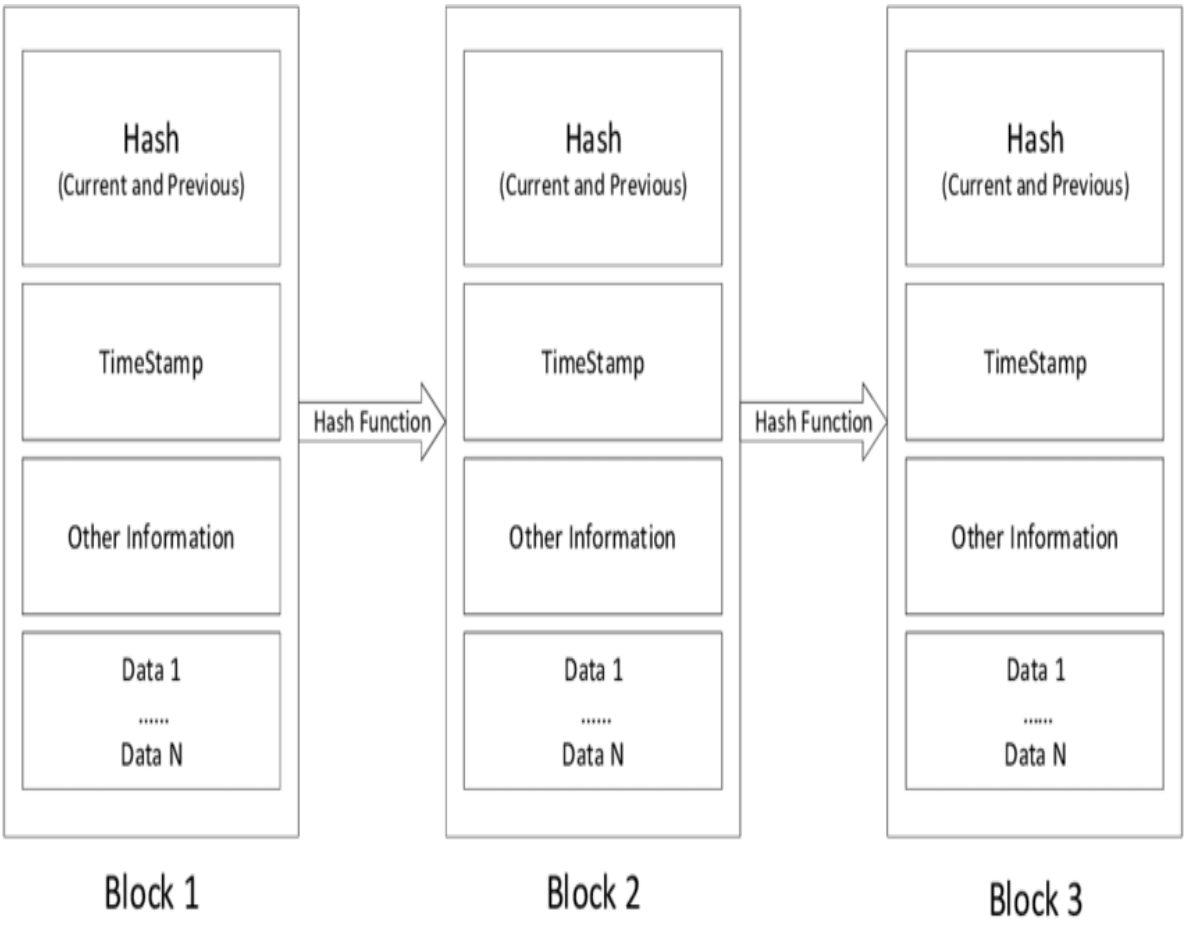


Fig. 2.5: Structure of Blockchain

2.6.1 Block

A square is perpetual information stockpiling. Square in the blockchain is comprised of square header furthermore, an organized in endorsed exchanges and hash pointer to the past block. In the SeFra system, Ethereum blockchain utilized for getting the eHealth records. In the decentralized organization, the hubs associated with a shared organization convention [67]. The Smart Contract runs on the Ethereum Virtual Machine (EVM), which goes about as a runtime climate. It naturally runs without the assistance of an outsider position.

At present, a normal of each square contains 350 exchanges. The digger dealt with consistently more trade. The excavator laborer makes a PoW (Proof of Work), which favors and checks the exchanges, and all confirmed exchanges are bundled and included as a square in a blockchain.

For example, consider a square in blockchain as a reliable, solid glass block. Each square will be open only for 10 to 20 sec, and no other square will be free in the interim. During that time, whoever bought anything (transaction), and whoever sold anything (transaction), everything consolidated in that block. When the time completed, that block is shut, and again it will be opened after that 15 second anyone can perceive what is inside that block yet can't change what is inside that block. After that time is completed, it is related with another square with a tough chain, and this occurs for all square in the blockchain. Each square records exchanges enlisted with hash and fixed and never modified [68].

2.6.2 Transactions

Each square contains numerous exchanges, and the exchange might be any information alongside a hash, parent hash, review data, and timestamp. Every exchange ought to contain hash, character, and timestamp information. Separated, other information properties can be fused, which are specific to the one-of-a-kind use case. Since portrayed the Merkle tree of exchange data adequately, at that point it ought to continue ahead to impacts a square information structure [69].

2.6.3 Header

The Header contains three unique arrangements of metadata as follows. The hash estimation of the past header, Merkle root tree, and mining rivalry.

2.6.4 Previous block hash

In Blockchain, each square is connected with the last header block, and with the new square hash made with the past block hash.

2.6.5 Merkle Tree

Merkle trees are a fundamental primary piece of a blockchain. A Merkle tree partners data is using SHA-256 hashes in a tree structure. An underlying root hash esteem made; this is the Merkle Root. As the kid hub included, the essential root hubs will contain hashes of the

youngster hub. The tree structure keeps up the solicitation that data is added to the tree and empowers it to approve changes to the kid hub. It is not difficult to recognize the changed hash by following the way of the tree. The fundamental benefit of this tree structure is that the approving the kid hub by contrasting it and a parent hash in the tree. Every quiet record hashed and put away in the square. The hash of the two patient records is hashed together to produce another hash. This strategy, eventually, gives a solitary root hash an incentive from all exchanges inside the square. The foundation of the Merkle tree contains the exchange of the squares. When the exchange made and put away in the square, at that point testing to adjust [70].

2.6.6 Mining

Mining is the foundation of all confirmation of work-based cryptographic types of cash. The confirmation of work is the prerequisite to playing out the PC computation is called mining. Now, the digger makes new squares and adds them to the blockchain. During this time, excavator uses gigantic computational ability to discover the response for cryptographic conundrums to satisfy a dangerous level. The essential utilization of mining is to affirm the genuineness of a Trade, or avoiding the alleged twofold spending, and to make recently progressed financial structures by compensating mineworkers for playing out the past task. The provokes allocated to all hubs in the organization. Every hub goes about as a excavator and tackles the riddle utilizing it is registering power. The Miner hub who tackles the riddle will get a prize, at that point the square is added into the blockchain.

2.6.7 Timestamp

Timestamping is the way toward checking the production of the exchange and change of the exchange regarding time. Each record alluded to existed at a particular date and time. This will keep away from the twofold spending issue. Security here suggests that no one not using any and all means the proprietor of the exchange should have the choice to change it whenever it has recorded given that the timestamp's genuineness is rarely compromised [71]. Every exchange hashed and hash is annexed with the exchange and set aside in the blockchain, which fills in as an ensured affirmation of the particular time at which that data existed. The evidence is because of a gigantic measure of computational exertion performed after the hash value

generated to the blockchain. Altering the timestamp would require more computational assets than the remainder of the system consolidated and is impossible unnoticed.

2.6.8 Nonce

A nonce is an irregular number that is added to a hashed block, when repeated, meets the difficulty level controls. The nonce is the irregular number that is chosen by blockchain excavators dependent on the numerical riddle. The nonce esteem relies upon the hash of the string data. The goal is to join a mathematical impetus to the completion of the message so that, when united, get a particular course of action of zeros at the beginning of the hash [72].
Totally, the organizing rules could be any course of action of characteristics 0-F at any location in the hash. The excavator chooses the hash esteem begins with the number of quantities of zero the choice simply dependent on the objective and trouble esteem. The probability of any foreordained course of action is correspondingly as likely. It should uphold more computational ability to reevaluate the nonce for each square in the chain.

2.7 Merkle tree implementation in blockchain

Merkle trees are the fundamental part of the blockchain. It permits us to get check of broad information. Merkle tree consolidates all exchanges and delivers a solitary computerized unique finger impression, accordingly engaging a customer to check whether or not a trade consolidated into the square. Merkle trees are made by again and again hashing sets of hubs until there is only a solitary hash left called the Merkle root. They are worked from the base up, from hashes of individual exchanges. Merkle root joins the exchange and stores it in the square header. It keeps up the trustworthiness of the information. Using a Merkle tree contemplates a smart and direct preliminary of whether a specific trade consolidated into the set or not [73], [74].

A Merkle tree contrasts from a hash-list. In Merkle tree, one branch can be download on the double, and the trustworthiness of each branch can be expeditiously affirmed, in any case of whether whatever is left of the tree isn't yet open and makes it beneficial that record separated into little data blocks, with the ultimate objective that simply little squares ought to be

downloaded again if the first form hurt. The SWOT analysis of blockchain is described in table 2.2.

Table 2.2: SWOT analysis of Blockchain

Strength	**Weakness**
Cost efficient No need for intermediates Automation Accessible world wide Transparency No data loss Autonomous	Scalability Low performance Lack of storage capacity Some results achieve with well-mastered technologies
Opportunities	**Threat**
Less fraud risk User get more control over data Availability of huge amount of data from different transactions Possibilities of address to new markets	Non standardization Interoperability issues

2.8 Series of Blocks

A blockchain is a brilliant plan to store data. This advanced data comes in blocks, these squares are integrated, and this makes the data perpetual. Exactly when a square of information added to the chain, it is data that can never be changed again, it will be straightforwardly open to any person who needed to get the information back in an exact way wherein it added to the blockchain, is shown in Fig 2.8. Each report conveys the transactions that cutoff to 1MB, etc.

Here reports are the squares of data. These squares are associated, the exchange in the square, which creates a novel mark for every exchange in the square [75]. On the off chance that there are any adjustments in the square data, the entire square mark gets changed. This interaction occurs through hashing.

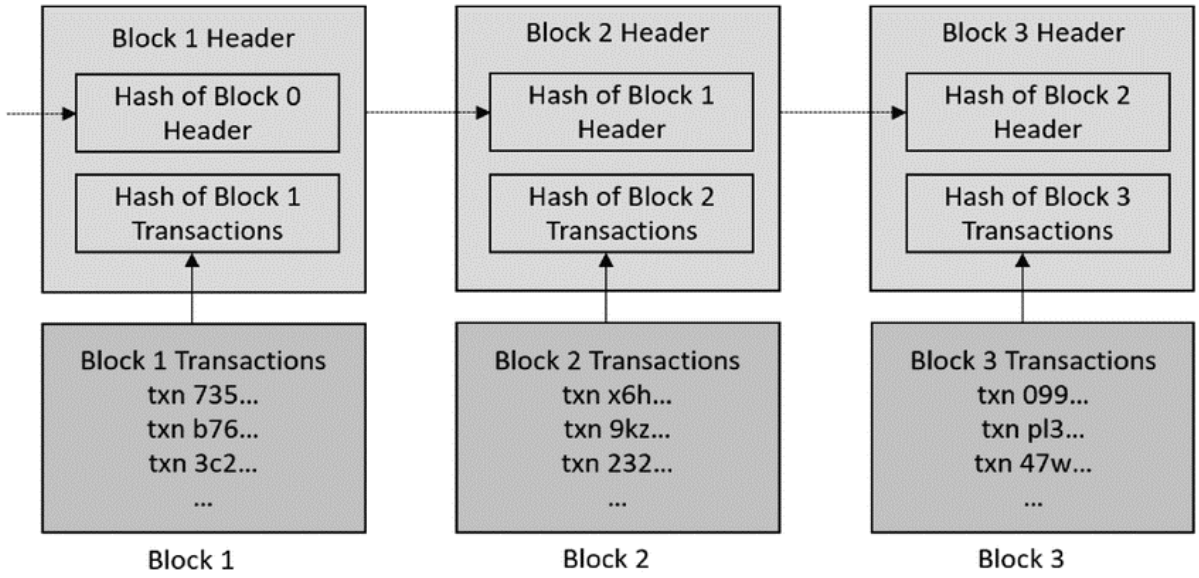


Fig 2.6: Series of blocks in blockchain

2.9 Advantages of blockchain

Blockchain has the advantages of being dependable, trustworthy, convenient, and permanent.

1. **Reliable**

Blockchain is not governed by a third party, but it does give all direct participants some contr ol over the entire chain.

As a result, the blockchain is much safer and more stable in the face of cyberattacks.

Even if one of the chain nodes is attacked and compromised, the rest of the distributed inform ation nodes will continue to operate and provide services.

2. **Transparent**

Transactions are available to all members, ensuring that activities are transparent.

3. **Smart contract**

Smart contracts can be created and sent in various blockchain stages (e.g., NXT, Ethereum, and Hyperledger Fabric). A few stages offer particular highlights for creating brilliant agreements including contract programming dialects, contract code execution, and security levels.

4. **Blockchain** is trustworthy and secure: The data in the blockchain cannot be altered in some way and remains unchanged.

5. **Irreversible**

It is possible to conduct simultaneous exchanges using the blockchain, which are both unalterable and easier to follow. This ensures that they can be endured indefinitely, with no chance of being altered or dropped.

2.10 Existing Healthcare Frameworks with blockchain

The chapter delves into the various existing healthcare ventures, such as MedRec, Medichain, Patientory, KSI blockchain, Provchain, BSPP and decentralized name based security. Many of the current healthcare programs are pilot ventures, while others are ongoing [77]. Guard time and Estonia, is the first organization to introduce a blockchain-based eHealth system, and KSI Blockchain is the name given to it. The Estonian government uses the KSI blockchain system.

2.10.1 Medichain

By allowing physicians and experts to access health information from anywhere in the electro nic health system, the Medichain framework stores health information in the appropriate geog raphic domain [86]. Figure 2.9 depicts the Medichain structure. The patient's health information is stored in the cloud, and the blockchain specifies the rules for accessing the

patient's health information. Other doctors can access some details from the patient's medical record using this device. Different departments, such as pharmaceutical and science, have access to the results. The researcher can access the anonymized data for analysis, while the pharmacist can access the anonymized data for prescription. For example, the researcher may obtain partial information from medical records, such as age, in a simplified form [86].

Each user is verified by a third party and granted a unique blockchain ID by the membership service provider. Each consumer has the ability to play the roles of patient, health care provid er, and caregiver. Per-user can register for all three roles and receive separate IDs for each. The health record can only be accessed by the user.

The owner and caregiver have permission to share the information with others.The medichain architecture (Fig. 2.7) looks at how patient health data is encrypted and stored in the cloud, such as prescriptions, billing, lab reports, and diagnostic photos. As a result, hash assets are held on the blockchain.
With the aid of their Smart Contract, they can access the electronic medical record. The Script File (Smart Contract) keeps track of the health record's viewing permissions and data retrieval.

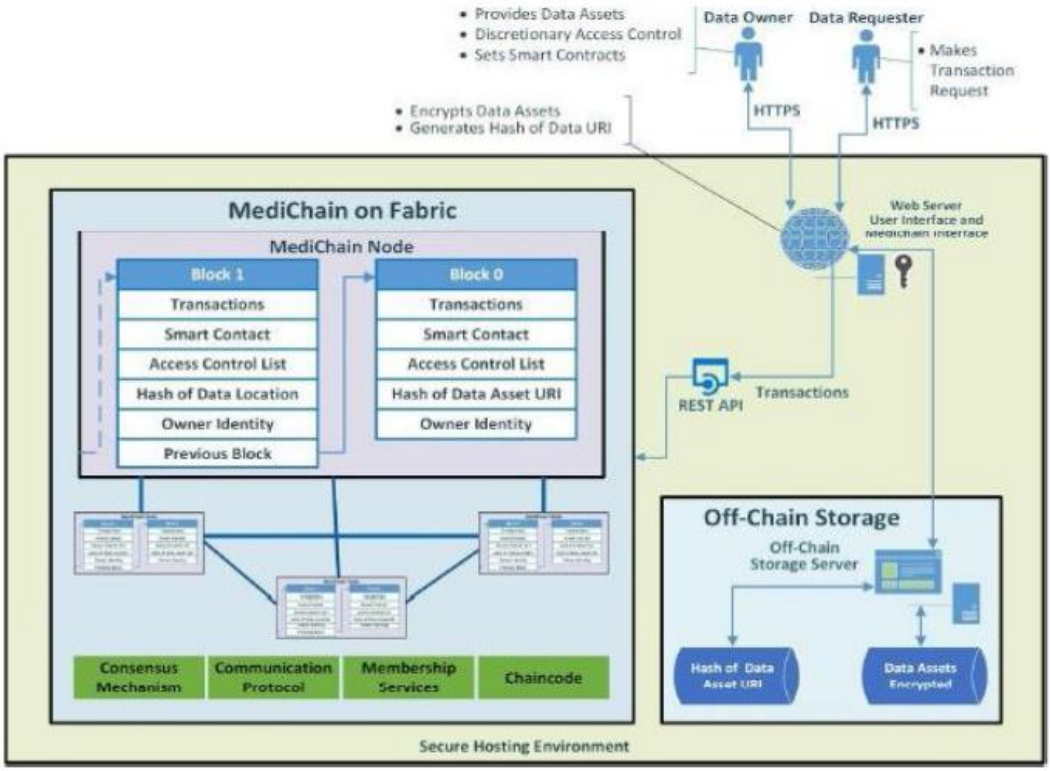


Fig. 2.7: Medichain Framework

The patient is the central figure of MediChain, and he or she has the authority to exchange health records with others. It is a safe protocol that allows patients, health practitioners, and caregivers to share health information. Performance testing, evaluating the blockchain application's likely attack vendors, security threats, and monitoring device activity are all part of MediChain's future work [86, 94].

2.10.2 Medrec

MedRec is a blockchain-based decentralized system for sharing electronic health information. This system provides patients with a comprehensive, ever- changing log, as well as easy access to their medical information between suppliers and treatment websites [95].

When considering healthcare data, using the specific blockchain properties of validation (auth entication), confidentiality, and knowledge sharing. to expand the number of restorative partn ers (scientists, general healthcare experts,etc)As a result of controlling and anchoring the syst

em using Proof of Work, to take an interest in the system as a blockchain ‘miner' and provide them with access to complete, anonymized information as mining rewards [96].

The MedRec architecture, as shown in Fig. 2.10, is used to protect the eHealth record in the b lockchain.
The MedRec system addresses problems such as system interoperability, slow medical data a ccess, and increased data quality and quantity. The anonymized data in the blockchain is held for the researcher's gain. The blockchain Smart Contract provides a log, which includes viewing permission and data access retrieval information. If a doctor or administrator creates a new medical record, the patient's only privileges are to share information with other providers. Each patient record is identified by a unique ID, such as an SSN or a date of birth. Using public-key cryptography, each patient record is linked to unique ID.

Contracts such as registrar contracts, overview contracts, patientprovider relationships, and so on are included in the architecture. The patient's medical history is preserved by the summar y contract. It contains references to Patientprovider Relationship Contracts (PPRs), which refl ect the system's current and previous participants. The patient has the right to share the medical record with the approved recipient, and the provider is likely to make suggestions to the patient. It sends out notifications to users about new relationships, ending updates, and patient acceptance that hasn't been accepted. The relationship status is set by the provider, and the patient can choose which relationships to accept, delete, or reject. In this case, the patient has the option of leaving or rejoining the distributed network several times. The patient will get the most recent blockchain by downloading it also keeps track of the most recent blockchain log [86].
User, admin, library, and database are the four components of this design. The patient information is identified and matched with an Ethereum address in Library, and the summary contract is then easily found. The new PPR is uploaded to the system by the supplier. It refers to the data held by the patient's Ethereum address on the blockchain. The patient will later find the data thanks to the transaction node, which connects the new PP R contract to the summary contract.

Per user is assigned a unique ID and address, and it's up to them to keep track of them.
The registrar contract address makes it simple to locate the summary contract. The modificati ons to the Summary contract were noted in real-time by services.

EHR Manager took notice of the user's message and linked to the local database automatically. Gatekeeper receives the client's cryptographically signed order, which is provided by the server. Identity assurance is the responsibility of the issuer. The data must be returned if the address has been given to the customer. With the aid of the registrar contract, the patient chooses which data to share with other users based on his address. When all of the components are combined with the EHR framework, the user can update, display, share, and retrieve data. The python framework was used to create this application .

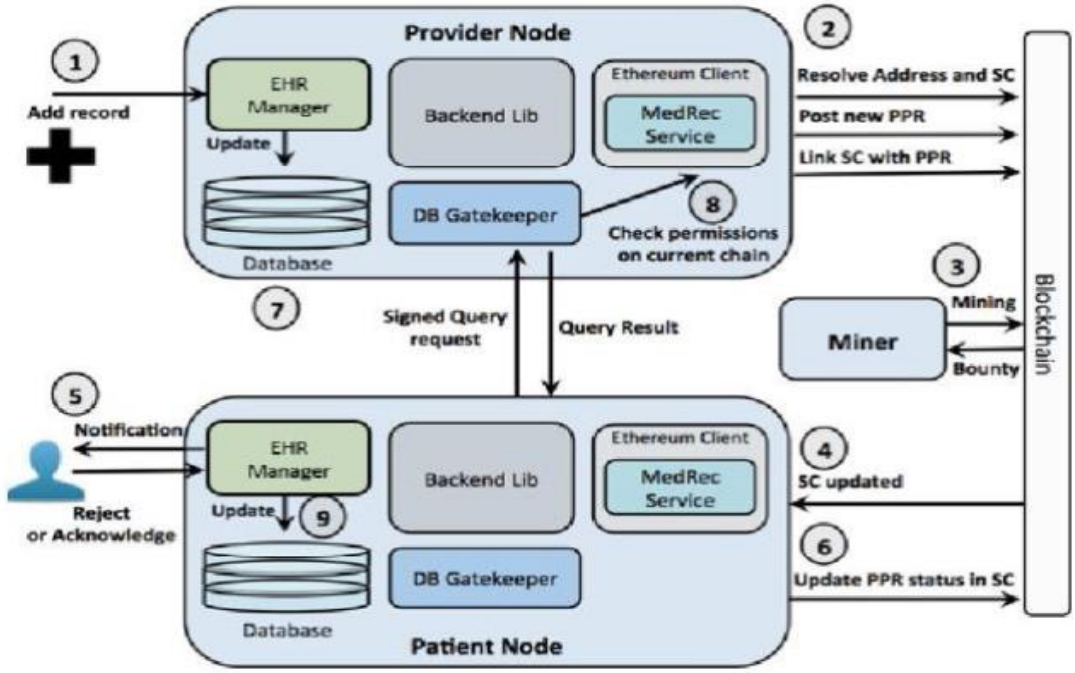


Fig. 2.8: MedRec System

The future work will include regularly working with various stakeholders such as a hospital, pharmaceutical firms, insurance companies, government agencies, and so on. More security testing is needed, and it is planned to be released as open-source software tool.

2.10.3 Patientory

Patientory, USA was created by ChrissaMcFarlane in 2015. It is a membership-based non-profit organisation. This website protects the privacy information of patients, medical institutions, and providers. Patientory organizer Chrissa McFarlane asked the UK government to "get behind a blockchain-empowered national IT system" during the malicious ransomware attack against the NHS [98]. while also assisting in the removal of legitimate deterrents in the healthcare system Information exchange between suppliers is growing. She predicted that the use of blockchain innovation in a complex national social insurance framework, such as the UK's, will last no more than two years – assuming there is political will to implement it have an impact. Patientory is mostly used for health information sharing (HIE), removing the need for third-party intermediaries [99]. The decentralised mechanism that facilitates trust disintermediation, lowers transaction costs, and improves integrity. The HIE reduces costs and improves the continuum of care cycle by reducing unnecessary administrations and copy tests while adhering to all HIPAA values benchmarks. The way healthcare stakeholders handle electronic medical records is changing thanks to patient link with clinical care teams and obtain details. Fig 2.11 shows a diagrammatic view of the Patientory scheme [103]. This system keeps track of patient-related outcome measures (PROMs), which enables clients to access a patient profile and track their medical history. Patients' side effects should be used in PROMs, as well as the treatment's personal satisfaction pointer. By providing an increasing point by point and full evaluation of drugs for particular conditions, the system will facilitate patient-doctor communication about the weight of treatment-related diseases. Special appointments, hospital costs, individual therapeutic data, protection, and drug store prescriptions are just some of the ways the system helps the patient.

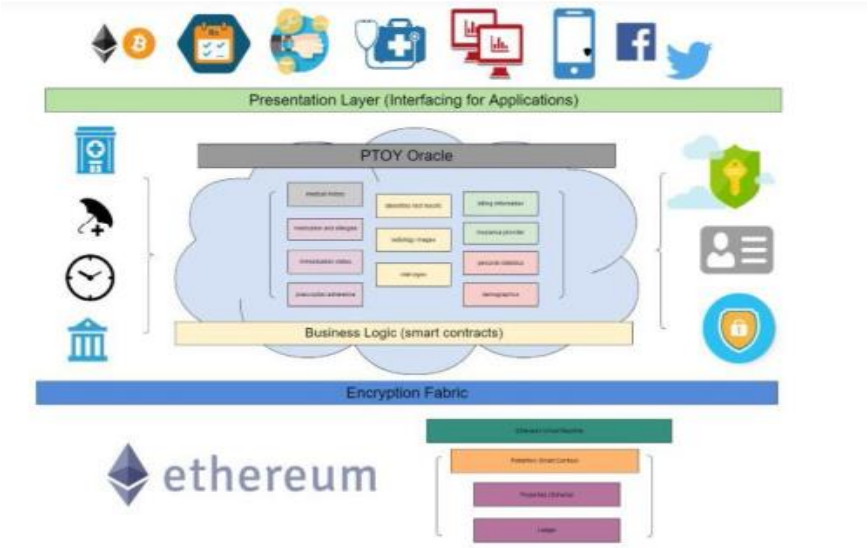


Fig. 2.9: Patientory Framework

2.10.4 ProvChain

ProvChain is a data provenance architecture based solely on blockchain and the cloud, as shown in Figure 2.12. Real-time cloud data provenance, improved privacy protection, tamper-proof environment, and provenance data validation were among the four goals set out. Provenance client activities are reviewed in realtime cloud data to collect provenance informa tion, which is also used to verify the access control policy. The information provenance recor d is collected in the Tamper Proof setting and then distributed to the blockchain network, whi ch secures the provenance information. The data stored in the blockchain is shared by peers. Without the assistance of a third party, ProvChain creates an open timestamped log of all client activities on cloud information [103]. Each piece of provenance data in the blockchain has a receipt that can be used for future verification. To preserve privacy, each user's data is assigned a hashed User ID in Enhanced privacy preservation. The data can be accessed by the Provenance inspector, but the original user is never discovered. The final step is data validation, which involves storing records in the blockchain network and having several nodes validate each block. Every provenance information passage is approved by ProvChain using a blockchain receipt.

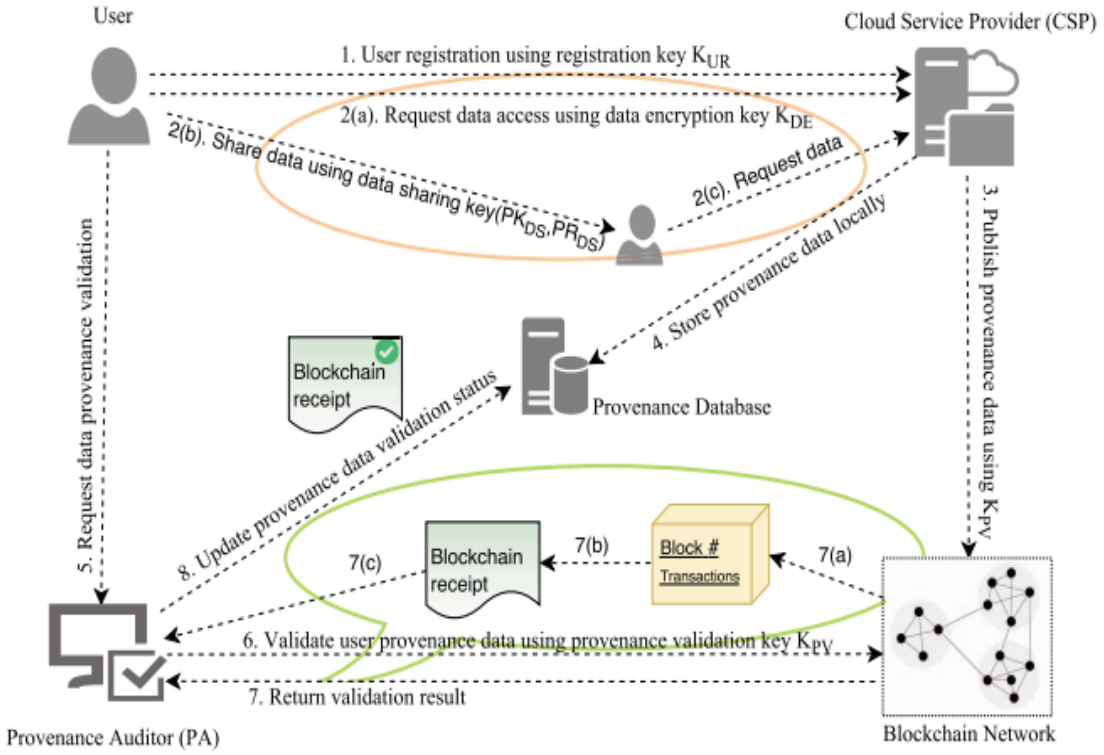


Fig. 2.10: ProvChain Framework

Cloud customer, Cloud service provider, Provenance Database, Provenance auditor, and blockchain network are all part of the Provchain architecture. The user has the ability to share and store their information on the blockchain. The data changes have been checked by blockchain nodes [112]. The cloud service provider is the next component; it provides storage and user registration. It tracks data changes and can gather a significant amount of information about each client's information activities in order to improve their administration; it also detects intrusion. It primarily safeguards their regular eHealth records. Provenance database records on a blockchain network which used for the malicious system. The provenance auditor can retrieve the data from the blockchain and validate the blockchain receipt. The Last one is the blockchain network consists of different nodes that will certify and recorded in the form of blocks. Future research will focus on developing data provenance for multiple clouds (Federated cloud). The validation process was performed on top of open-source, and this architecture was used to enhance security.

2.10.5 Keyless Signature Infrastructure (KSI)

Estonia's eHealth infrastructure is the world's most technologically advanced. Guard time, a blockchain pioneer, and Estonia's eHealth Authority signed an agreement in March 2017 to verify the health records of over a million Estonians. The Keyless Signature Infrastructure (KSI) blockchain was launched by the Estonian government. To avoid any security breaches, the Blockchain was developed [85]. A popular eHealth platform was proposed by the Estonian government. The guard time is the first blockchain organisation to introduce an eHealth system. The KSI was founded by a community of 150 cryptographers, designers, and security draughtsmen. The security draughtsmen have a lot of experience protecting structures from intruders. Different countries deal with data breach management, securing the fundamental infrastructure, enabling safe e-government action, and collaborating with financial markets, media delivery partners, insurance companies, and aviation undertakings.

Keyless signature infrastructure is a data-driven encryption invention that relies on cryptography hash functions, needs only hash-value learning, and is best implemented as a binary tree. Figure 2.13 shows the KSI hashing signature. The KSI system consisted of four parts: a gateway, an aggregator, a verifier, and cores. The hash values are received by the gateway, which forwards them to a higher layer, where the aggregator aggregates the transaction and sends it to the centre. For each second, the core keeps track of the top root value. The KSI signature was created and will be used to access the transaction in the future. For the eHealth system, the KSI provides auditability, governance, accountability, and security. In 2016, the keyless authentication method was patented. Over 95 percent of the data is produced by providers and doctors and is then digitised. The majority of the data are sensitive and, in many cases, contain inherited information about patients [106].

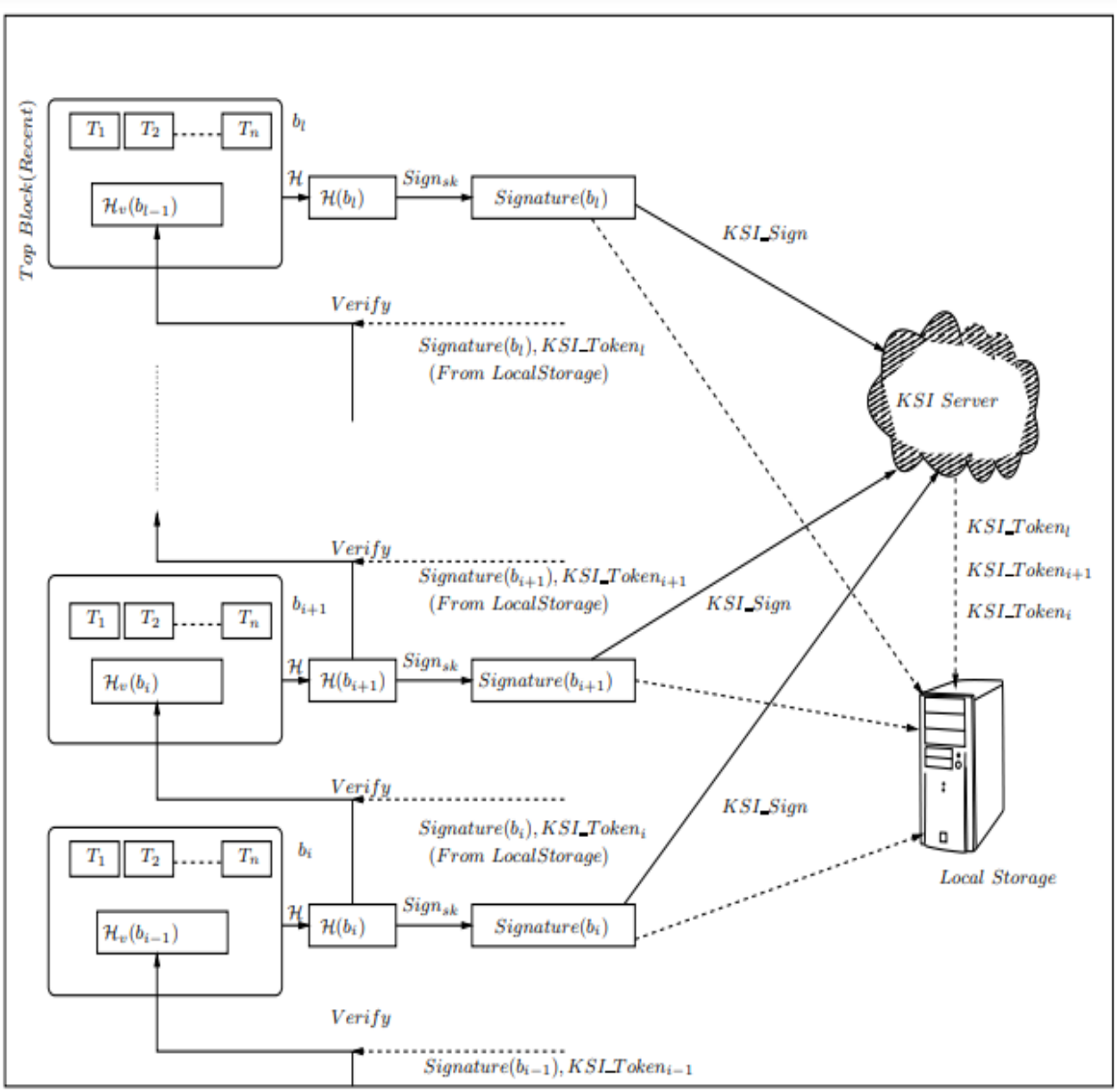


Fig. 2.11: Keyless Signature Infrastructure Hashchain

2.10.6 Blockchain-based Secure and Privacy-Preserving PHI sharing protocol (BSPP)

The exchange of electronic health records will improve treatment accuracy, and the eHealth system's problem is protection and privacy. The electronic health record is safe and confidential thanks to blockchain, as seen in Fig. 2.14. Private blockchain and consortium blockchain are the two forms of blockchain that are used. The protection of the files can be improved by storing the electronic medical record in a private or consortium location. Every piece of information,

including PHI, the patient's unique identification, and the keyword, is publickey encrypted in order to achieve information security, access control, security safeguarding, and secure search. The role of the block generator is to create a new block in the blockchain. The author proposed a JUICE scheme to quantify efficiency [107].

The author proposed the BSPP platform, which is a blockchain-based stable and privacy-preserving PHI sharing protocol. The majority of city doctors are willing to share their medical records [108]. Two blockchains were used for security purposes: a private blockchain for each hospital and a consortium blockchain. The keyword of the Patient health record, which is created by the hospital, is stored in the own blockchain store, the patient's health record, and the consortium. The structure has three components: a system manager, a service provider (a hospital), and clients (patients). The device manager is in charge of charging the system.

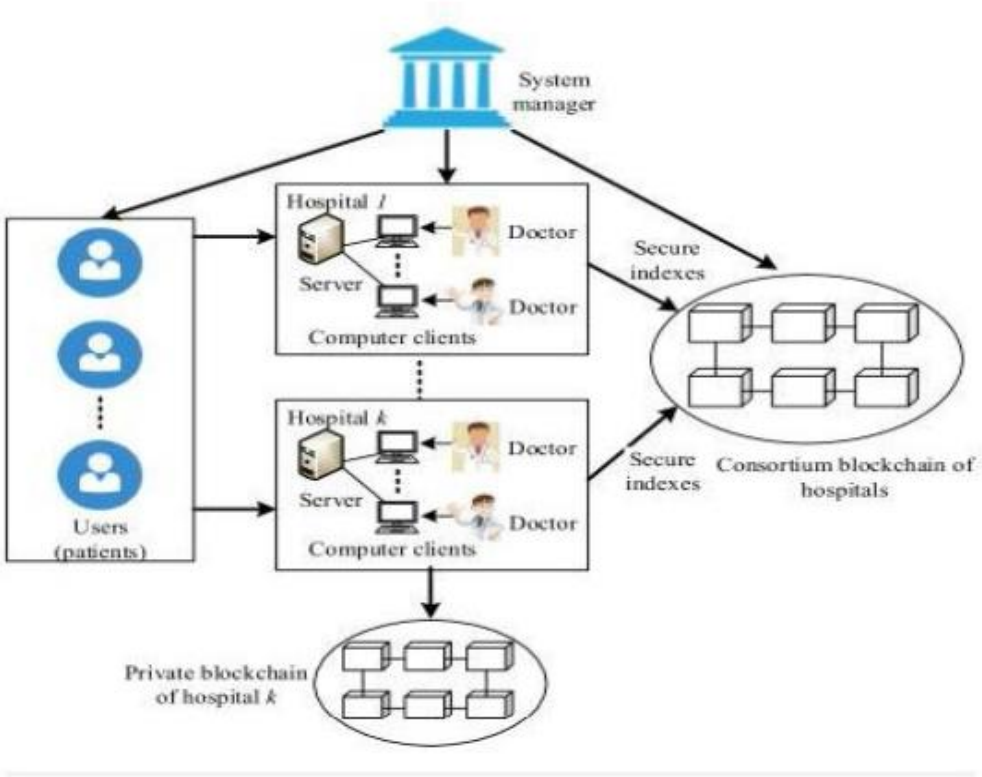


Fig. 2.12: Blockchain-based Secure and Privacy-Preserving PHI Sharing Protocol

Any client and professional must register with the framework supervisor. For doctors and patients, it generates parameters and maintains the public key tree. The next person is a doctor who helps the patient with medical issues. Each hospital has a server and a number of PCs

where the doctor enters the patient's medical information. The doctor creates a block for storing and broadcasting health information. The registration table for both the doctor and the patient is held on the server [109]. It is up to them to collect new blocks for the private blockchain and figure out new blocks for the consortium blockchain. The new block for the consortium blockchain is checked by the node, to obtain the client's health records, the doctor must be verified outside of the private blockchain. Last but not least, before observing the doctor, the patient must first report on the server.

After enlistment, the server will issue a token to each patient. To ensure the validity of the token, the patient should show it to the doctor and authorize the doctor to produce the patient's health record. The patient visits many hospitals for various treatments, with all of the patient's health records being stored in the hospital's private blockchain. Each patient's health record is encrypted and decrypted using the patient's public key and private key. The signature ensures the health record's credibility. Focus on storage overhead, time overhead, and communication overhead when assessing results. The Ethereum blockchain and a Smart contract were used to create this project. For the Smart Contract, solidity was used. Java and Javascript were used to build the tool. The conjunctive keyword search will be considered in future work, as well as the creation of a verifier election algorithm and a special miner for the health care blockchain.

2.10.7 Decentralized Name-based Security

For security purposes, the author discovered three parameters: system name, content, and user. The information centric network (ICN) network's content delivery system. The content protection framework is used to protect the content that is distributed. Content storage, content integrity, and content provenance verification are all provided by the HIBE. As a result, there is no trusted authority or central authority to produce keys [111].

The identity of the user is regarded as a public key. Each personality's private key is generated by the Private key generator. The Patient needs to share the specific content name (Patient record or file) with another person, and it then uses content names to provide integrity protection and content provenance verification. During the transaction, the content integrity defence guarantees that the content does not change. Each piece of information stored in the content storage node is delegated in content storage delegation. Using the trust delegation algorithm, the owner may allow the storage node to store content on his or her behalf. The

HIBE Delegation Algorithm generates secret keys SKs that correspond to content item names, stores them in an approved node, and distributes them to this node. The other user sends a query to blockchain to retrieve the information in Content Retrieval, and the question contains the content name of the requested content name. Following that, the other user issues a regular ICN content retrieval request.

The HIBE scheme was used for the original order settings, and the Charm-Crypto Library was used for implementation, The maximum data size in Namecoin is 520 bytes. The blockchain is 1.4 GB in size, and searching for records takes less than 5 milliseconds. The trusted party obtains a copy of the blockchain and responds to a request sent over a protected channel. The data owner may delete the authorization from a storage node to store any content using the de-authorization method. The use of key expiration is another choice. In all responses, a key expiration date was appended to each transaction. Comparison of existing E-healthcare frameworks exhibit in table 2.3.

Table 2.3: Comparison of existing E-healthcare frameworks

Framework	Description	Technology
Medichain [86]	Each user is verified by a third party and granted a unique blockchain ID by the membership service provider. Each consumer has the ability to play the roles of patient, health care provider, and caregiver. Per-user can register for all three roles and receive separate IDs for each. The health record can only be accessed by the user.	Blockchain Smart Contract
Medrec [95]	The MedRec system addresses problems such as system interoperability, slow medical data access, and increased data quality and quantity. The anonymized data in the blockchain is held for the researcher's gain.	Blockchain Smart Contract

Patientory [99],[101]	Patientory is mostly used for health information sharing (HIE), removing the need for third-party intermediaries. The HIE reduces costs and improves the continuum of care cycle by reducing unnecessary administrations and copy tests while adhering to all HIPAA values benchmarks.	Ethereum
ProvChain [103]	Cloud customer, Cloud service provider, Provenance Database, Provenance auditor, and blockchain network are all part of the Provchain architecture. The user has the ability to share and store their information on the blockchain. The data changes have been checked by blockchain nodes.	Blockchain network and cloud
Keyless Signature Infrastructure (KSI) [85], [106]	Keyless signature infrastructure is a data-driven encryption invention that relies on cryptography hash functions, needs only hash-value learning, and is best implemented as a binary tree.	Hash chain
Blockchain-based Secure and Privacy-Preserving PHI sharing protocol (BSPP) [107]	The author proposed the BSPP platform, which is a blockchain-based stable and privacy-preserving PHI sharing protocol. The majority of city doctors are willing to share their medical records. Two blockchains were used for security purposes: a private blockchain for each hospital and a consortium blockchain.	Blockchain
Decentralized Name-based Security [111]	For security purposes, the author discovered three parameters: system name, content, and user. The ICN network's content delivery system.	Information-centric networking

Table 2.3 depicts existing e healthcare frameworks and their respectively used technologies. MediChain is a public blockchain medical information network and data stored off-chain in a compliant cloud, MediChain uses blockchain to record pointers and rules on usage and anonymity [86]. MedRec is a blockchain-based decentralized system for sharing electronic health information. This system provides patients with a comprehensive, ever- changing log, as well as easy access to their medical information between suppliers and treatment websites [95]. Patientory is mostly used for health information sharing (HIE), removing the need for

third-party intermediaries [101]. In ProvChain framework used to preserve privacy, each user's data is assigned a hashed User ID in Enhanced privacy preservation. The data can be accessed by the Provenance inspector, but the original user is never discovered. The final step is data validation, which involves storing records in the blockchain network and having several nodes validate each block. Every provenance information passage is approved by ProvChain using a blockchain receipt. Keyless signature infrastructure is a data-driven encryption invention that relies on cryptography hash functions, needs only hash-value learning, and is best implemented as a binary tree. Blockchain-based Secure and Privacy-Preserving PHI sharing protocol is a blockchain-based stable and privacy-preserving PHI sharing protocol. The majority of city doctors are willing to share their medical records. Two blockchains were used for security purposes: a private blockchain for each hospital and a consortium blockchain. Decentralized Name-based Security used for security purposes, the author discovered three parameters: system name, content, and user. The information centric network (ICN) network's content delivery system. The content protection framework is used to protect the content that is distributed [111].

CHAPTER 3

Research Methodology

This section covers the research methodology to access existing system and proposed framework. In order to access existing E healthcare system a questionnaire was prepared consisting 40 questions related to various issues of data entry, data backup, data movement. This questionnaire consists of some open-ended questions and this was filled by interviewing administrative officers of hospitals for checking how existing system of tertiary hospitals of Punjab store and process data. After accessing existing system, a framework is proposed with blockchain technology.

3.1 Research Gap

Traditional Electronic health record (EHR) model used in tertiary hospitals of Punjab exhaustively depends upon trusted server, server hold data from numerous transactions happened from service providers, regular patients' registration system, transmit system. Due to which data travelled from different transactions is not secure due to use of client server architecture. Common security issues in e healthcare in particular confidentiality, authorization, integrity, data theft immense problem in traditional healthcare system of Punjab. Study focuses on secure e healthcare system of tertiary hospitals of Punjab, where numerous transactions performed in seconds, to secure E- Healthcare system we have implemented blockchain technology with consensus mechanism.

In existing model every peer is connected to one trusted server, transactions performed in model but leading problem we identify after data analysis is transactions responsibility in existing model more than 45% transactions unconfirmed on network data of all unconfirmed transactions stolen by the attacker. Transactions those are completely performed in the system stored on database node, but problem is this as data entered to the transaction as well as stored in database, through which data is easily available and not secure.

Electronic Health Records are one-of-a-kind electronic documents that contain information about a patient's medical history, demographics, prescription drugs, laboratory tests, and computerized tomography, among other things [113]. Tertiary hospitals of Punjab store patient's records in database using online platforms all these records are stored using common client server architecture in database. With exchange data custodians, which are commonly

used for the interchange of health information across healthcare stakeholders, EHR systems have been criticized for centralizing control, malfunctions, and attack-points. Although adhering to protection, privacy, legal, and other regulatory constraints, EHRs have struggled in the face of multi-stakeholder and device requirements. Hospitals, rather than patients, have full control over electronic health records (EHRs), which makes obtaining medical advice from various hospitals more difficult. Patients must concentrate on the specifics of their own healthcare and regain control over their medical records.

The rapid advancement of blockchain technology, which includes medical records and patient-related data, promotes population healthcare. This technology gives patients access to electronic health records (EHRs) that are free of charge from care providers and treatment websites. Electronic health records (EHR) now a revolution in healthcare sector due to which patient's data is stored in database from different peer in the e-healthcare. There are numerous transactions performed in e healthcare in which data without any change state stored as user enter the personal information, prescriptions etc., directly stored in the database there is not any method used to store data in secure form. Security is depending upon the client-server architecture and on the basis of secure socket layer. Physicians are usually very worried that an unauthorized party might gain access to patient information contained in an electronic medical records system and abuse it, resulting in legal problems as a result of a breach of the security of the patients' records. Electronic records shared automatically with the help of web services and service providers those connected with govt. agencies, insurance sector, lab prescription and some other transactions related to e healthcare but vital issues in healthcare for securing data. These problems rise every sec that is big problem for securing data from unauthorized access, attacks, data breach. Cloud computing is commonly used in healthcare, but it comes with its own set of security problems. According to data, about 10% of cloud services used in healthcare are considered high risk, while 70% are considered medium risk. Since there have been cases of medical identity fraud, healthcare providers must protect access to all clinical applications. Hackers used patient information to gain access to the information and begin their path to more. Cyber criminals attempt to steal billing and insurance records details. Their aim is to obtain sensitive information such as security numbers, credit card information, and other financial information. Mobile health devices make it easier for physicians and patients to work together in a shared care system [114]. Although doctors used to enjoy viewing patient information and receiving clinical information through mobile apps, more and more people are gaining access to data, putting security at risk. In these challenges we find there is not any security framework applied to any one of the parameters in tertiary

hospitals of Punjab due to which data is encrypted when entered in the data base and data is stored in every transaction as fire, there is not any kind of change when data travelled over the system or from one to other sourced as transaction done on patients' edge or dr. edge. For example, if a patient's personal information is stored in data base that is in the form of simple text, whether it stored on local system or on host system. In that case it will become very important to provide security to e healthcare where billions of transections done in a minute, Data envelopment analysis is a technique for assessing operational efficiency in the context of logical and scale efficiency of an entity, as well as agreeing on a benchmark and working according to it, or setting a benchmark if there isn't one. The research of the study is incorporate to Design and implementation of security framework for e- healthcare using blockchain technology. Transactions completed edge to edge will be secured using blockchain. In which we will implement a consensus mechanism for secure transactions.

3.2. Research Objectives

1. **To collect and analyze E-healthcare data of tertiary hospitals of Punjab.**
2. **To model security framework for hospitals having E-Healthcare set up to record data.**
3. **To propose and implement consensus algorithm on E-healthcare data.**
4. **To compare the proposed framework with existing systems.**

3.3 Sampling Methodology

This research incorporates two distinct aspects one is to collect E-healthcare data from tertiary hospitals of Punjab for assessing existing E healthcare infrastructure and secondly propose framework using blockchain. Super specialty hospitals are considered from areas of Punjab and are classified into three sizes: small, medium, and large, based on the number of beds. Small size hospitals are between 40 and 70 beds, medium size hospitals are between 70 and 100 beds, and large size hospitals are over 100 beds. Both Inpatients and out patients getting treatment from these hospitals and their data is mostly stored in e healthcare data base. The hospitals were selected from a list of hospitals run by doctors who are members of the Indian Medical Association. From each of the study areas, government and private tertiary level hospitals handling inpatients/ outpatients were chosen for investigation.

3.3.1 Hospitals for study

The hospitals were selected from a list of hospitals run by doctors who are members of the Indian Medical Association. From each of the districts chosen for the research, government and private tertiary level hospitals with more than 40 beds were chosen. A total of 48 tertiary hospitals were chosen from the entire list. Quota sampling is used to choose hospitals. Quota sampling is done based on hospital size; different sized hospitals are needed for this research's objective, and three different sizes of tertiary hospitals are considered: small size is between 40 and 70, medium size is between 70 and 100, and large size is more than 100 based on number of beds. In this study, quota sampling was used because it is the most basic and common method of conducting research, and the number of beds was introduced as a sub-point of differentiation, Data was obtained from hospitals based on their scale (large, small, and medium) and the study outcomes achieved.

Because of its high potential to deliver more reliable and cost-effective patient care, healthcare data management has gotten a lot of attention in recent years. Inpatient's details are stored in e healthcare system in tertiary hospitals of Punjab, from the process of registration to their discharge each transaction is maintained on the database. As many transactions processed in e healthcare system, that's why for healthcare providers it is important fact to secure transactions of patients in electronic health records (EHR). To achieve this in healthcare providers for making data security on distinct peer on the network they set out various research to provide security in healthcare. It is far too critical to them to maintain a verifiable degree of client satisfaction. To do this, healthcare providers conduct different studies to determine patient satisfaction levels and develop strategies for better serving them. Choosing the best instrument and technique to involve patient satisfaction is, however, a significant test for healthcare support.

The survey was created to study on patients records from 48 hospitals, the survey was produced in two different languages: Punjabi and English. Since the study's target population was from Punjab, a Punjabi language survey was developed. Patients in Punjab's multi-quality 48 tertiary emergency hospitals, especially those with tertiary-level diseases and located in urban areas, are included in the report.

In tertiary hospitals of Punjab, out patient's facility is available through which patients go to hospital for treatment but not stay there for night that category of patient's transactions also recorded in the database. Out patient's details require security due to less transactions because once outpatients visit to hospital, it is not a scheduled visit for long term that's why due to less transaction it's important to provide security to electronic health record.
Consider the respondents' level of awareness; a total of 40 questions have been distributed to them. In order to comprehend the different behaviors of respondents, various measurement scales have also been considered. The report includes patients from Punjab's 48 high-quality tertiary emergency hospitals, especially those with tertiary-level diseases who live in urban areas.

3.3.2 Secondary data sources

The major online information sources incorporate sites of World Health Organization, Ministry of Health and Family Welfare (India), National Sample Survey Organization (India), Central Bureau of Health Intelligence (India), annual reports of Hospitals, Health Department (Punjab), Emerald, JSTOR, Science Direct, Nature, Taylor and Francis. Different diaries, papers, books and so on were likewise eluded for the present investigation. Aside from the online information sources, numerous organizations, for example, Punjab State Planning Board (Chandigarh), Parivar Kalyan Bhawan (Chandigarh), Department of Health and Family Welfare, Punjab Mini Secretariat (Chandigarh) and libraries of Punjab university Chandigarh had been visited every once in a while, to gather auxiliary information.

The imperative information has been gathered from the administrators of distinct hospitals, they are the dealing and responsible persons in the organization. Scales have been developed for the processing of critical data. Based on an existing survey of writing, scales have been created. The primary activity is to identify the responsible persons for communication related to e healthcare system of the hospitals and then concise to their own systems that is responsible for store healthcare data. Based on existing studies, a pool of medical hospital administration-related factors was developed in the first phase.

The collected data were analyzed using different statistical methods in order to fulfil the objectives. It's worth noting that the study was carried out using SPSS (Version 21).

3.3.3 Finding Parameters from the data

Table 3.1 Detail of parameters

Name of parameter	Type
Age	Number
City	Text
Gender	Text
Purpose	Text
Lab test prescribed	Text
Inpatient / Outpatient	Text
No. of days	Number

In e healthcare, electronic health records (EHR) hold countless parameters which are related to personal and professional both. As patient complete their registration process than data transfer to the hospital data base after verification again it pathway to the doctors through which doctors access the information an again perform operations on the data, so in electronic health records (EHR) data stored electrically according the designed parameters. After discussion with the administration staff of 48 hospitals of Punjab. List of parameters are available in the table 3.1 through which hospitals store patient's information. After deep study on parameters in e healthcare, it is crystal clear that without parameters data never be stored. Data is collected from 48 tertiary hospitals of Punjab, 1000 rows data target from each hospital. As discussed with the administration staff of hospital they refused to give data of personal attributes of patients.

In the database age parameter is an important parameter, which has many characteristics in the study because it defined distinct persons age those are visit in the hospital and accordingly, we can easily find the patients according to diseases with respect to their age. Age is stored in the

form of numbers in database. City attribute is used to store patient's city from which they belong due to this attribute, segregation of data can be applied city wise and there are many techniques according to which study demonstrate the collection of records from different cities. People's interactions with and access to healthcare are affected by their gender. The organization and delivery of health services can either restrict or allow a person's access to healthcare knowledge, support, and services, as well as the outcomes of those experiences. Health care should be available, affordable, and appropriate to all people, and it should be delivered with consistency, equality, and integrity. In general, the biological distinctions between males and females, such as genitalia and genetic differences, are referred to as "sex." Anatomical and physiological variations exist between male and female sexes. The word "sex" is often used to refer to biological distinctions. In electronic healthcare records, at the time of registrations gender are defined but patient's biological selection over their gender is required. The electronic healthcare system has collection of different parameters that are responsible to store different types of data in the database. Purpose is the field used to store data that describe the visit purpose of patients in the hospital. Transaction store visit purpose of patients permanently in the data base, framework assign doctor to each patient according to their purpose of visit. If a patient is register online in any tertiary hospital in Punjab than after communicate with the administration staff of the hospitals, it is found that when patients purpose is selected than, according to selected purpose doctor's detail are available from database and then pick out for the patient. For example- If any patients are register for purpose neurosurgeon at that time available doctors from the system at the time of their registration in that hospital are available, only from the neurosurgeon department.

The laboratory is both the most and least used resource in the healthcare system. The first is that laboratories are used as factories or mines by almost all other medical fields, and the second is that laboratory personnel lack clinical expertise. Healthcare is working to become more modern, effective, and patient-centered. Laboratory is not a service provided by the doctors, execution of this factor is depending upon the purpose patient visit and identification of disease. Lab test prescribed is text type attribute in which super specialty hospitals of Punjab stores data related to lab test prescribed or not in the patient's treatment series. Inpatient and outpatient is next field in database, this field store data related to patients those stay night in hospital and also for all other patients visit hospital and return back to their homes after checkup. Attribute number of days, record inpatients record in the hospital, in the form of numbers display exact figures related to the patients stayed in the hospital.

3.4 Research Framework

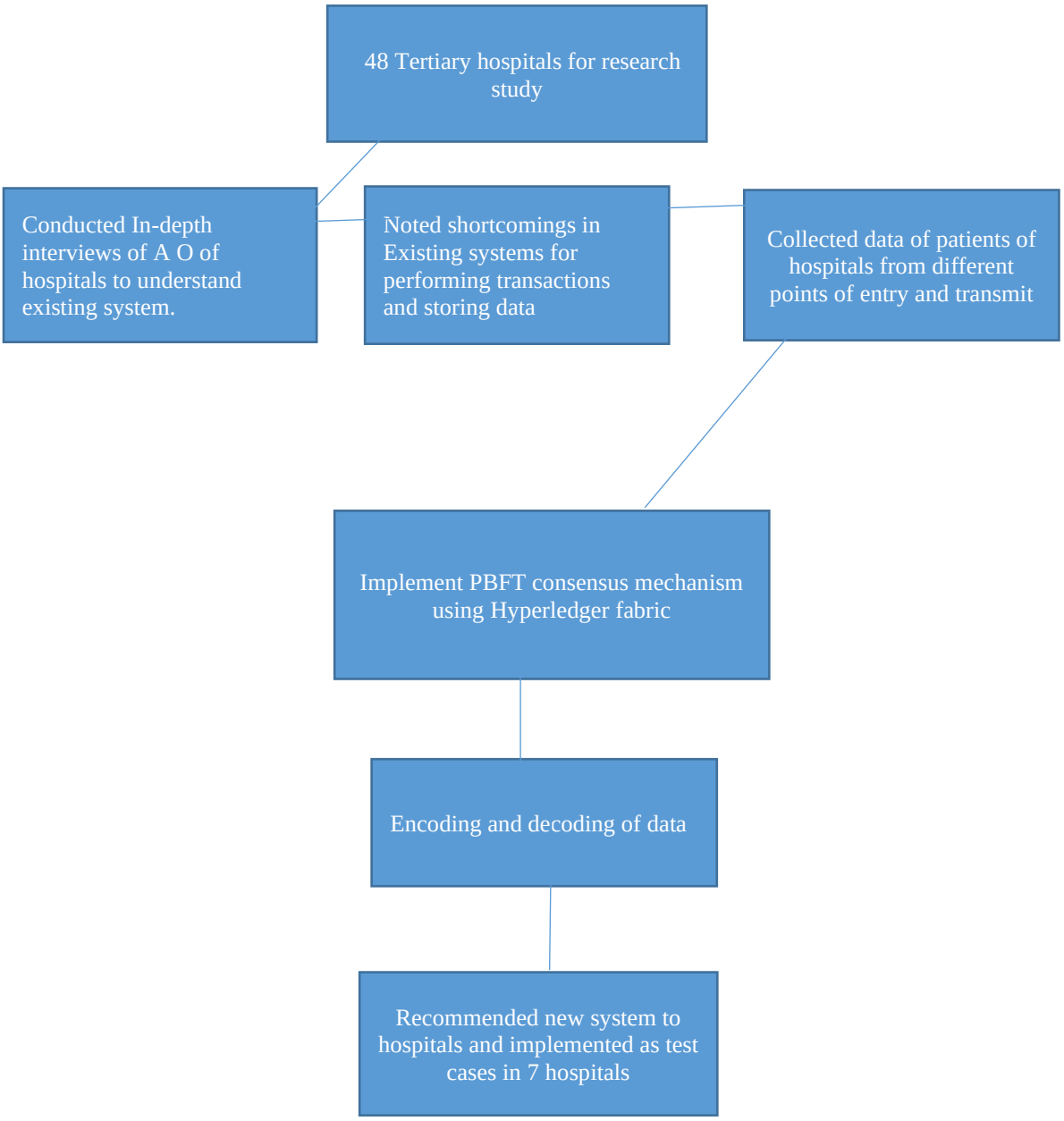


Fig 3.1: Research framework

This study is divided into several phases, each with a step-by-step process for data collection and analysis. It is a multistage process in which some time stages must be followed in parallel while others must be followed in sequential order, as follows:

Tertiary hospital of Punjab are super specialty hospitals and trauma care centers those are mandate part of the e-healthcare. Each and every transaction is recorded electronically in the data base. Due to this clause we decide to target 48 tertiary hospitals of Punjab. This phase involved research idea for collection of 1000 rows data from each selected tertiary hospitals of Punjab. After selection of hospitals and plan data set collection next phase of study is conduct in-depth interviews with administration officers of hospitals, because how transactions of hospital data performed in e-healthcare system. Transactions happened from different end in which both patient and doctor are responsible. Set of questionnaires designed and share with administration officers, through which their responses had been recorded. From 48 administration officers in interview discussion held on distinct level of challenges in healthcare that are data entry, data security, data movement and data disposal. In data entering phase questions related to fresh entries in database from different sources, technologies, platforms and methodology used to get data from patients had been discussed. After noted respondent's response, next discussion held on data security in which process followed by the tertiary hospitals of Punjab to secure data and data transactions performed dynamically had been discussed using questionnaires. Next phase of questionnaire related to data movement. Data movement is an important process held in system through which data travelled from peer to peer using network. Ending phase in questionnaire is discussion with administration officer of hospital according to their techniques used for the data movement in their electronic healthcare system (EHS). Responses had been recorded from every administration officer from 48 hospitals.

After gathering information from respondent's study found shortcoming in existing system for perform transactions and storing data. It had been analyzing for healthcare system of Punjab from data collected and discussion with administration officers that, in Punjab client server architecture is used for making transactions, data from one node to other node is directly send without any encryption, due to which each record is simply travelled with the clear information that is easily available for all of the sources in the data base even though it is accessed by the others in clear format. As mentioned for the transactions in the electronic health records (EHR), Too much sensitive information is travelled over network in unsecured manner. Data is updating while transactions numerous times, from different end but in execution cycle of transaction, data is not secure because as user become part of the transaction their sensitive information can be theft and un authorized access may happen. No transparency method for

data access is provided, a complex system is used for the access information without any take care of security.

Collected data of patients from tertiary hospitals of Punjab from both entry and transmit. From registration process to transmit, 48000 rows from 48 tertiary hospitals of Punjab have been collected. There are seven attributes in data set that are Age, City, Gender, Purpose, Lab test prescribed, Inpatient / Outpatient, No. of days. Collected data is stored after numerous transactions. From entry and transmit data is collected and arranged in one file after arrangement of data. Data passed through numerous techniques like missing values checking, check rage, type of data in file, data completeness checks has been implemented.

For apply security in e healthcare using blockchain technology, proof of work algorithm is applied on collected data for providing security in e healthcare. Proof of work is consensus algorithm in blockchain technology which is used to provide security in blockchain. The consensus process is the foundation of blockchain since it decides if a new block is legitimate and who keeps track of it. As a result, it has an effect on the overall system's security and reliability. The initial consensus algorithm in a blockchain network is Proof of Work (PoW). The algorithm confirms the transaction and adds another block to the chain. Minors (a group of people) compete against each other to complete the network transaction in this algorithm. Using Proof of Work (PoW) process of finish against each other is called mining.In e healthcare many complex transactions performed, proof of work (PoW) is responsible for unconfirmed transactions that are mined using blockchain and the data in the records after each work encoded and decoded for providing security in electronic health records (EHR).

In next phase of study extend to recommendation of new system to tertiary hospitals of Punjab as long as implement designed framework for secure e healthcare system. New system capable to secure data on E-healthcare system using blockchain technology as compare to existing systems. Due to this after comparing new system with existing system that are already used in Punjab for secure E-healthcare data in tertiary hospitals of Punjab, we recommend our proposed system to hospitals. Our proposed framework using blockchain technology, Hyperledger fabric and PBFT consensus mechanism. For testing purpose in 7 hospitals, our system is implemented in Punjab to secure e healthcare system using blockchain technology. Using our system patient’s details entered to the system using blockchain network and blockchain is responsible for secure transactions in e healthcare system.

3.5 Blockchain in healthcare

Data in the healthcare sector requires a high level of security and confidentiality. The term "privacy" applies to individuals who have the legal authority, authorize or reveal personal details to others. This necessitates cooperation among healthcare providers and regulators, as well as the development of agreed-upon policies and procedures. The first step in deciding who should have access to confidential patient information is to consider privacy [115]. Owing to additional regulatory provisions to protect patients' medical records, the healthcare sector has special protection and privacy requirements. In the Internet era, as cloud storage and the adoption of mobile health devices increase the exchange of records and data, the possibility of malicious attacks and the compromise of private information increases. As the scale of healthcare data expands, security measures to protect the data are needed. As a result, the United States and other countries have put in place security standards and legislation to protect their medical records.

EHR innovation is the focal point of progress in medical services advancement. Electronic healthcare record will develop to be a suitable escort for medical clinics. EHR innovation is the focal point of progress in medical services advancement. Electronic healthcare record will develop to be a suitable escort for medical clinics. For execution of electronic healthcare record brief incitement will help occupy up an adequate fragment of the innovation ventures. Endurance in serious market will be difficult to remain. Electronic health records consist of patients, doctor’s information that consists of different transactions, in which huge amount of data is generated. Degree and more extensive range of EHR, including the trading of patient data, solidly to improve the quality consideration, proficiency and profitability, and facilitate a superior interoperability of patient data across the hospitals. Brought together completely acknowledged EHRs record having which incorporates the patient's healthcare data: which is outright, defended and exact. It will improve the arrival of venture and thus expanded appropriation pace of EHR. Generally speaking, motivation of EHR is, the capacity to rapidly give care and to use sound judgment. With EHR selection all advantages will achieve all partners in the country, including, doctor, sellers, patients and society all in all. System has sensitive information about doctors, patients and society requisite to secure transactions performed in EHR. Because data travelled in number of nodes, from one block to other block

data travelled and security constrains are required to apply, that’s why a secure framework is provide to e healthcare system that secure records of EHR.

Blockchain is a revolution for providing security in e healthcare. Using blockchain we can secure transactions in electronic health records (EHR). Blockchain technology is based on a distributed network that stores data in tamper-proof formats. Existing transactions cannot be changed because blockchain transactions can only be revised or introduced by generating new hash values [115]. Characteristics that distinguish the blockchain from others.

3.5.1 Distributed ledger: The transactions are appended on the network in a distributed system, which allows for system recovery by removing a single point of failure or centralized entity.

3.5.2 Consensus Mechanism: Transactions are only changed when all of the network's confirmed users agree to the transaction's terms.

3.5.3 Provenance: On the blockchain network, you can see the entire history of your data or asset.

3.5.4 Immutability: Records on the network can't be changed or tampered with, so all data is safe and stable.

3.5.5 Finality: A transaction on a blockchain cannot be changed or reversed once it has been committed.

3.5.6 Smart contract: The codes are generated on a blockchain network, and they are executed by the device and nodes in response to a trigger case. As a result, the codes are executed automatically within the time frame.

The introduction of blockchain technology has the ability to minimize transparency and security problems, such as third-party confidence, at any point of a transaction; this ensures that all intermediaries or third parties are removed.

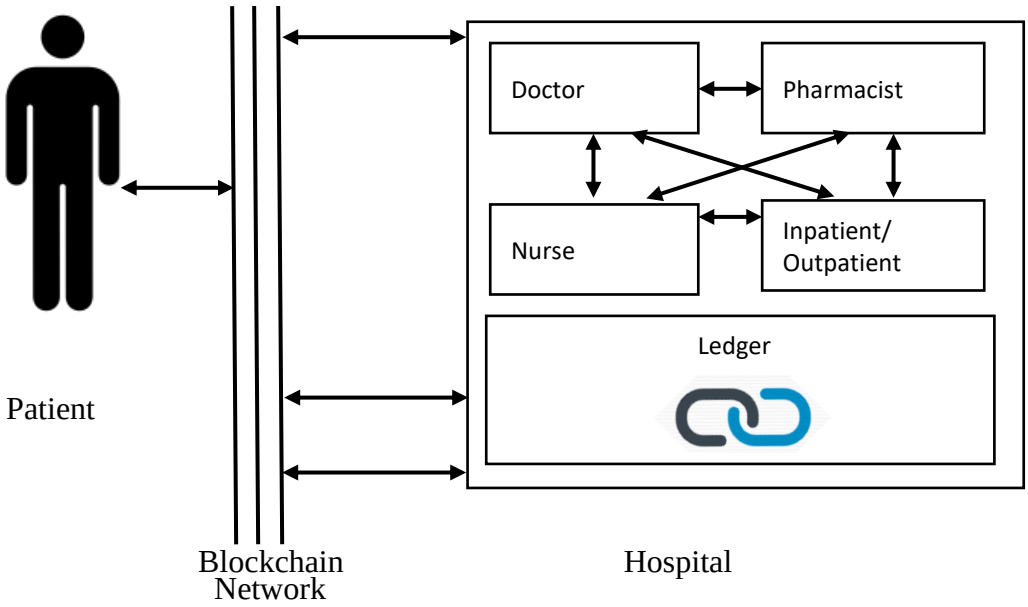


Fig 3.2 Blockchain in E Healthcare

3.6 Blockchain Transactions Design

Blockchain is a distributed ledger technology that uses a sophisticated working sequence to check and validate transactions across a network, resulting in an immutable, reliable, and consensus-based ledger. Several stages are required to accomplish a blockchain transaction. In the initial phase, the network node requests the transaction. The transaction is then broadcast to all network peer nodes, which includes all PC nodes. The SHA-256 algorithm is then used by the blockchain network to generate a unique hash. After that, all hashes are connected via a previous hash, resulting in an unbreakable network of transactions. If anyone wants to append a transaction, the network node or a smart contract will verify it, resulting in consensus. This immutable ledger, therefore, cannot be modified [117, 118], it can only be appended to a block transaction. This method results in a decentralized system that is both stable and dependable. It verifies the user's authenticity using an algorithm. Crypto currencies, contracts, patient healthcare records, and clinical data are all examples of verified transactions. After a transaction is authenticated, it is added to the ledger and a new block is created in the network. An Index, Time stamp, Info, Previous hash, and Current block hash are all part of the block's structure. The blockchain is then appended with a new block, making it stable and impenetrable to alteration or modification. The transaction is completed or committed to the network in the final phase.

3.7 Consensus mechanism in Blockchain

A blockchain consensus is a set of rules that must be adhered to in order for the blockchain to continue to function. Consensus is utilized in blockchain to obtain an agreement on adding fresh data value to distributed servers or network nodes. The basic purpose of consensus in a blockchain is to achieve agreement among nodes in a distributed network, therefore it's crucial.

A blockchain is made up of several data blocks that are distributed throughout a network. In a decentralized network, a node is a server that has a copy of the blockchain. Each node on the network has the same copy of the blockchain, and they all use the same consensus rules to validate and create new blocks. The blockchain contains data from a huge number of transactions in each block.

Without consensus, blockchain is nothing more than a storage mechanism for encrypted and unencrypted data. Consensus enables it to be decentralized because all nodes in the network obey the same laws, ensuring uniformity for all blockchain copies. As a consequence, any improvement made in one blockchain is checked and adopted by another in the network.

Blockchain has a distributed structure, which ensures that every node in the network has a copy of the same blockchain, making it permanent. But, in order to exchange the same type of information, all nodes must agree. As POW adds a new block, all of the nodes in the network try to solve complicated cryptographic puzzles, and the first node to solve it adds the new block, while the other nodes update their blockchain to reflect the change.

This is the major aspect that a blockchain never work from consensus mechanism, when transactions rapidly performing in the system than Consensus algorithm allows all nodes in the network to reach a mutual agreement, that is why it is so essential in the blockchain technology.

3.8 Proof of Work (POW)

Each of the consensus algorithms is Evidence of Work. A node must publicly prove that it did a certain amount of work to validate a transaction, as the name implies. Node must demonstrate

the validity of its work by solving a difficult cryptographic puzzle. Supreme terms of Proof of Work (PoW) are: -

3.8.1 Block*:* A block consists of a set of transactions, a nonce, a timestamp, the preceding block's hash, the puzzle response (Nonce), and an index value. Each block in the blockchain is linked to the previous block.

3.8.2 Miners*:* POW is carried out on the bitcoin blockchain by miners, who keep the blockchain running by supplying a large amount of computational power in order to solve a cryptographic puzzle. They are rewarded for solving the puzzle by making a block. Miners compete with one another to create a genuine block of transactions. Miners aggregate all pending transactions from the decentralized network, then solve a cryptographic problem by guessing a random number (nonce). Miners generate a block after successfully solving the problem, which they then push into the network for other nodes to verify, so that after verification, other nodes can connect the block to their own copy of blockchain.

3.8.3 Nonce*:* To discover the value of nonce, miners must solve a cryptographic challenge. A nonce is a unique number that can be used just once. It's usually a random number derived from a set of outcomes. A nonce is a value that is contained in each block of the blockchain. This nonce is equivalent to sprinkling a pinch of salt over the contents of a block. If nonce is added, the hash output of the block's contents will move.

3.8.4 Hash*:* Hashing is a cryptographic technique that transforms input data into output data of a predetermined scale. The SHA-256 algorithm is used for Bitcoin. SHA-256 produces a number with a fixed length. The entire output would change if the input was changed slightly, but the output would still be the same length.

In POW blockchain, to build the next block, all nodes must validate transactions, but only the first node that successfully computes it can add the new block. The other nodes in the network will stop trying to construct it as soon as they obtain it and move on to the next block. Producing proof of work is expensive and time-consuming, but it is simple for others to check. No one knows the hash of the last registered block in nonce. The miner must locate it, which is the cryptographic challenge. The miner must try each number one by one. The cryptographic

puzzle is asymmetric, meaning that it is difficult for miners to solve but simple for nodes to check. Each block added to the blockchain must adhere to consensus rules, and any block that does not do so will be rejected by network nodes. Proof of Work is used in Bitcoin to ensure that the miner has the right copy of the blockchain and that all transactions are checked and in line with all other nodes in the network. When a miner completes a proof of work puzzle, the results are released to the network for verification, including the previous block's address, the list of transactions in the block, and the nonce. The network's other nodes automatically verify if the results are correct. If the results are right, the other nodes add the block to their blockchain copies [121].

Adding leading zeroes increases the complexity of a cryptographic puzzle. Since a single change in the string of nonce changes the output hash value entirely, adding leading zeroes increases the puzzle's difficulty. The Blockchain network determines the level of difficulty. As you would assume, the more difficult it is to assess the nonce, the higher the difficulty setting. Nonce cannot be calculated using a formula. It's merely a collection of hits and misses. The miners' "job" is evaluating nonce to obtain a hash value for the block data, and the right performance of the puzzle is the "proof."

3.9 Hyperledger fabric

Hyperledger Fabric, an open-source project from the Linux Foundation, is the modular blockchain framework and de facto standard for corporate blockchain applications. Plug-and-play components are used to handle a wide range of use cases in the open, modular design, which is intended as a platform for developing enterprise-grade applications and industry solutions [122].

The Hyperledger blockchain initiative was established in December 2015 by the Linux Foundation (the same organization that created the Linux Operating System). This project was created to serve as a hub for the development of fully accessible blockchain technology and distributed ledgers.

Many companies want to share data in a distributed database, yet no single owner can be trusted by everyone. This is a problem that blockchain solves. Blockchain technology allows for

secure, transparent direct transactions, creating confidence in the efficiency of peer-to-peer networks. Businesses' adoption of this technology involves a fundamental transformation in their business practices. It's a means to digitalize a variety of procedures and industries. Enterprise blockchain, on the other hand, is a team sport, as the Hyperledger community has demonstrated. The technologies are building blocks for core, cross-industry systems that will grow in size, complexity, efficacy, and value as time goes on. Because Hyperledger technologies are open-source code bases established with collaborative design and governance, businesses see them as a reliable framework for building blockchain applications. In just a few years, the first wave of enterprises to adopt Hyperledger technologies progressed from early-stage testing to proofs of concept to production systems. These implementations demonstrated that, when correctly designed and implemented, blockchain may deliver significant speed, security, and transparency benefits.

Now it's a race to put this technology to use. Concerns about public health, climate change, social justice, misinformation, privacy, and other concerns are driving the need for multiparty systems that promote trust, efficiency, and authenticity. The use of enterprise blockchain technologies is rising as a result of all of this.

Hyperledger technologies are already transforming a number of market spaces. As shown in the following table 3.2, these include supply chains, trade finance, and healthcare.

Table 3.2 Hyperledger in Action [122]

Market	SUPPLY CHAINS	TRADE FINANCE	HEALTHCARE
KEY HYPERLEDGER PROJECTS	Hyperledger Fabric Hyperledger Sawtooth Hyperledger Grid	Hyperledger Fabric Hyperledger Indy	Hyperledger Fabric Hyperledger Indy Hyperledger Aries
CHALLENGE	Supply chains are the driving force for industries around the world. For products to reach their markets, they flow from farms, mines, forests, and factories through a network of manufacturers, suppliers, shippers, and distributors. Often the journey starts with raw materials or components that are assembled along the route. Multiple parties are each tasked with a segment of a product's journey but all have a stake in its successful delivery.	Auditability and efficiency are vital in the financial market, especially for enabling backend transactions to keep commerce and trade flowing. Institutions are looking to digitize lending and other services to lower operational costs, reduce fraud, cut settlement times, support new asset classes, and streamline cross-border payments.	Technology is a cornerstone of today's complex healthcare market. Despite the increasingly digital infrastructure designed to link providers, payers, patients, and public health officials, gaps remain in how critical data is captured, secured, and shared.
HYPERLEDGER'S IMPACT	Hyperledger technologies are being used to create a shared, secure audit trails in a range of supply chain deployments and networks. These solutions make it possible to track and trace products and components in near real-time as they make their way from party to party in the supply chain.	Hyperledger technologies are playing an increasing role in digital trade, supporting new cross-industry networks that reduce reliance on central authorities to authenticate transactions.	Hyperledger technologies have been put to work by the government agencies, insurance groups, hospitals, and pharmaceutical companies in many ways.

CHAPTER 4

Data analysis and interpretation

4.1 Research Analysis

1. **To collect and analyze E-healthcare data of tertiary hospitals of Punjab.**
2. **To model security framework for hospitals having E-Healthcare set up to record data.**
3. **To propose and implement consensus algorithm on E-healthcare data.**
4. **To compare the proposed framework with existing systems.**

The emphasis in this section of the thesis is on data analysis for healthcare system assessment and implementation and proposing of security framework to protect e healthcare data. Analysis of healthcare system assessment is based on a data collected from questionnaire after receiving replies from administration employees at 48 tertiary hospitals in Punjab. Before proposing and implementing security mechanism in hospitals it is very much imperative to access healthcare system which is already existing for which we have designed one questionnaire consisting 40 questions which cover different aspects of healthcare system assessment related to data entry, data backup, registration process, security infrastructure, data sharing ,third party data control .After collecting data and data analysis it had been observed that hospital are having process for data entry and token n generation only but if we talk about security ,Hospitals does not have any proper sound mechanism to protect data and if some of them have they are using traditional client server model to control data which is not flexible and scalable enough to imbibe unexpected number of patients data if arrived and administrators does not have any control over the data .

The questionnaire is divided into four major sections, each of which contains information about the current system for data base transactions in the electronic healthcare system. The following are the broad categories under which we create questionnaires and collect responses.

- Data entry
- Data Security
- Data movement
- Data disposal

Questions was surveyed from administrator officers from various tertiary hospitals, when the question was asked about "Are you using an e-healthcare system?". Responses from administrators have been recorded and are displayed using figures, with Fig 4.1 representing responses in an area chart that tells us all of the 48 selected hospitals for our study responded that they are using the e-healthcare system.

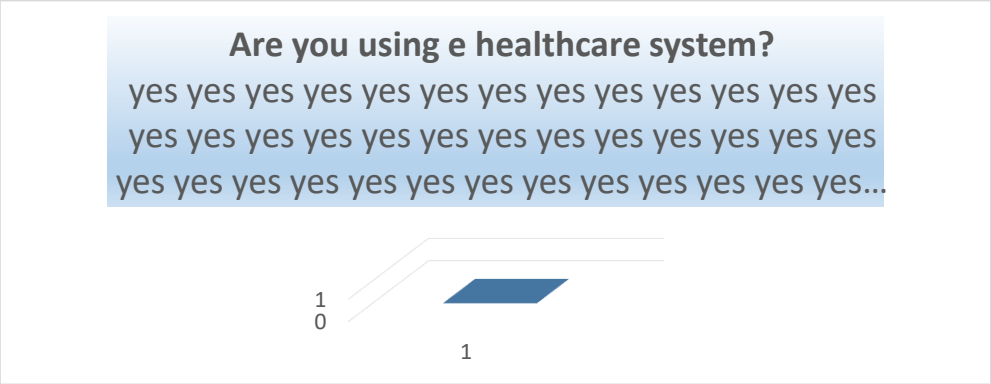


Fig 4.1: Representation of question 1 – Are you using e healthcare system?

When the questions related to e healthcare system used in tertiary hospitals asked, response collected yes from all the hospital administrators. Hospitals used online registration, medical history of patients. Response received yes from all the hospitals. In Fig 4.2, the bottom line of the neutral vertical axis 0, which describes the Point 1 value on the axis for response yes, represents that series in the chart for response yes to the question is represented on the bottom line of the chart for response yes to the question.

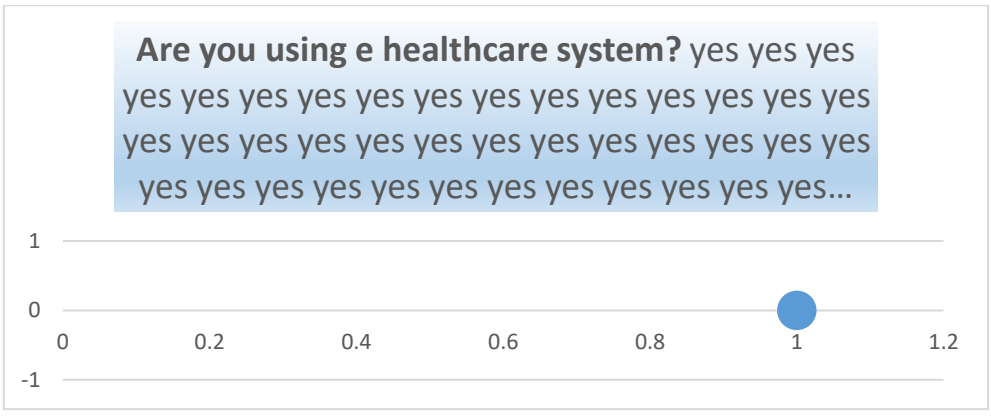


Fig 4.2: Representation of question 1 – Are you using e healthcare system?

In Fig 4.2 plot area from 0 axis to the positive position from the chart till positions from 0, 0.2, 0.4, 0.6, 0.8, 1, and 1.2 responses are yes that's why these are visible as a bubble on spot 1 in the figure. Vertical axis and plot response is yes for the question "Are you using E healthcare system?"

Those who replied yes, question 2 was asked from them 'What is major purpose of Using E-Healthcare system?' and options given are Data entry, Data Access to patients, Data Access for Administration, Data storage, Easing process flow, Data analysis. In the response data entry has highest percentage that is 75%, percentage of data access to patients is 10%, percentage of data access to patients is 0%, data storage is 10%, Easing process flow is 0% and data analysis is 5%. Responses of next cross-question has been collected from the question that is "**Do you use online application for patient's registration process?**"

After receiving all of the responses, a chart is prepared to analyze them. We Received responses from 48 Punjabi tertiary hospitals and "yes" response from 85.4 % (41 hospitals), which means we get responses for the question from online applications used for patient registration, including walk-in entry details, and there are 14.5% (7 hospitals) those who replied "no" among chosen hospitals that respond for the question. Fig 4.3 bars on the chart depict data as a series of total points on the vertical (Value) axis. The majority of replies to the question Do you utilize an online or mobile application for patient registration are affirmative. The majority of hospitals employ an online registration process to keep track of their patients for future reference.

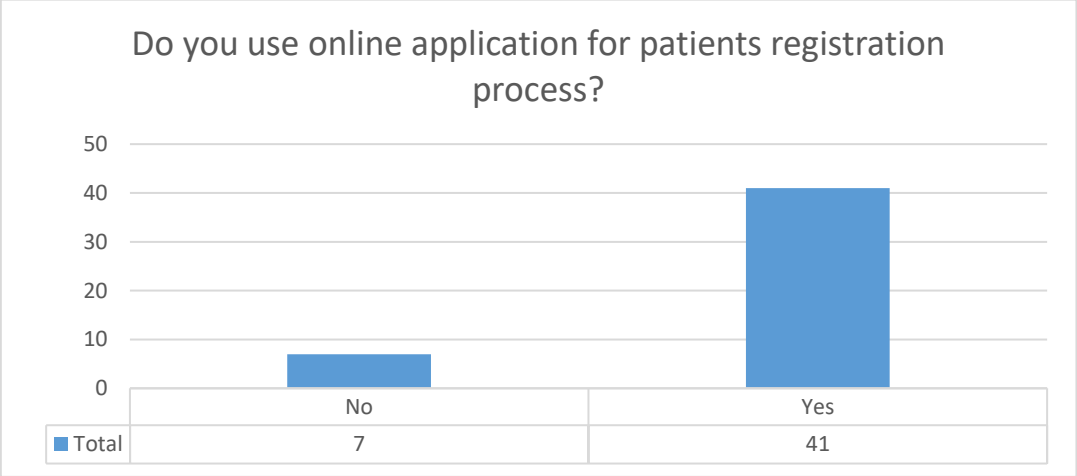


Fig 4.3: Representation of question 3 – Do you use online application for patient's registration process?

Fig 4.4 also represents that the the majority of responses notch to the tip of the data with the 41 responses, which is the highest value in the data representation, indicating yes response on the horizontal (Category) axis w.r.t. vertical axis. According to the responses gathered, the second response implies that there is no minimum point on the floor.

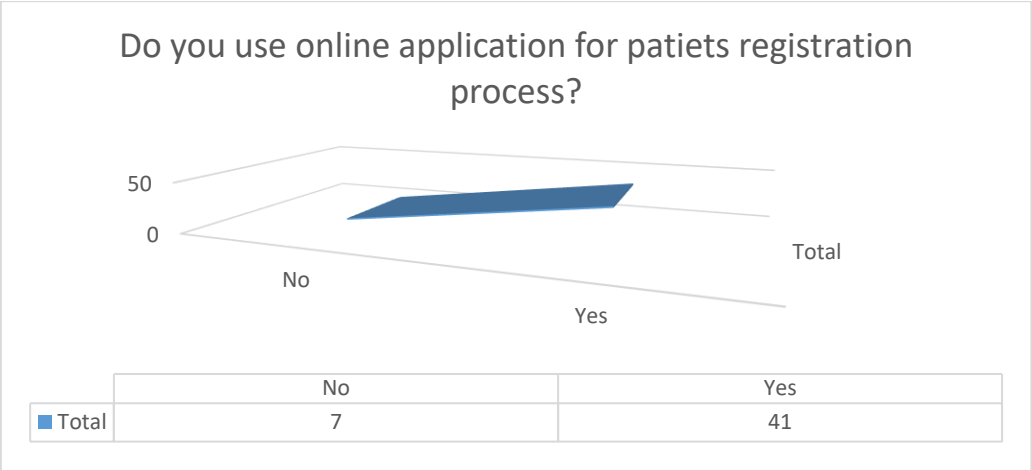


Fig 4.4: Representation of question 3 – Do you use online application for patient's registration process?

When question is being asked for whether you are using Mobile application for registration as in previous question almost 85 % replied that they use online system, now in case mobile application 39.5 % replied about use of specific mobile application through which patient can register and see its medication history rest they replied that there system is capable of registration from mobile but no specific mobile application is available In the E-healthcare system, walk-in registration is possible as well as emergency registration. Both processes are distinct in nature, with one being a walk-in registration process on the counter and the other being an emergency registration process where there is no such entry procedure but a transaction procedure for the entry block.

When question is being asked from patients related to "Can patient initiate registration process before visiting Hospital?". It is very important if registration process is available before visiting hospitals, some hospitals have advance appointment system with doctors but 70.8% (34 Hospitals) of them replied they have only advance registration system and 29.1(14 Hospitals) replied they have only walk in entry no advance registration is available even online. Those

Hospitals those are even providing online services but still in some of them after online initiation walk in registration is mandatory

When Question related to hospital administration is asked about issuing E token, that is ‘Does E token is provided to patients after registration?’. E token is a unique number provided to patients after online registration, according to this process response has been recorded and illustrate in figure 4.5. There are 45.8% (22) response for yes and 54.16% (26) responses for no demonstrated in following fig 4.5

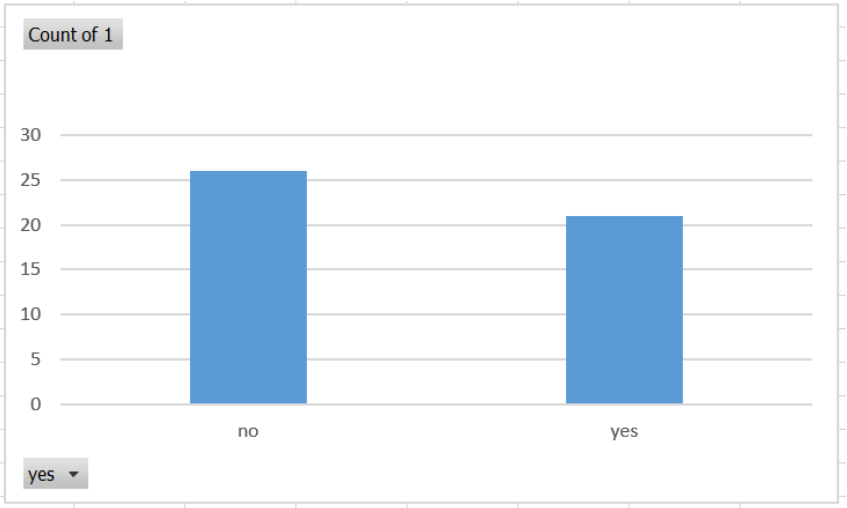


Fig 4.5: Representation of question 6 - Does E token is provided to patients after registration?

Next question request to collect information about the reusability of E-tokens. Responses demonstrated in figure 4.6. 37.5 % (18) hospitals not reused the e token after one time visit. Then next question was related to collect information about the reusability of E- Token in number of days. Response of this question collected from those hospitals who provide response yes in question 7. Fig 4.6 shows the response in the form of days. From 48 tertiary hospitals 37.5% of hospitals gives response yes for reused E-token again. There are 6 hospitals that reused e-token for 15 days, 6 hospitals that reused e-token for 7 days and 6 hospitals that reused e token for 30 days.

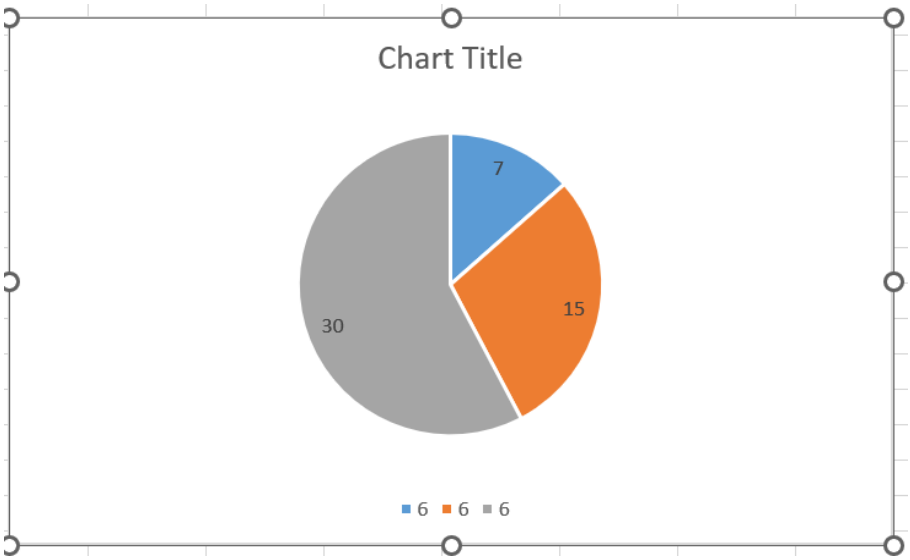


Fig. 4.6 Representation of question 8 - If E-token Reused than how many days it is valid?

Aadhaar is a 12-digit unique identification number issued to Indian citizens by the Central government. It is issued and managed by the Unique Identification Authority of India (UIDAI). Question 9 has requested to collect the responses for registration of patient linked with Aadhar card number. All collected responses illustrate in fig 4.7 shows that 52.0.9% (25) of hospitals responded no and 47.9% (23) hospitals responded yes.

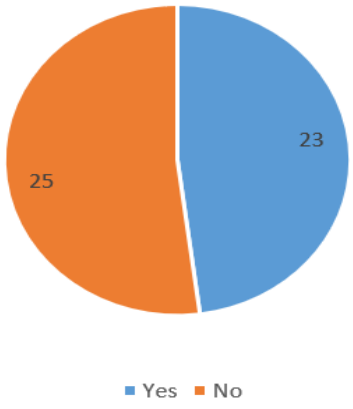


Fig. 4.7 Representation of question 9 - Is Registration of patients linked With Aadhaar card number?

Walk in entries in hospitals play an important role because this is the direct information passed to the system and stored in database. Next question request is to collect the responses

for question related to walk in entries for e-healthcare system allowed or not. Response from all 48 hospitals is yes which is illustrated in fig 4.8.

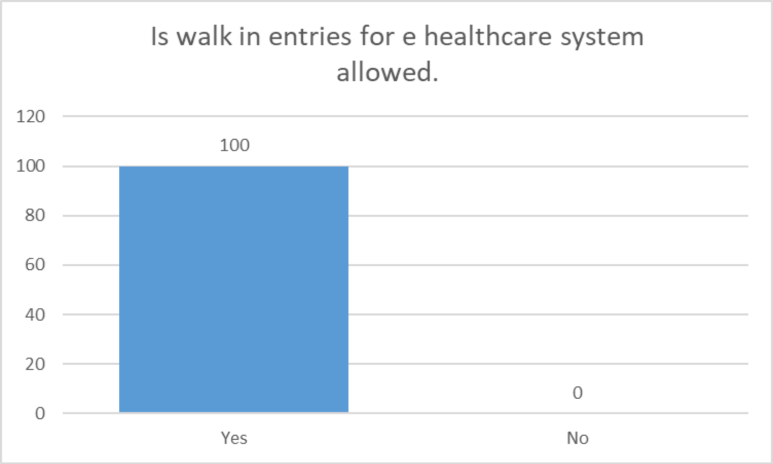


Fig. 4.8 Representation of question 10 - Is walk in entries for e healthcare system allowed.

Verification is a crucial term; a patient's registration process is only completed after their information has been validated. After consulting with hospital administrators, each hospital verifies patients' data with the Unique Identification Authority of India (UIDAI). Responses displayed in fig 4.9

Fig 4.9: Representation of question 11 – Does verification process is followed for verifying patients' information.

Fig 4.9 depicts information about the responses and a sequence of data labels using a verification method, with the answer yes displayed on the chart area in relation to the vertical axis. The way the question is described with the linked entries is represented by the legend entry. Most of hospitals as asked were using Aadhaar based verification but some hospitals not made it mandatory to verify with Aadhaar and other proof also they are accepting for patient verification process.

E-healthcare is a massive system that stores patient transactions. Electronic health records (EHR) have a variety of features that are used to store data in the system. E healthcare data is vairy.

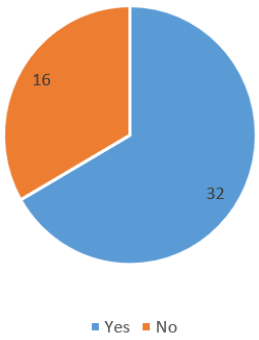


Fig 4.10: Representation of question 12 – Attributes used to store data of patients?

The quantity of attributes collected in response to the question "Attributes utilized to store data of patients" will be represented in fig 4.10. On the chart area, data is represented as points on the horizontal axis value and the vertical axis value. E healthcare data is used for various purpose for controlling organization to analyzing and predicting operational procedures for future. attributes that are mostly used to store data are related to name of patient, area from where patient belongs, doctor want to visit, problem of patients, any medication history, age.

The primary factors that are responsible for storing connected data entries are data base attributes. There are two distinct techniques to storing data in an electronic healthcare system. To maintain healthcare records, hospitals use a variety of qualities, thus after receiving responses from hospital administrators, we depict data after analyzing it in the charts provided.

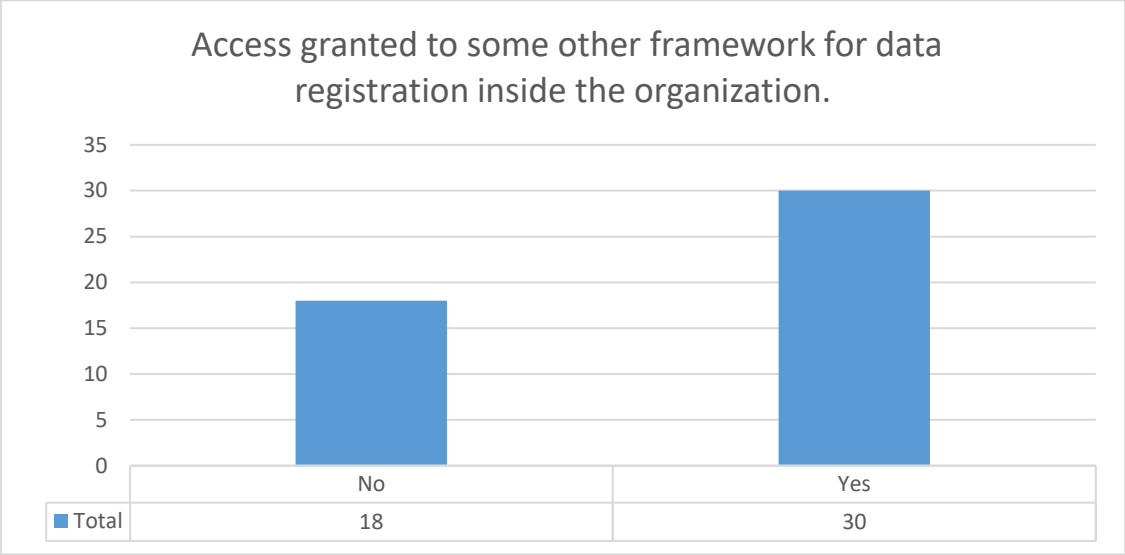


Fig 4.11 Representation of question 13 – Access granted to some other framework for data registration inside the organization.

Fig 4.11 displays data as a bar chart in the chart area, with the horizontal and vertical axes representing data for distinct records of yes and no having 30 and 18 values, respectively, indicating that the count of access granted to another framework for data registration within the organization is visible based on the responses.

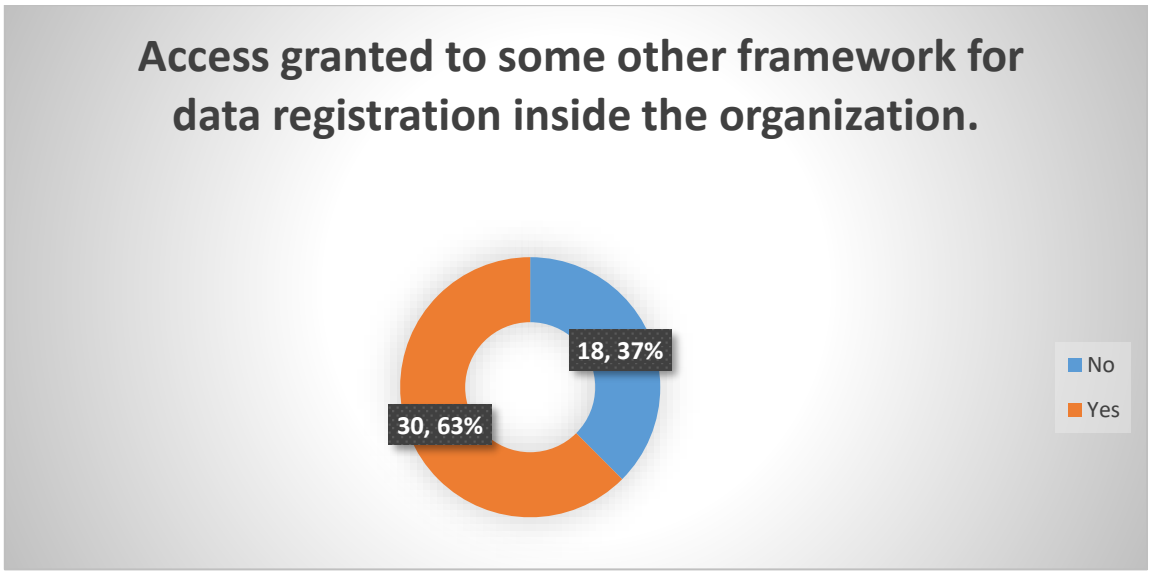


Fig 4.12: Representation of question 13 – Access granted to some other framework for data registration inside the organization.

There are two different data series for yes and no responses in fig 4.12 data display in the shape of a pie chart. Yes receives 30% of the series points, while no receives 18%. Following an investigation of the data, it was discovered that many hospitals from the selected 48 hospitals provide access to other frameworks inside the business, while just a handful do not provide access to other frameworks for the registration process.

Many external systems are either directly or indirectly connected to the e-healthcare system. We give our results in the form of charts after collecting data for this question.

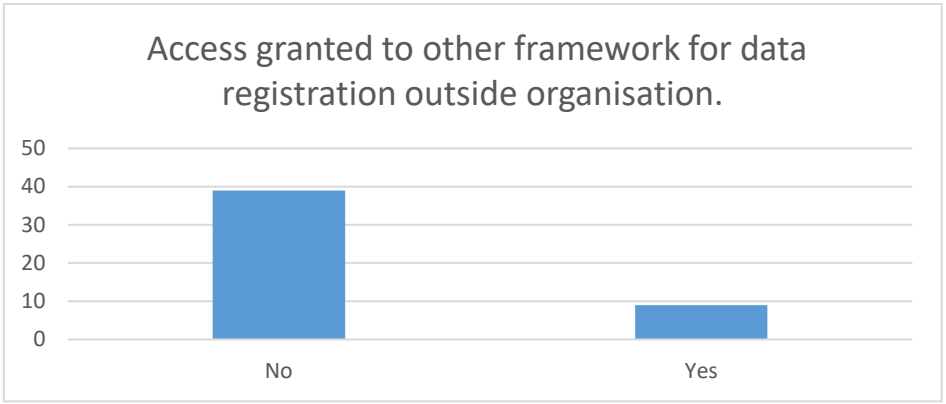


Fig 4.13 Representation of question 14 - Access granted to other framework for data registration outside organization.

Fig 4.13 depicts data in a bar chart, with two distinct series representing data in yes and no collections from hospitals. There were 39 no responses and 9 yes responses.

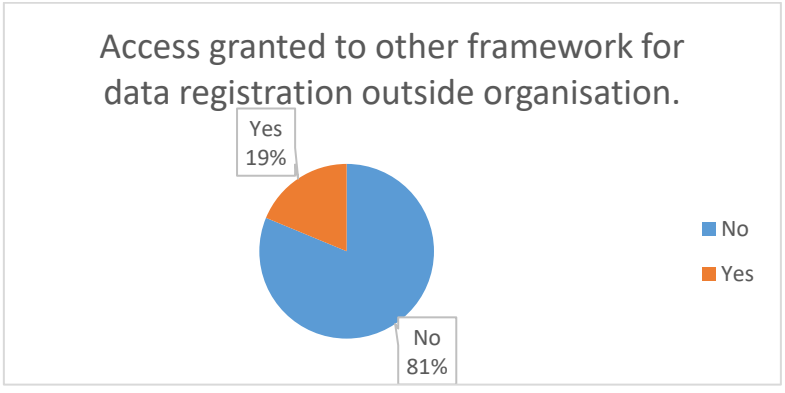


Fig 4.14: Representation of question 14 – Access granted to other framework for data registration outside organization.

Fig 4.14 depicts data in the shape of a pie chart, with 19% for yes and 81% percent for no. This suggests that just a few hospitals allow access to their registration procedure using other systems. On the chart, there are two legend entries that reflect details. On the graphic, the data labels show the results and their percentages.

The issue with increasing the use of IT foundation in e-medical services appears to be security concerns when frameworks are trusted with medical data. Electronic health records (EHR) contain a variety of transactions as well as common security concerns such as unauthorized access, data theft, and confidentiality. The following data analysis focuses on a query linked to the security of electronic healthcare records in this question posed to hospital administrative officers: "Any system that protects our electronic health records?"

Fig 4.15 represent question 15, question asked for confirming whether any existing system already used in tertiary hospitals of Punjab for protect electronic healthcare records and responses collected “no” from all hospitals. The contribution of technology can be found in almost every sector around the world. This has created a paradigm shift in how patient data is collected, stored and used when needed. What used to be a very hectic and time-consuming task is now easy. Previously, physician records were handwritten, took months to complete for each patient, were piled up and stored in large rooms, and had little security for approval. These records are now kept electronically with minimal fuss through a variety of software and electronic devices that are easy to store and available with just a few finger taps. The situation has improved, but security flaws remain.

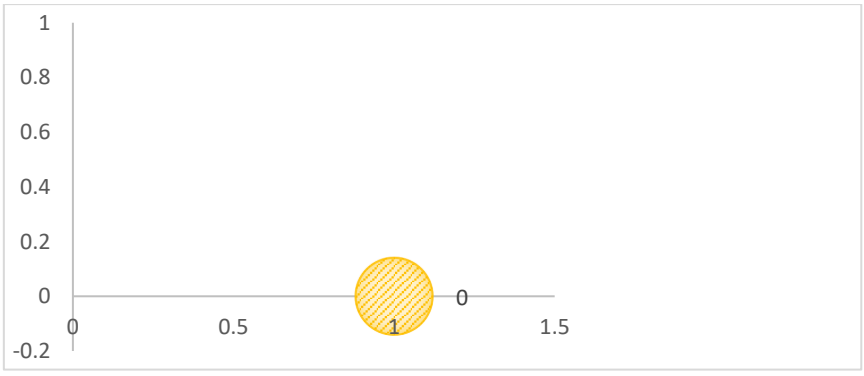


Fig 4.15: Representation of question 15 – Do you have system in Hospital that protects our electronic health records?

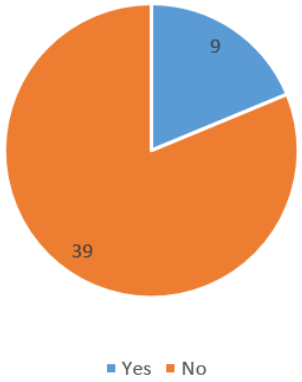


Fig 4.16: Representation of question 16 – Doctors having access to patient's data?

Access to data from one peer to another peer may be possible in an electronic healthcare system. This issue pertains to doctor access to patient data; according to the study, doctors access patients' data after registration on a regular basis. The responses are displayed as graphs. The supreme conclusion is no, which is 39 presented data labels in the chart 81 percent responses, and the pie chart displays the count of those hospitals from selected hospitals where doctors may access the patient's data.

The data in fig 4.16 is shown above. The series has been displayed as pie chart from yes to no, with the number of responses evident. The total number of legend entries is 48, with a vertical axis range of 0 to 45 due to the chart's maximum value of 39 for No.

Non-physicians and non-nurses in the health-care field Paramedical workers in the healthcare industry include medical technicians, emergency medical technicians, and physician assistants. Electronic health records are accessible from different systems in the healthcare system; in this issue, we examine data for hospitals for paramedical workers who have access to patient data in tertiary hospitals. Electronic health records have access from multiple systems in the e-healthcare system; in this question, we analyze data for hospitals for paramedical staff having access to patients' data in Punjab's tertiary hospitals, and responses from 48 selected hospitals are recorded and displayed in the charts.

Fig 4.17 ,4.18 shows the results of the expo in an area chart that shows yes and no responses. No result is indicated by 35 responses, whereas affirmative is shown by 13. The chart's range is shown by vertical values.

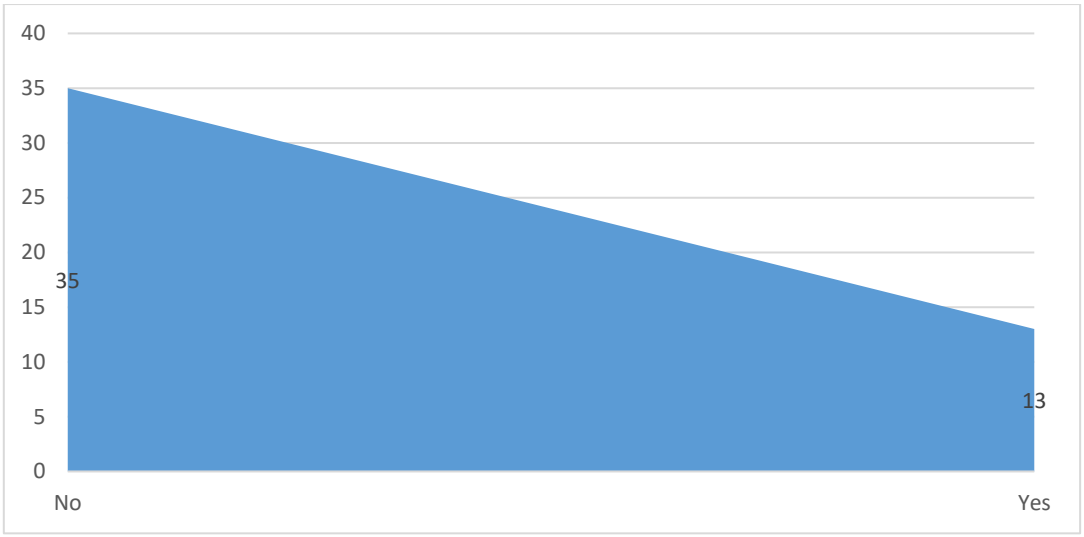


Fig 4.17: Representation of question 17 – Paramedical staff having access to patient's

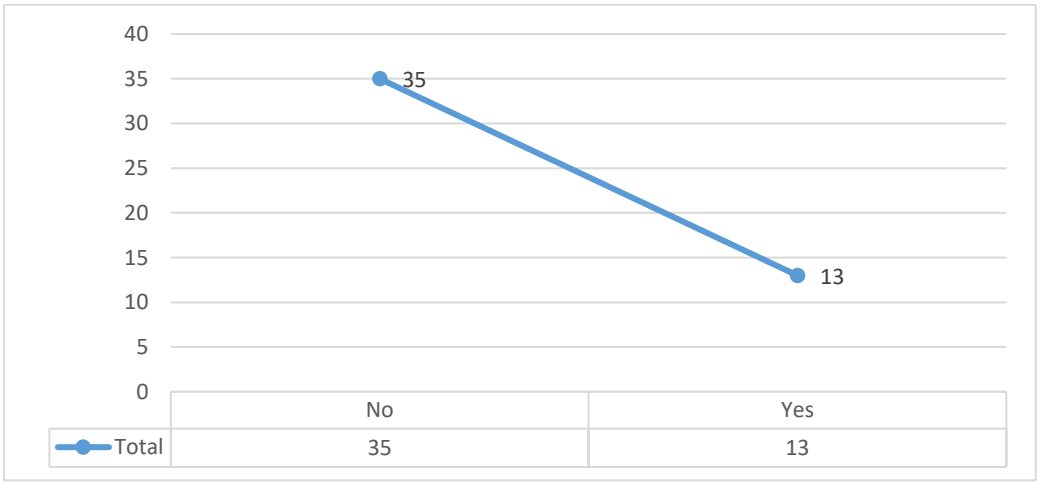


Fig 4.18: Representation of question 17 – Paramedical staff having access to patient's data?

The medical history of a patient can help determine the likelihood that they will develop lifestyle diseases like diabetes, heart attacks, etc., which are the primary cause of major medical issues. Question 18 "Patients have access to their own recent medicinal history." Request to collect answer from hospitals and 51% hospital response is no and 49% hospitals patients can access their medical history as shown in figure 4.19.

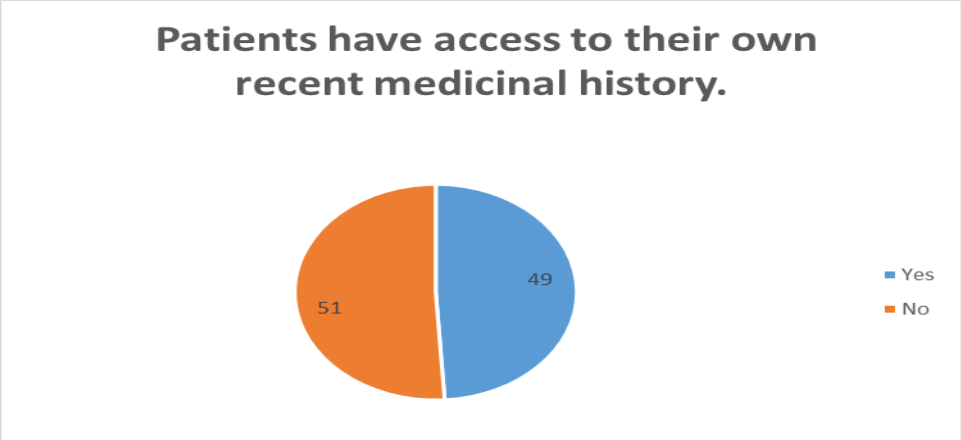


Fig 4.19: Representation of question 18 - Patients have access to their own recent medicinal history.

Data classification is a crucial phrase in an organization where millions of transactions are done in a matter of minutes. By employing classification, we can obtain data based on a variety of characteristics. Our analysis is represented in fig 4.20 and 4.21 by the classification of data in Punjab's e-healthcare. Fig 4.19 shows data after analysis with a range of 0.8 to 1.2 on the horizontal axis and a data range of 1, 0 and 1, indicating that the response is not one for all entries. The responses are divided into yes and no categories.

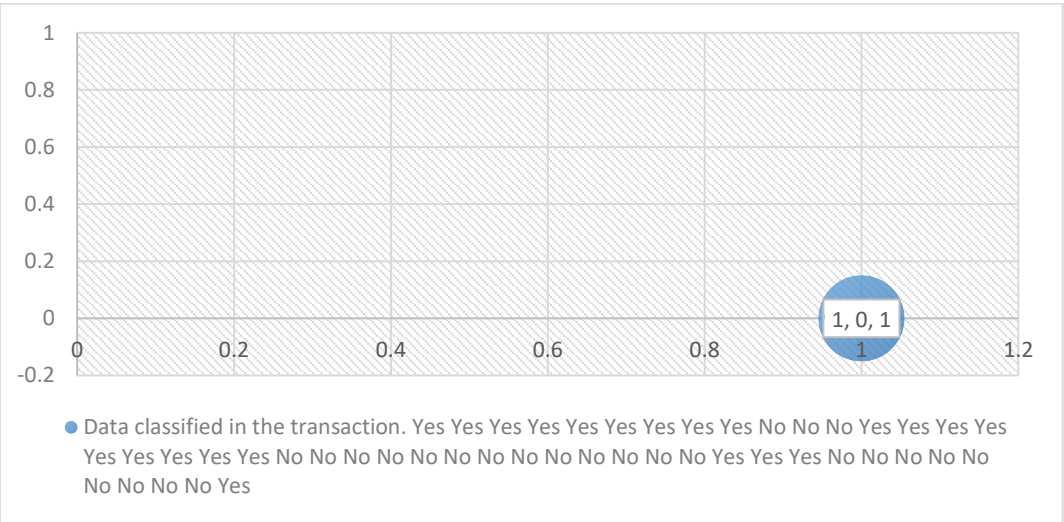


Fig 4.20: Representation of question 19 – Data classified according to transaction?

Question 19 requested to collect information about the classification of data in transaction. There are 25% hospitals that are not classified any data in the transaction and 75% hospitals classify data as per transaction execute. Stacked bar chart implements in next stage that represent data for two levels of stack for response yes and no. Data table in the fig 4.21 show result and their respective counts for yes and no. Data table has count values for no is 25 and for yes 23. Stacked bars represent data on chart area.

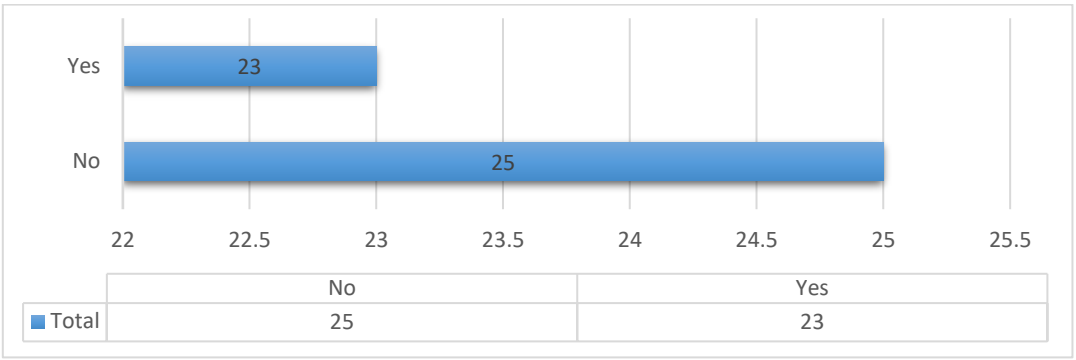


Fig 4.21: Representation of question 19 – Data classified according to transaction?

Question 20 requests for notice any existing system used in hospital for track transactions and detect security incidents. Response from hospitals collect in the form of yes and no, 69% responds no and 31% respond yes as depicts in fig 4.22.

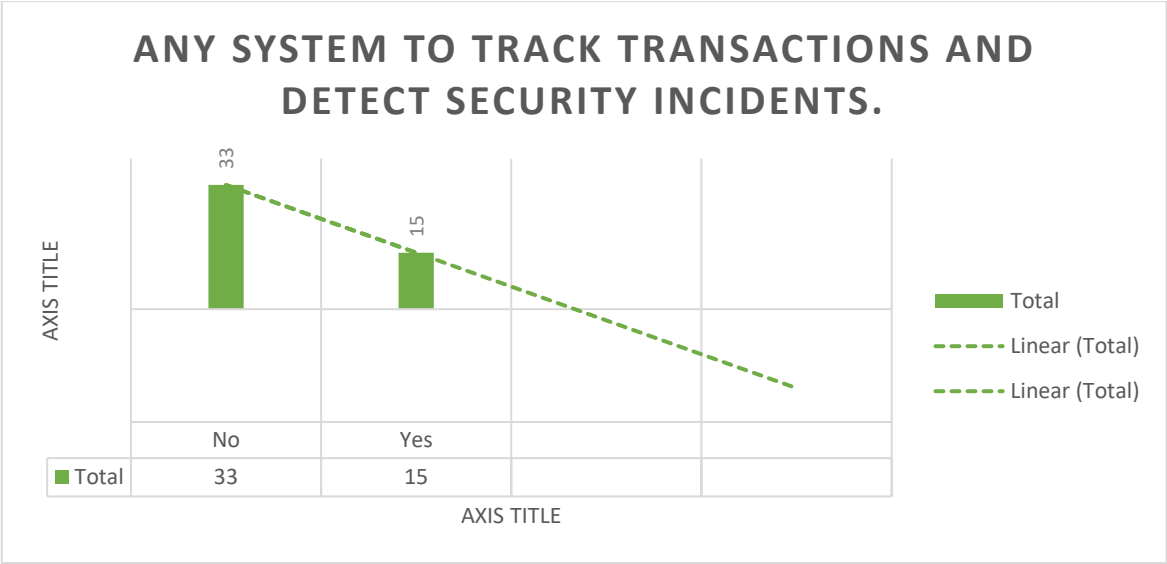


Fig 4.22: Representation of question 20. Any system to track transactions and detect security incidents.

Question 21 demonstrate using column chart implement. In which next stage that represent data for two levels of stack for response yes and no. 50% of hospital respond for sure they use secure path for transactions and 50% hospitals respond no for secure path of the transactions. Data table in the chart show result counts for track transaction and detect security incidents. Data table has count values for no 33 and for yes 15.

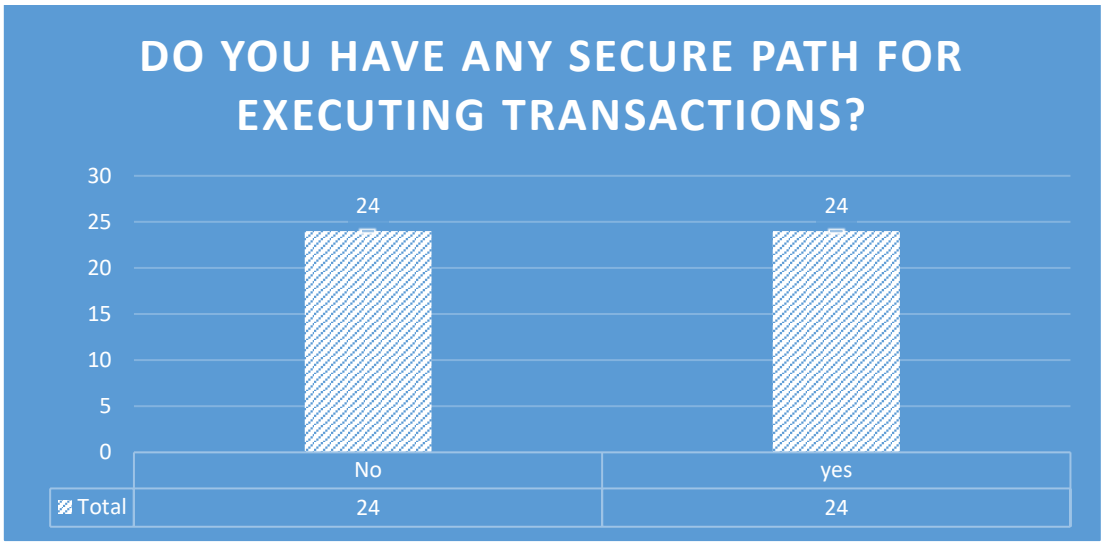


Fig 4.23: Representation of question 21 - Do you have any secure path for executing transactions?

Fig 4.23 indicate Column chart implement in next stage that represent data for two levels of stack for response yes and no. Data table in the chart show result counts of construct any secure path for executing transaction. Data table has count values for no 24 and for yes 24.

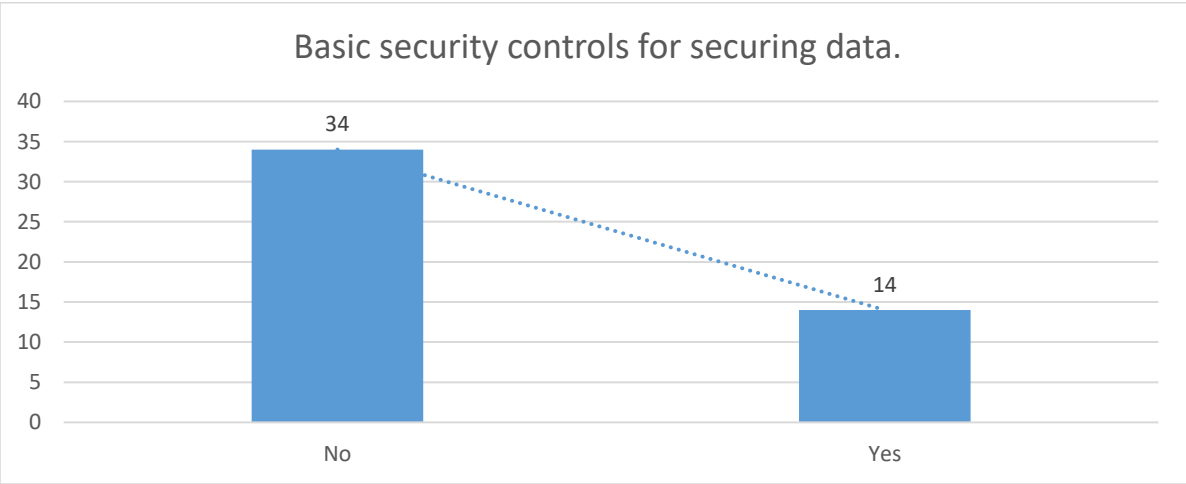


Fig 4.24: Representation of question 22 – Basic security controls for securing data.

Question 22 queried for collect information about basic security controls for securing data available in hospitals. Stacked bar chart implements in next stage that represent data for two levels of stack for response yes and no. Data table in the chart show result and their respective counts for yes and no. Data table has count percentage for no is 29% and for yes 71% and respective values are 14 and 34. Fig 4.24 ,4.24 has demonstrated analysis done

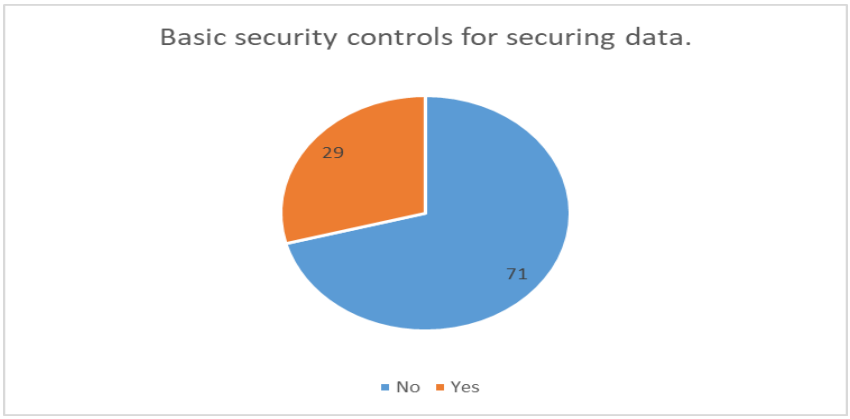


Fig 4.25: Representation of question 22 - Basic security controls for securing data.

In question 23, queried for "What do you think is it required to improve transaction path? "And response collect for yes and no, count of responses in case of yes and no are respectively 40 and 8. Pie chart implement in next stage that represent data for two levels of stack for response yes and no. Data table in the chart show result and their respective counts for yes and no. Fig 4.26 illustrated same analysis about improving transactions.

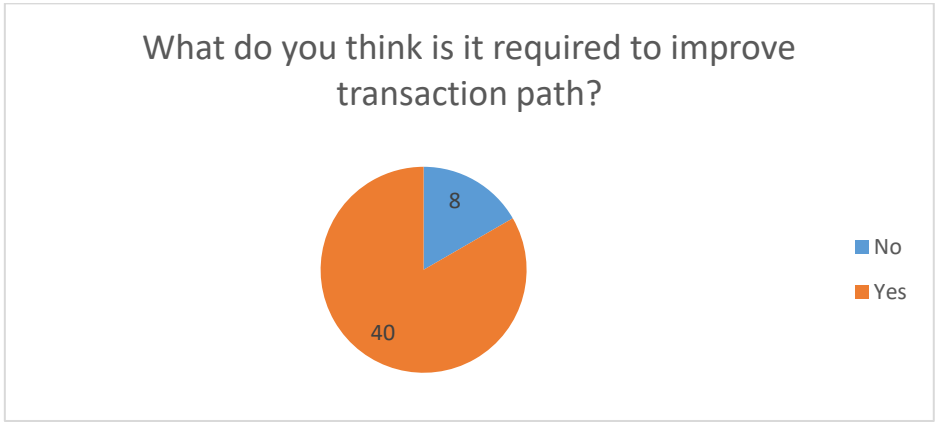


Fig 4.26: Representation of question 23 – What do you think is it required to improve transaction paths?

Pie chart implement in next stage in fig 4.27 that represent data for two levels of stack for response yes and no. Data table in the chart show result and their respective counts for yes and no.

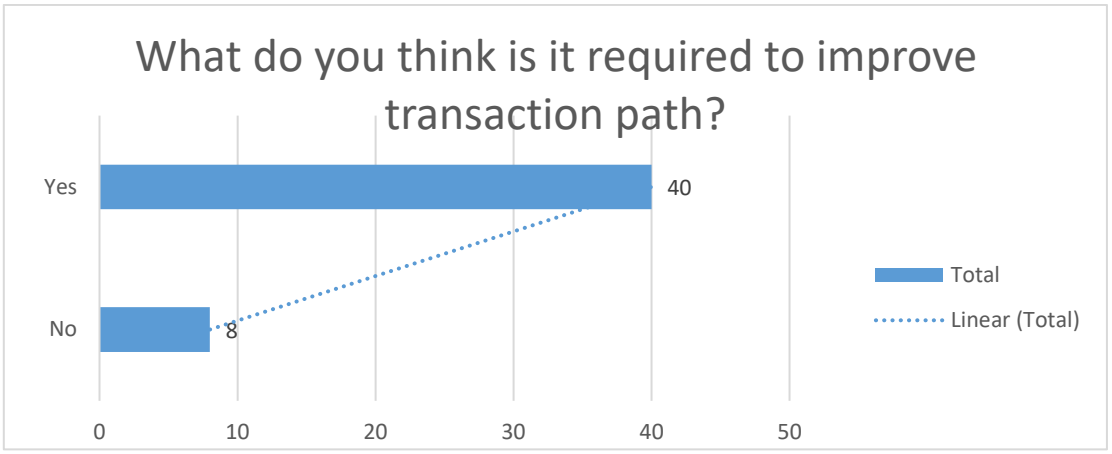


Fig 4.27: Representation of question 23 – What do you think is it required to improve transaction paths?

Question 24 queried to get responses from administration of hospitals whether any difficulty in transaction processing notes. Answer provided in the form of yes and no. Stacked bar chart fig 4.28 and fig 4.29 implements in next stage that represent data for two levels of stack for response yes and no. Data table in the chart show result and their respective counts for yes and no. Data table has count values for no 8 and for yes 40. Stacked bars represent data on chart area.

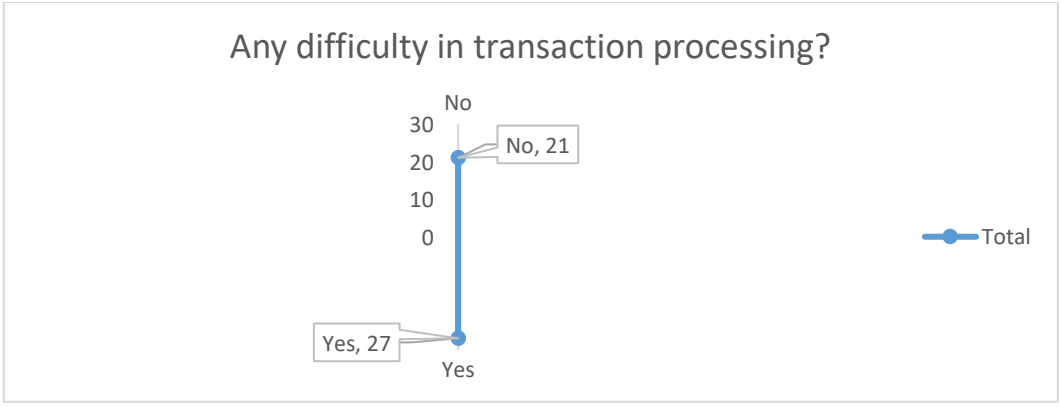


Fig 4.28: Representation of question 24 – Any difficulty in transaction processing?

Fig 4.27 and 4.28 indicate Line chart implement in next stage that represent data for two levels of stack for response yes and no. Data table in the chart show result and their respective counts for yes and no. Data table has count values for no 21 and for yes 27.

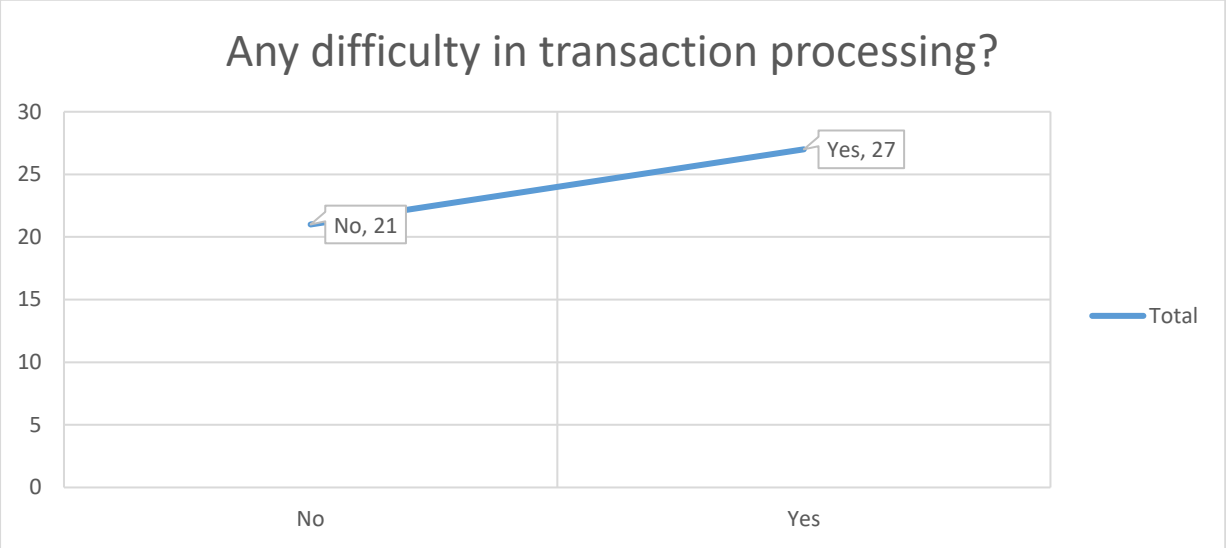


Fig 4.29: Representation of question 24 – Any difficulty in transaction processing?

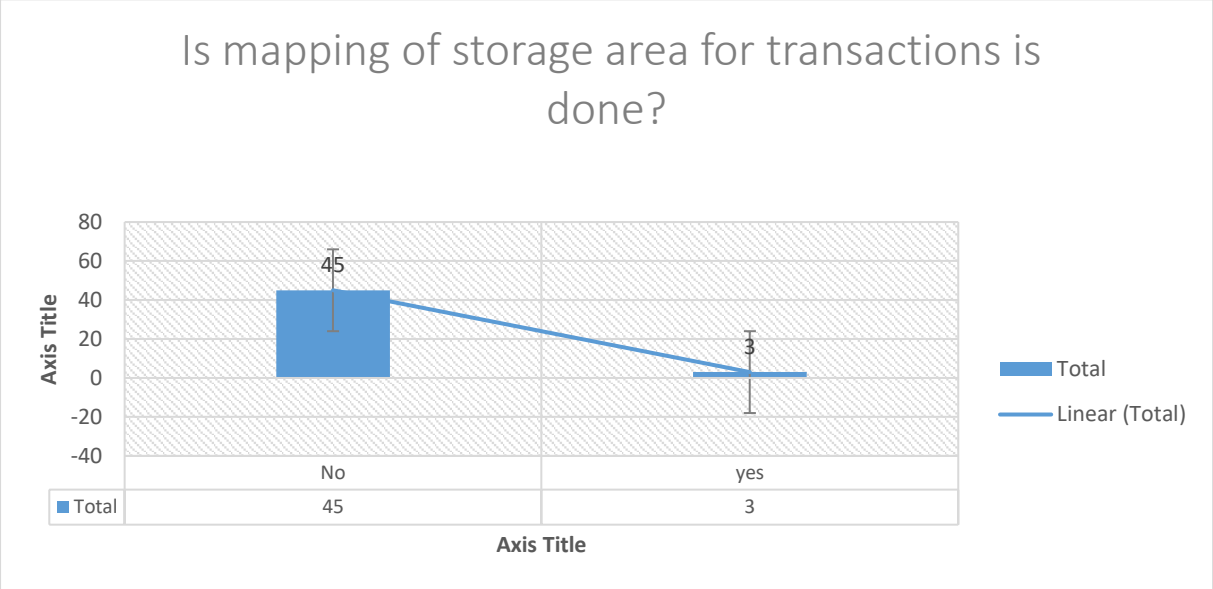


Fig 4.30: Representation of question 25 – Is mapping of storage area for transactions is done?

Fig 4.30 indicate Line chart implement in next stage that represent data for two levels of stack for response yes and no for question related to mapping of storage area in case of replication of data. Data table in the chart show result and their respective counts for yes and no. Data ranges for no is 45 between 0 to 45 and for yes is 0 to 3.

A fundamental idea in human resource development is training. It is involved teaching and practicing a specific talent until it reaches the target level. Question 26 queried for training provided for accessing e healthcare system. Responses of question 26 represented in figure 4.30. 75% Reponses indicates for yes and 25% responses indicates for no.

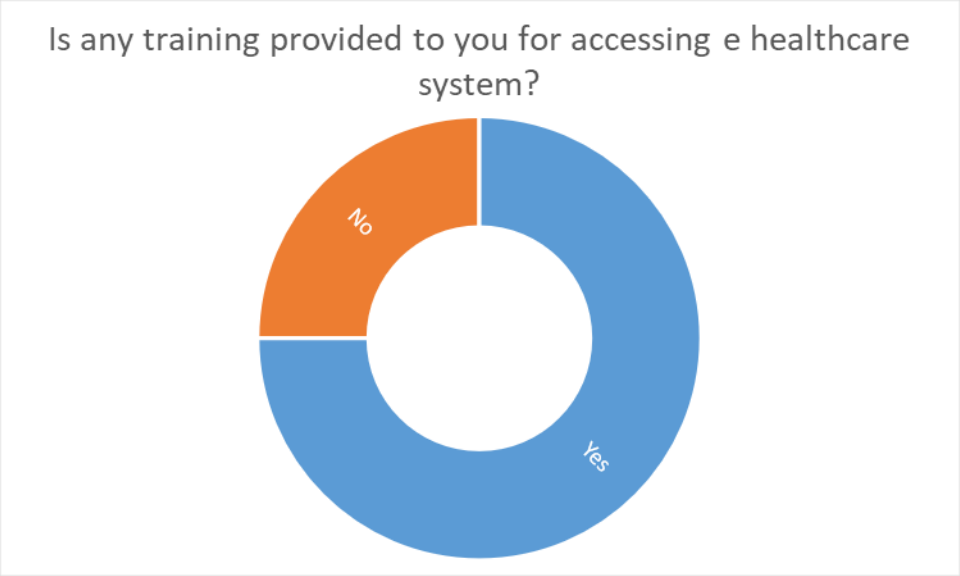


Fig 4.31: Representation of question 26 - Is any training provided to you for accessing e healthcare system?

Numerous transactions performed in e healthcare system; it is required to secure transactions in e healthcare system. The next question queried for “How security provided to transactions”. 31.25% of administrator’s respond for yes, 68.75 % admin staff response was no because they directly interacted with the web application don’t know if any system for transaction security they use.

In the event of a main data failure, the backup's goal is to make a copy of the data that can be retrieved. Primary data failures may come from hardware or software issues, data corruption,

or a human error like a malicious attack (virus or malware), data deletion accident, or another human-caused event. To aid a company in recovering from an unexpected catastrophe, backup copies make it possible to restore data to a previous point in time. Question 28 queried for the backup and recovery plan availability in e healthcare system and fig 4.31 show responses in the pie chart 42% responses collected for “no” in those hospitals administrator told no backup plans they have in their hospitals. 58% hospitals administrators respond for “yes”.

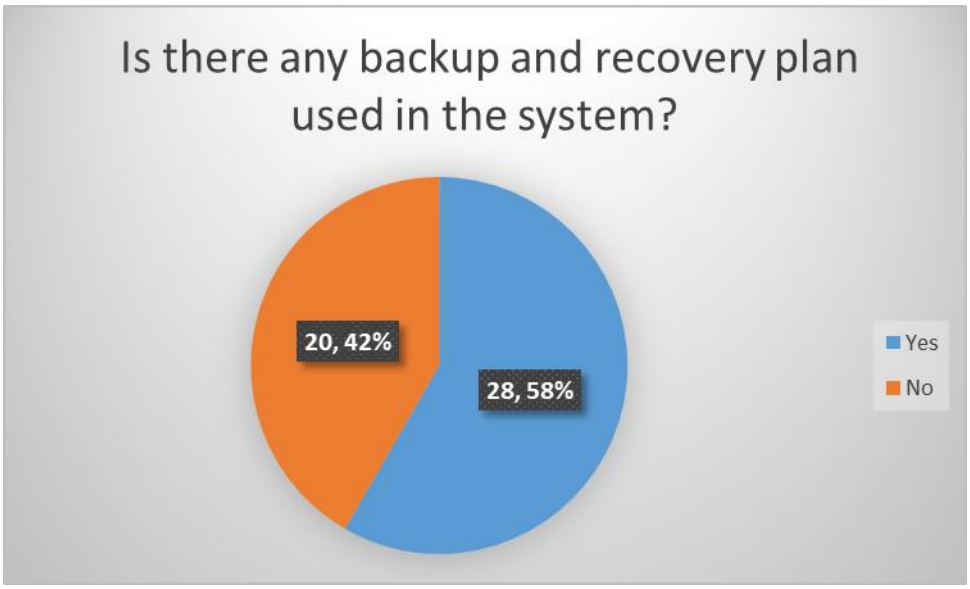


Fig 4.32: Representation of question 28 - Is there any backup and recovery plan used in the system?

Health care data management is the collection of patient information from various providers' and organizations’ sources. It enables health care professionals to input patient data into a single database so that it may be safely kept, processed, and shared. Question 29 queried to know the third-party services used for data managing in tertiary hospital of Punjab. 25% response relates to hospitals having third party services for managing data and 75% of hospitals administrators respond that there was no use of any third-party services for data managing. When question related to security issues in healthcare asked to administrator, information provided is 70.8% of them said security issues they have Health information exchanges and electronic health records because, 29.1% of them said outdated technology used in hospitals is concern of security issue.

The disclosure of private, sensitive, or otherwise confidential data into an unsecure setting is a data breach. A data leak may happen by chance or arise from an intentional attack. Every year,

millions of people are impacted by data breaches, which can range in size from a doctor accidently viewing the wrong patient's file to a widespread attempt to hack into government servers in order to obtain private information. When question related to data breach is being asked most of administrators, they replied that they do not have any idea about this but still 77 77.0 % of administrators respond for no and 23.0% respond for yes. Administrators from those hospitals respond for yes for data breach next question floated to them is “How do you know?”. There are number of reasons they ask for sure their data has breached. Their patients got emails, phone calls and SMS from insurance companies, medical lab consultancies etc. Sometimes information is replaced with unknown information.

Health insurance companies always in search of patient’s data which they can use for the purpose of their sole profit in selling insurance even in this research work 37.5 percent of administrators they said insurance companies try to contact them directly and indirectly about patients data but according to Medical council of India guidelines that for 3 years data of patients can be shared and deleted from system so they refused them ,But system of data entry is like that from where data in entered , how many people process data as there are lots of leak points in the system through companies able to get data and administrators even said that there team is working on it .

When question related to whether medical labs are approaching hospitals for any data related to patients, initially administrators were reluctant to provide information but 29.1 percent of them said yes that many private medical labs approached them for data related information directly and indirectly as medical labs want to utilize data for selling their products and services.

Some administrators said that if patient want only then they are sharing data as data which is collected by hospitals contain comprises of administrative and demographic data, medical diagnosis, medical treatment, prescription medications, laboratory test results, physiologic monitoring data, hospitalization, patient insurance. Some Hospitals don't have adequate electronic medical record systems, and they don't know who is logged into the system or have a way to track them down ". "This makes it very challenging to actually identify who is removing data, Additionally, many hospitals and clinics lack explicit protocols on whether to delete or keep data. Reports can also be located near the reception area at diagnostic facilities, and it's unclear how much data the receptionist and the doctor have access to.

When question related to data disposition is asked to administrators most of them almost 87.5 percent they replied and answered that they does not have any idea about data disposition and around 12.5 percent those who replied that there is policy of data disposition but when asked about policy they do not have any idea as only 2 administrators they know about that according to medical council of India guidelines hospitals need to maintain and all records of patients digitally or physically for 3 years from commencement of treatment for Indoor patients and for 1 year for outdoor patients.

Data analysis is very important and useful if any organization is collecting data and then they can use data analysis concept to get insights about data. When question related to this is asked from hospital administrators 43.7 percent said that they use basic data analysis to fetch information related to total patients visits weekly and monthly , patients visit doctor wise weekly and monthly and disease wise data analysis they are doing in order to find out which area is infected with what type of disease and 47.9 percent said that they are using data analysis mostly as reporting tool but it was not there routine task to analyze data ,When any higher official ask then they make report for them and 8.4 percent said that they are not using any type of analysis and only third party and policymakers are analyzing data they are into collection phase only .Those who replied that they are analyzing data for different purposes most of them are using Microsoft excel as reporting tool to create graphs and present data to their peers whenever required ,Few of them said about usage of tableau and power BI but not at very advance stage .The system they are using for data entry have some features which can create different graphs and charts of different attributes with which they are analyzing data and that graphs are sufficient for them as they said for data analysis . Big data-driven approaches are being used by healthcare systems to achieve the goal of learning health systems and enhance the standard of care. Many are doing this in collaboration with third-party commercial firms to offer unique data processing and analytic capabilities, as well as to give personal health information to a for-profit sector that may keep and sell data. As When question is being asked about data analysis 8.4 percent said they are using third party services for data entry and analysis and rest of hospitals are using tool for data entry as analysis tools also but these 8.4 percent said they had control of sensitive data of patients like there personnel data and purpose of visit data.

After completing almost all necessary question to be asked from hospital administrators a question related to hospital efficiency is being asked as hospital efficiency is really important aspect of process-based organizations. Hospital efficiency can be measured with many methods

like Data envelopment analysis DEA but here question is form administrators about their overview and not too much about data centric and almost all replied yes that EHR provides accurate, current, and detailed patient records. It makes patient records instantly accessible, allowing for better coordinated and efficient care. EHR makes prescribing safer and more dependable. EHR gives doctors the ability to evaluate tests, view results, and submit prescriptions when away from the office, enhancing their freedom and speeding up patient treatment. Doctors will have the freedom to view the records on smartphones, tablets, or desktops from anywhere at any time through internet connectivity rather of waiting for couriers or racing back to the offices. Many administrators even said that with an EHR, productivity is more than just producing paperwork quickly. Typically, scheduling and time management are used to measure productivity. Physicians can evaluate more patients each day with the help of modest tweaks to their scheduling procedures, such as having two patients ready to go when the clinic opens and allowing patients to arrive 10 minutes before their appointment.

EHR adoption in the healthcare sector has gradually and innovatively replaced manually filing patient information in folders. One of the notable changes in the healthcare sector is the growing adoption of electronic health records (EHR). EHR implementation in a healthcare system is more difficult than it seems. The implementation and usage of an electronic health records system may provide a number of difficulties so when this question is being asked form administrators most of 52.03 percent replied that issues related to training of data entry operators, retaining of employees, cost of implementation and technical problem if occurs very difficult to reinstate. 25 percent said that major challenges is about fear of data leakage of sensitive information of patients that is why they are not paying too much stress of data analysis. 22.9 percent said that implementation cost, training and data leakage are most prominent issues need to addressed.

4.2 Consensus Mechanism

Sharing healthcare data among organizations has become more difficult as a result of technology advancements. Data compatibility may be hampered by heterogeneous data modelling, and the usage of several healthcare terminologies limits data interpretation. Even if the semantics and structure of data have been accepted, data security and consistency have been taken into account. Numerous attackers are attracted to authorized suppliers and centralized data storage. It's more difficult to maintain a consistent perspective on a patient's record through data sharing networks. Proof of Word and Interoperability for data discovery and access were

validated using a consensus approach. This method provides a centralized source of trust for network consensus as well as computes consensus verification of semantic and structural interoperability. This consensus process provides better trade off in contradiction to other network modelling [123, 124].

Modern healthcare systems are known for being extremely complicated and expensive. Improved health record management, the use of insurance companies, and blockchain technology can all help to lessen this. The original purpose of blockchain was to offer distributed records of money-related transactions that were not reliant on centralized authorities or financial organizations. Breakthroughs in blockchain technology have enhanced medical records, insurance billing, and smart contracts transactions, offering permanent access to and security of data as well as a distributed database of transactions. One of the most significant benefits of blockchain technology in the healthcare industry is that it can improve the interoperability of healthcare databases, allowing for greater access to patient medical records, device tracking, prescription databases, and hospital assets, as well as the entire life cycle of a device within the blockchain infrastructure. Access to a patient's medical history is required to properly prescribe medicines, and blockchain has the potential to significantly improve the healthcare services framework. Several frameworks and tools for measuring the performance of such systems, such as Hyperledger Fabric, Composer, Docker Container, Hyperledger Caliper, and the Wireshark capture engine, are studied as possibilities for reducing present constraints in healthcare systems using blockchain technology.

To secure e-healthcare system, we design a framework using blockchain to secure electronic healthcare transactions. Policy on Access Control Algorithm for enhancing data accessibility between healthcare providers and assisting in the simulation of environments to implement the Hyperledger-based electronic healthcare record (EHR) sharing system that employs the chain-code concept. Latency, throughput, and Round-Trip Time is all performance parameters that have been adjusted in blockchain networks to achieve better outcomes. Unlike standard EHR systems, which are built on a client-server architecture, the suggested solution is built on blockchain, which improves efficiency and security. Smart technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning, Virtual Reality (VR), and Augmented Reality (AR) have altered engineering and manufacturing industries such as automotive, computing and electronics, and aerospace and defense. Hospitals and general practitioners, for example, employ a range of healthcare systems. They've grown in strength

and utility through time. In addition, mart technologies have improved their ability to handle big data volumes in real time, allowing for speedier identification and diagnosis of ailments, as well as automated therapy options and comparisons. Transparency and communication between patients and healthcare providers are also improved with the usage of blockchain technology.

The proposed algorithm for exchanging electronic health records, which is based on the blockchain network, is given. As a result, a blockchain-based EHR sharing system architecture is developed. The network employs a variety of block transaction processes and parameters. On the suggested technique, the EHR can be spread to other users in the blockchain network utilizing a shared symmetric key and private key. In addition, the optimal EHR sharing algorithms are investigated for a smooth functioning and reduced communication time.

Proposed system to secure electronic health records using blockchain divided into four participants: - Patients, Clinical, Lab and system administration. Fig 4.33 shows the connection between all these participants.

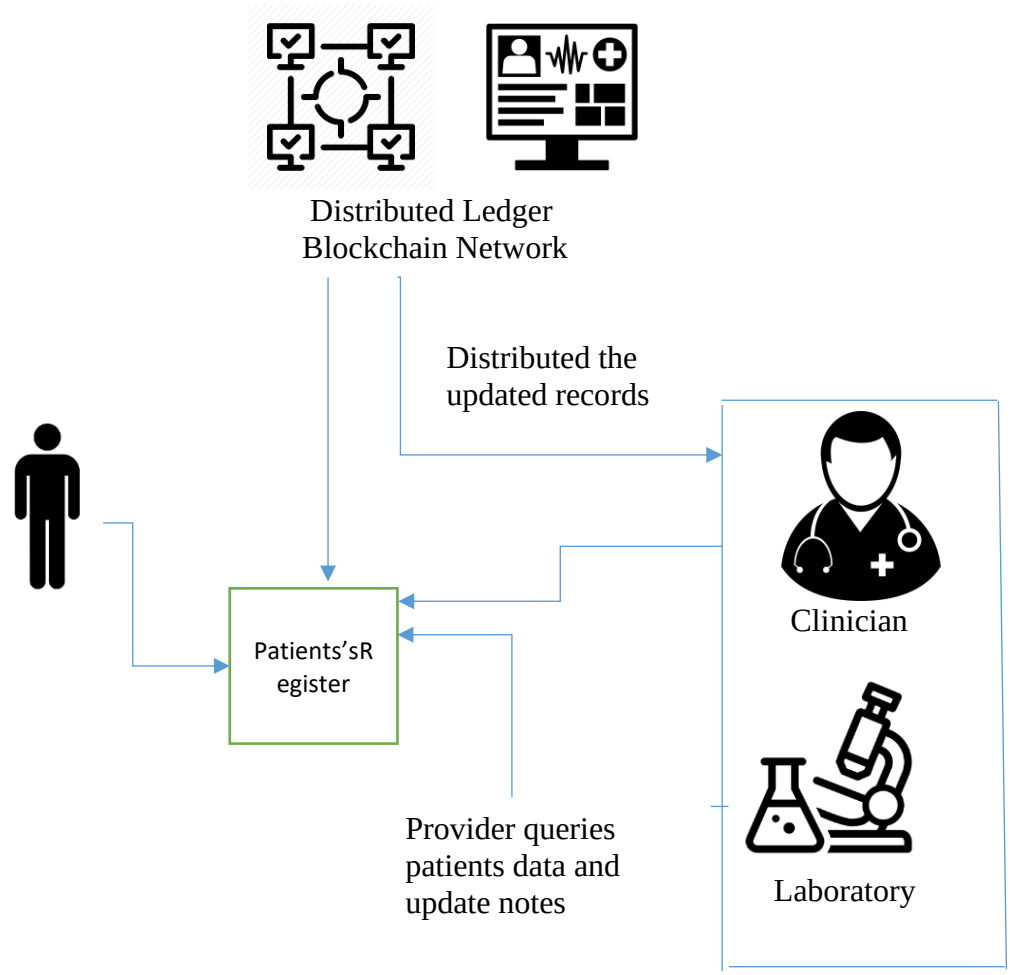


Fig 4.33: The Connection between all the participants in E Healthcare System.

The four types of participants in the EHR sharing system are administration, patients, clinicians, and laboratory staff. In a blockchain network, Algorithm 1 represents the precise execution of admin. The admin's enrolment certificate is requested from the certifying authority. The system is completely within the admin's control, including the ability to write, read, update, and remove participants. If clinicians, patients, or laboratory employees are genuine, the administrator can assign each participant a unique ID that allows them to access the blockchain network. If a participant's behavior is deemed undesirable, the administrator can remove them from the Hyper ledger blockchain network by posting a comment. Table 4.1 lists the acronyms used in the algorithm.

Table 4.1 Abbreviations

C_A	Certificate Authority
E_C	Enrolment Certificate
C_{ID}	Clinician ID
P_{ID}	Patient ID
L_{ID}	Lab ID
P_K	Private Key
P_{DL}	Patient distributed ledger
C_{DL}	Clinical distributed ledger
L_{DL}	Lab
N_{Admin}	Network admin
B_N	Blockchain network
U_{Name}	Username
P_{REC}	Patient Records
M_{PID}	Medical records of patients

Algorithm of admin is access to the transactions, input enrolment certificate (E_C) from certificate authority (C_A), actual input given to the blockchain network. Output access to the P_{DL}, C_{DL} and L_{DL} transactions for all (P_{DL}, C_{DL}, L_{DL}) € B_N. Algorithm initialisation start from network admin. N_{Admin} may be justifiable node. N_{Admin} can Create, Read, Write, Update and Remove C_{ID}, P_{ID}, L_{ID}.

Algorithm 1: Algorithm on Admin working

1: **Procedure** Admin (P_{ID}, C_{ID}, L_{ID})
2: **while** (True) **do**
3: **if** (C_{ID} is valid) **then**
4: Add Clinician to the blockchain network
5: Add Clinician (B_N, CID)
6: Grant access (C_{ID}, U_{Name}, P_K)
7: **else**
8: Not exist (C_{ID})
9: **end if**
10: **if** (P_{ID} is valid) **then**
11: Add Patient to the blockchain Network
12: Add Patient (B_N, P_{ID})
13: grant access (P_{ID}, U_{Name}, P_K)
14: **else**
15: Not exist (P_{ID})
16: **end if**
17: **if** (L_{ID} is valid) **then**
18: Add Lab to the blockchain Network
19: Add_Lab (B_N, L_{ID})
20: grant access (L_{ID}, U_{Name}, P_k)
21: **else**
22: Not exist (L_{ID})
23: **end if**
24: **end while**
25: int FLAG; {0 means bad behavior, 1 means good behavior}
26: **for all** (,,) **do**
27: **if** (behaviour_node (FLAG) then
28: Not update (C_{ID}, P_{ID}, L_{ID})
29: **else**
30: Remove update (C_{ID}, P_{ID}, L_{ID})
31: **end if**
33: **end procedure**

In electronic healthcare system numerous transactions has been executed in some seconds, the systematic execution of patient module is displayed in proposed algorithm 2, In this case, the patient node asks for a private key to access network administration. The patient has different powers after being allowed access to the blockchain network, including the ability to read, write, and revoke EHR records. The patient node's identifier in the blockchain network is used in this method. Patient, clinician, and laboratory staff records can be viewed or searched across the network if the patient has a valid node. If M_{PID} is on a patient's hyperledger network, M_{PID} can give the clinician node access to read and update the patient's medical records in the blockchain network.

Algorithm 2: Algorithm on Patient working

---

procedure Patient (P_{ID})
while (True) **do**
if (P_{ID} € BN) **then**
if (P_{REC_1} not B_N) **then**
    Create_records(P_{ID}, P_{REC_1}, B_N)
else
    Update_records(P_{ID}, P_{REC_1}, B_N)
    Read_records(P_{ID},P_{REC_1},C_{ID}, L_{ID}, B_N)
end if
else
    Not_exist(P_{ID})
end if
if Visit(P_{ID},C_{ID}, L_{ID}, B_N) **then**
    M_{PID} = Medrecord(P_{ID})
if then M_{PID} P_{DL} (B_N)
    Grant_records(M_{PID},C_{ID}, L_{ID}, B_N)
else
    (C_{ID}, L_{ID}) ← NOTIFY (" Patient Medical record does not exist")
end if
if (M_{PID} C_{ID}, L_{ID} Treatment_completed(P_{ID})) **then**
    Revoke_records(M_{PID}, P_{REC_1},C_{ID}, L_{ID},B_N)

22: **else**

23: (C_{ID}, L_{ID}) ← NOTIFY(”P_{ID} voluntary revoke M_{PID}”)

24: Revoke_records(M_{PID}, P_{REC_1},C_{ID}, L_{ID},B_N)

25: **end if**

26: **else**

27: Not Visit

28: **end if**

29: **end while**

30: **end procedure**

In the blockchain network BN, algorithms gain access to the PDL transaction process. A valid node in the patients distributed ledger should be able to read, write, and revoke electronic healthcare records. Step 17 recommends that if medical records are unavailable, the system should notify the clinician that the patient's medical history is unavailable. If the patient does not want their data to be shared after the therapy is finished, the patient can revoke access from the laboratory staff member or doctor on the network. Step 20 recommends that if MPID is in the clinician's or laboratory's distributed ledger network, the patient can invoke the revoke method to revoke access to the blockchain network. Otherwise, the patient can inform the clinician or laboratory personnel by voluntarily cancelling access and then using the calling method.

Algorithm 3 depicts the clinician module's precise operation. In the input step, the clinician asks the network administrator for a key to permit login. The clinician is provided access to clinician distributed ledger transactions during the output phase. A genuine node should be used. Patients' medical records are granted to the physician if CID is a member of the blockchain network. The clinician can then access and change the system's permissioned EHR. The clinician can write records in the distributed ledger network even if they don't have access to the patients' IDs. A clinician can also use the network to find available clinicians and laboratory personnel. Clinician working has been demonstrated on the blockchain network where CID € BN, get access to CDL having read/write permissioned electronic healthcare records by the patients and capture medical records of patients over blockchain network BN.

Algorithm 3: Algorithm on Clinician working

1: **procedure** Clinician (C_{ID})
2: **while** (True) **do**
3: **if** (C_{ID} € B_N) **then**
4: **if** (Granted M_{PID} C_{ID} **then**
5: Read_records(C_{ID}, P_{REC_1}, M_{PID}, B_N)
6: Update_records(C_{ID}, P_{REC_1}, M_{PID}, B_N)
7: **else**
8: Write_records(C_{ID}, M_{PID}, B_N)
9: Read_records(C_{ID}, L_{ID}, B_N)
10: **end if**
11: **else**
12: Not_exist(C_{ID})
13: **end if**
14: **end while**
15: **end procedure**

Transactions in the lab are recorded in electronic health records. Algorithm 4 shows the process for executing lab work in a methodical manner. In this instance, the laboratory staff requests the private key from the network administrator. Access to the distributed ledger network is granted if the node is determined to be valid in the output of the input request. The lab node works in the same way as the clinician node. The lab node may read medical records and provide reports depending on the results of tests performed on patients, such as blood tests and immunity testing. This node can also look for available laboratory professionals and clinicians across the entire network.

Algorithm 4: Algorithm on Lab working

1: **procedure** Lab(L_{ID})
2: **while** (True) **do**
3: **if** (L_{ID} € B_N) **then**
4: **if** (Granted M_{PID} € L_{ID} **then**
5: Read_records(L_{ID}, P_{REC_1}, M_{PID}, B_N)
6: Write_reports(L_{ID}, P_{REC_1}, M_{PID}, B_N)
7: **else**
8: Read_records(L_{ID}, L_{ID}, B_N)
9: **end if**
10: **else**
11: Not_exist(L_{ID})
12: **end if**
13: **end while**
14: **end procedure**

If the node is verified to be valid in the output of the input request, access to the distributed ledger network is given. The lab node functions similarly to the clinician node. The lab node may read medical records and generate reports based on the results of patients' tests, such as blood tests or immunity tests. This node can also search the entire network for available laboratory personnel and clinicians.

Whenever another square is communicated to the organization in a decentralized square chain, every hub has the choice of adding it to the worldwide record duplicate or eliminating it. To forestall the expansion of the worldwide record (block chain) and keep away from undermined attempts or pernicious assaults, agreement is utilized to search out most of the organization to vanquish on a solitary condition of adjustment. Specifically, block chain is considered a huge, shared worldwide record that anyone can alter. An ill-disposed offense happens when a hub chooses to alter the condition of the worldwide record duplicate, or when a gathering of hubs connives to attempt to do as such. For instance, if Alice somehow managed to send 10-cycle coins from her wallet to Bob, she could need to guarantee that nobody in the organization can

mess with the exchange content and that she can modify 10 digit coins to 100 piece coins [125]. To guarantee accuracy and security on a worldwide scale, a common public record should have a solid and powerful agreement system that is issue lenient and meets the necessities that I all hubs should keep an indistinguishable square chain simultaneously, and ii) it shouldn't depend on incorporated position to keep pernicious foes from disturbing the coordination interaction. To be exact, each message sent between hubs should be confirmed by countless organization members through an agreement-based arrangement. Also, the organization in general should be tough to halfway disappointments and 'assaults, for example, when a bunch of hubs is associated with being malevolent or when a message on the way is spoiled.

The best agreement procedure for block chain execution should meet the prerequisites of a vigorous conditional record with two key properties: vivacity and perseverance. Regardless of state moves, determination guarantees a steady reaction from the framework. For instance, assuming one hub in an organization demonstrates that an exchange is in a "steady condition," following organization hubs should approve it as consistent assuming that it is answered and questioned truly. Since all hubs or cycles are alive, they can ultimately satisfy all qualities or pursue all choices. At last, it says that getting those arrangements might take an OK timeframe. By joining these liveness and sturdiness, it guarantees that the conditional record is successful, permitting just verification exchanges to be approved and focused on. The huge advantages of square chain, as demonstrated above, are basic for medical care and biomedical applications. The main creating application field of square chain circulated record innovation is medical care. Block chain is a dispersed record that is utilized to deal with and store medical services related fields for the motivations behind trading, sharing, and recording, assessing, and approving basic purposes among partners. The most engaged field connected with block chain reception in medical services/biomedical applications is its basic infra-structure for Health Information Exchange (HIE), wellbeing exchanges including patients, payers, suppliers, and other appropriate gatherings. These applications are then classified in light of their essential objectives for using block chain-based information capacity, which are Enhanced clinical record the executives, further developed protection asserting strategy, and sped up biomedical/clinical exploration. Progressed biomedical/medical care information record system depicts applications past HIE. Several studies and projects, including MedVault, healthcare data gateways, Fatcom, Gem Health Network, BitHealth, and others, focus on exchanging patient care data with block chains to improve medical record administration. Many well-known companies, such as Accenture and Deloitte, are using Blockchain

technology into their health-care data and record-keeping processes. Guard time, a firm that offers a block chain-based solution in Estonia to protect 1 million health records, is another notable example. This study employs consensus techniques for the aforementioned applications. This is a group-based protocol for achieving group dynamical agreement. In contrast to majority vote, consensus emphasizes that establishing an agreement may benefit the entire grouping as a whole. The crisis of dynamically achieving group consensus is reliant on group-based coordination. Because of defective processes and bad actors, these coordinated consensuses are modified with.

Spyder IDE (Integrated development environment) used for implementation and testing of code using python programming language for test POW. Python is one of the most dynamic and adaptable programming languages currently accessible. Python has grown in popularity since its introduction in the 1990s, and many of people are learning this Object-Oriented Programming language today. If you're new to programming, you've probably heard about the recent buzz surrounding Python's capabilities and are probably wondering what makes this programming language so unique.

4.3 Why python for blockchain?

4.3.1 Advanced

Python has been around for a while and is steadily gaining traction in the computer world. Python has greatly progressed as a language and is currently at an advanced stage, ensuring stability and dependability. Python is supported by a huge and dedicated community of developers. It's a technology with a bright future, so you can rest easy knowing that your project won't be built on an out-of-date language. Furthermore, Python has a short learning curve, making it easier for developers to understand it in a fair amount of time, and allowing even inexperienced engineers to participate to Blockchain projects right away.

4.3.2 Simple and minimalistic

Python's philosophy is based on simplicity and minimalism. Many of its features contribute to its simplicity; for example, in Python, white spaces denote code blocks, and developers don't have to worry about using curly brackets or keywords. They can code a blockchain in Python

without needing to write a lot of code. Python, for example, enables the creation of a rudimentary blockchain in less than 50 lines of code.

4.3.3 Python is popular

Python's popularity is another quality that makes it a good choice for a Blockchain-based enterprise. If you look at this year's TIOBE index, you'll notice that Python is ranked third among all programming languages. And the popularity index shows that it is steadily increasing. In practice, this means you'll have no trouble assembling your project team because there are a lot of Python coders out there, including those with academic or scientific backgrounds. However, having ready access to Python specialists isn't enough.

4.3.4 Python can be run compiled or un-compiled

Python, unlike C++, is a scripting language that does not require compilation to be understood by computers, making the life of developers easier. Consider the scenario of running an application and discovering a flaw. If you're using a compiled language, you'll need to stop the application, go back to the source code, repair the problem, recompile the code, then resume it. You don't have to recompile code with Python; all you have to do is correct the error and reload your application. And that's a huge plus when it comes to creating blockchains. The performance of scripting languages can be harmed by translating code on the fly. That's why Python provides the option of pre-compiling code, as well as a variety of additional speed-up approaches, providing Blockchain developers a choice.

4.3.2.5 It has free packages for Blockchain

Another big benefit of utilizing Python in a Blockchain project is that it provides developers with a library of free packages to aid in the writing of code.

4.4 System Requirements and Implementation

Least framework necessity to make blockchain in E-Healthcare services framework is, the design boundaries are altered according to appraisal, for example, block size, block time, underwriting strategy, channel, asset distribution, and record information base and so forth. The reenactment PCs have the accompanying setups:

- 2 Core CPU (Intel Core i5 1.3GHz), or AMD Athlon CPU
- Minimum 3MB shared cache
- Minimum 4GB memory
- 1 Gbit/s network
- 120GB Solid State Drive (SSD)

Configuration has been varied according to the mining process increased on blockchain network, but minimum system requirements are above. Operating system used for creating a blockchain is Ubuntu 20.04 LTS.

We have created a blockchain using core python programming through which we implement our proposed algorithms for lab, clinician, patients and record assets. In code we use hashlib, pickle and random libraries of python. Hashlib module provides a standardised interface to a variety of secure hash and message digest methods. The SHA1, SHA224, SHA256, SHA384, and SHA512 secure hash algorithms (specified in FIPS 180-2) are included, as well as RSA's MD5 algorithm (defined in Internet RFC 1321). The phrases "message digest" and "secure hash" are synonymous. Message digests were the name for older algorithms. Secure hash is the modern phrase for it. The pickle module implements binary serialisation and de-serialization protocols for Python object structures. Pickling is the process of converting a Python object hierarchy into a byte stream, while unpickling is the process of converting a byte stream (from a binary file or bytes-like object) back into an object hierarchy. Pickling (and unpickling) is also known as "serialisation," "marshalling," 1 or "flattening"; nevertheless, the words "pickling" and "unpickling" are used here to avoid confusion. Random module implements pseudo-random number generators for various distributions. There is uniform selection from a range for integers. A method to construct a random permutation of a list in-place, as well as a function for random sampling without replacement, are all available for sequences.

We assigning different number of cpus to admin lab and clinician, in the peer network their transactions are smoothly executed with the following python script, transactions between the admin, lab and clinician secure using blockchain technology in the code, we first defined the previousBlockHash accrding to that our blockchain is going to operate the records, first nonce in the blockchain network initialized to 0, according to the transaction an array passed for Asset-Backed Securitization in blockchain network is from admin to clinician , lab to patient

and clinician to patient. For securitization of these assets using pickle dump nonce are implemented, for every transaction a unique hash generated by sha256.

```
import hashlib
import pickle
import random
block_header = {
   'previousBlockHash':
'effb6c85c6ee147a0f6813f1f6b6f12ffed373cef37a47cd59f4945427872f3d',
   'nonce': 0,
   'transactions': [
      {
         'from': 'Admin',
         'to': 'Clinician',
         'amount': 10
      },
      {
         'from': 'Lab',
         'to': 'Patient',
         'amount': 10
      },
      {
         'from': 'Clinician',
         'to': 'Patient',
         'amount': 10
      }
   ]
}
hashed_block = pickle.dumps(block_header)
m = hashlib.sha256(hashed_block)
difficulty_hash=
0x00FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
difficult_decimal=
45231284858326638837332416019018714005183587760015845327913118753091066265 5
admin = 3 * ['Patient']
patient = 5 * ['Clinician']
```

```
medical_record = 1 * ['record']
cpus = [admin, patient, clinician, medical_record]
miners = []
for cpu in cpus:
    miners.extend(cpu)
random.shuffle(miners)
while int(m.hexdigest(), 16) >= difficulty_hash:
    block_header['nonce'] += 1
    m = hashlib.sha256(pickle.dumps(block_header))
    print('Nonce Guess: ' + str(block_header['nonce']))
    print('Resultant Hash: ' + str(m.hexdigest()))
    print('Decimal value of hash: ' + str(int(m.hexdigest(), 16)) + '\n')
    miner = miners[block_header['nonce'] % len(miners)]
    block_hash = m.hexdigest()
print('Valid Hash: ' + str(int(m.hexdigest(), 16)) + ' is less than ' + str(difficulty_hash))
print('Miner who Mined Block: ' + miner)
```

CPU assigned to different assets, numbers of CPU can be varies according to requirement of network. Before mining process firstly cpu assigned to assets than chain code has implemented using hashlib sha256, block header generate for the assets. Results after execution of code demonstrated in the different figures according to the mined block over the blockchain network, as claimed by the algorithm. Mined Clinician Block on Blockchin is has successfully mined from administration to clinician and patient to clinician, display in figure 4.34.

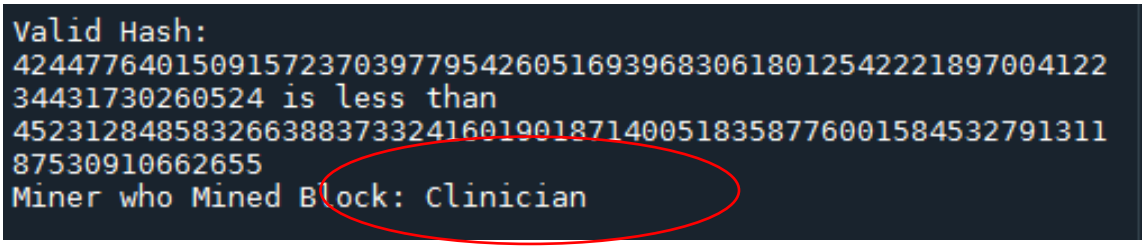


Figure 4.34: Mined Clinician Block on Blockchain

In figure 4.35 block is mined for Lab it hosted on the blockchain for patient and lab and lab to administrator. Information from patient to laboratory and from administrator to patient and laboratory block is mined with secure hashing.

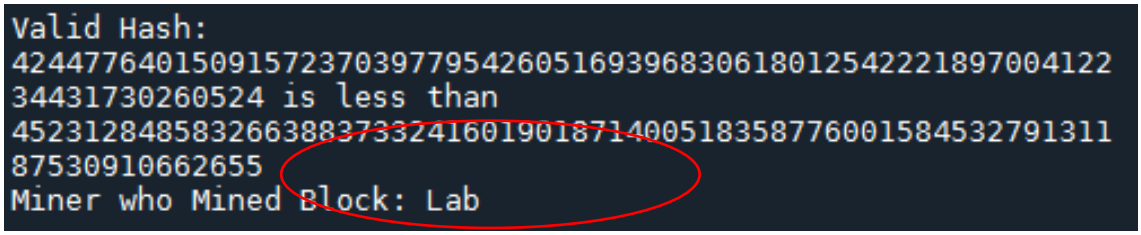


Figure 4.35: Mined Lab Block on Blockchain

Patients' information is one of the sensitive information on the network in e healthcare system after verification of hash using proof of work new block is mined for the patient is shown in figure 4.36. Block after successfully mined on the blockchain network.

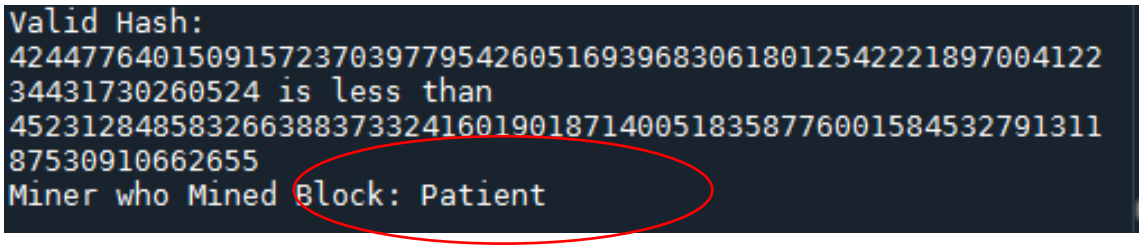


Figure 4.36: Mined Patient Block on Blockchain

In electronic healthcare system when new block for the whole record before storing to the database is mined on the blockchain network, figure 4.37 shows mined block for the record.

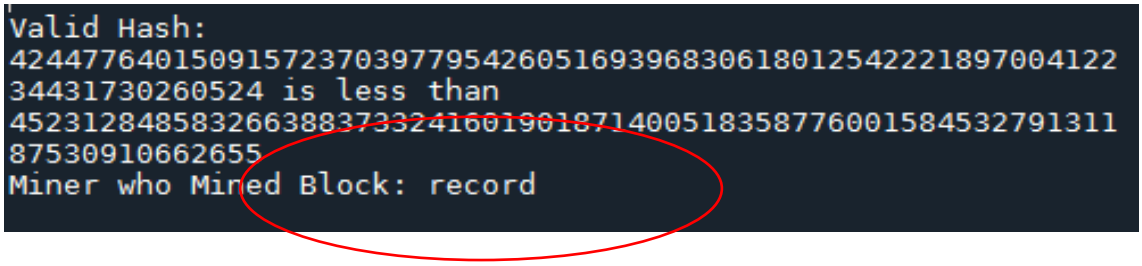


Figure 4.37: Mined record Block on Blockchain

4.5 Why Proof of work

Common consensus mechanisms include a workload proof mechanism (PoW), a rights proof mechanism (PoS), and a practical Byzantine fault tolerance mechanism (PBFT) [125]. PoW is a computationally intensive algorithm as well. It would be unfeasible for hospitals to build big computer centres solely to mine transaction data. We were astonished to see the PoW utilized so frequently for all of these reasons. We expected algorithms like proof-of-authority or proof-of-stake to be far more popular, as they address all of the previously mentioned PoW drawbacks of consuming more power than alternative consensus mechanisms. We have tested all the result after implement PoW, is more optimized that other consensus mechanism.

It would be extremely beneficial in providing high-quality personal healthcare if we could securely collect and preserve an individual's whole medical history, including every doctor's visit, on blockchain, where every data event is time-stamped and cannot be tampered with. Proof of labour makes selfish mining impossible.

There are numerous parameters that are classifying how POW is better than POS, and BFT. Parameters are Decentralization, Government intrusion, Security, Wealth maintenance, Economics all are explain in table 4.2.

Table 4.2 PoW Vs. PoS

A parameter of comparison	PoW	PoS
Decentralization	Tolerable	Risks of centralization
Governmental intrusion	Not possible	Possible
Security	Enhanced	Risks of breaches
Wealth maintenance	Controllable	Unpredictable
Economics	Solid	Questionable

In its Proof of Work algorithm, Hyperledger, for example, employs Practical Byzantine Fault Tolerance. Table 4.3 demonstrate comparison of PoW consensus and BFT consensus.

Table 4.3 PoW cosensus Vs. PoS consensus

Parameter	PoW consensus	BFT consensus
Node identity management	open, entirely decentralized	permissioned, nodes need to know IDs of all other nodes
Scalability (no. of nodes)	excellent (thousands of nodes)	limited, not well explored (tested only up to n ≤ 20 nodes)
Scalability (no. of clients)	excellent (thousands of clients)	excellent (thousands of clients)
Power consumption	Poor	Good

From explanation, it has been observed that PoW has capability to execute thousands of transactions with secure manner and excellent execution of clients.

4.6 Deployment Phase

Hyperledger fabric, a framework based on blockchain technology, and Hyperledger composer, its sandbox, are used to create the protocol. An EHR system is being proposed. Hyperledger is a blockchain-based initiative. The permission-based Distributed Ledger Technology is open source (DLT). It was created by the Linux Foundation to support a variety of applications. Multiple applications can be implemented using smart contracts and logic in the blockchain system. Hyperledger composer in which smart contracts created and tested using network visualization. It's a permissioned and consortium-oversaw blockchain, and that implies that all individuals are known to each other, it is totally free from even a hint of harm to guarantee that the organization. Since this structure isn't area explicit, it could be utilized to develop agreements and business networks utilizing Java, Go, Node.js, and different dialects. It also ensures safe communication between participants and organisations that employ the Crase Fault Tolerance (CFT) and Byzantine Fault Tolerance (BFT) protocols. Fault Tolerance (BFT)

is a consensus process that does not involve the use of a computer Mining will be more expensive.

For arrangement and introduction with hyperledger texture and arranger, "Docker" is utilized. Docker is a working framework compartment that a designer and additionally framework director can use. In the compartment, it tends to be utilized to make, convey, and run hyperledger-based applications or business organizations. It empowers the engineer to merge all conditions and functionalities into a solitary compartment. The hyperledger texture and arranger organization can be worked inside a compartment utilizing docker.

The entire framework is arranged into a network during the measurement phase. It displays the installation of the developed or experimental system with hyperledger dependencies on the primary host. The host's job during preparation is to run the EHR system that is linked to the calliper tool hyperledger environments. The calliper framework is used to set up the experiment's primary host during the second phase. The measurement setting is then left to the calliper and hyperledger hosts.During the measurement, all nodes are observed by installing Wireshark, which collects packets with tcp dump and the docker container's synchronised local loopback server. All packet and network visibility is gained by creating a pcap file. The nodes are finished. The Hyperledger fabric is made up of peers and orders as well as the Certificate Authority (CA).

Following the completion of the measurement, an experiment is carried out. Caliper and Hyperledger environments have been used in the virtualization of the node utilising Docker. The numerous trials are carried out in the calliper after configuring the pre-measurement script. The measurement collection, which includes all transaction data, is retrieved from the hyperledger calliper. After all of these stages have been completed, the system is evaluated. Spyder IDE, which runs on Anaconda Navigator, is used for evaluation. The Wireshark tool is also used to collect network data, which is saved in a pcap file that reads all TCP packets, sending times, source port, and destination port. For better visualisation, all network IPs have been substituted with the hyperledger calliper and peer organisation node names. All of the transactions that are executed during evaluation, such as transaction send rate, throughput, latency, organisations, peers, max CPU usage, and memory usage, are retrieved and then processed for transformation in the calliper report file of HTML. The data is then shown in a variety of ways using matlablib.

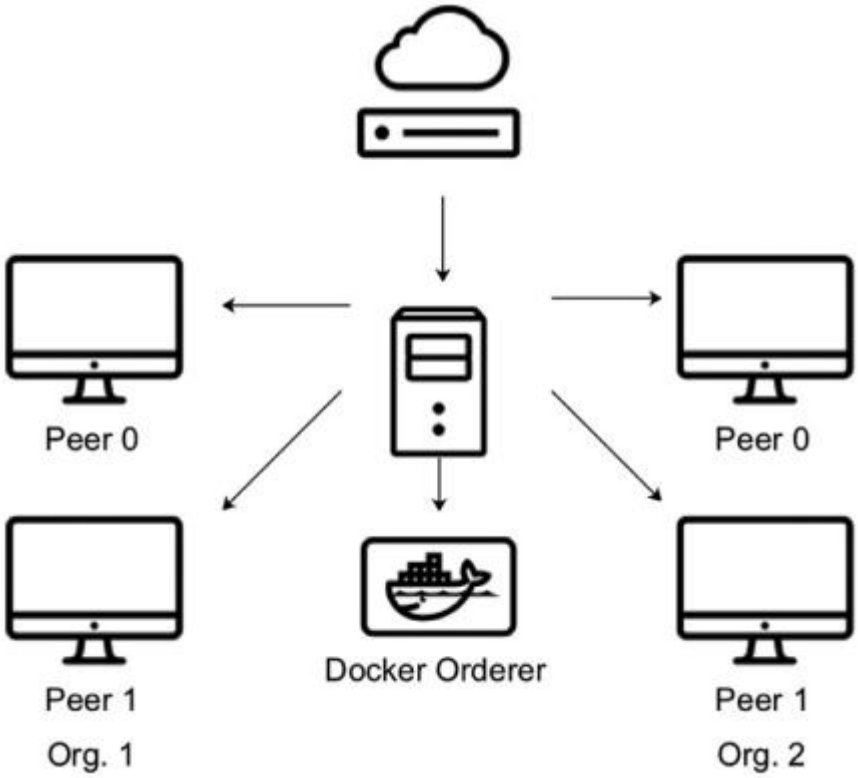


Figure 4.38: Network Structure

Several experiments are given in order to show the EHR system's functioning and to provide insight into the Hyperledger Fabric benchmarks for system evaluation. Several use scenarios are simulated in this study, including one organization vs. one peer, two organizations vs. one peer, three organizations vs. one peer, two organizations vs. two peers, and three organizations vs. two peers. Each organization in the network has a number of ledger peers, each of which holds a copy of the ledger. The formation of blocks is handled by a single orderer host, whereas the workloads are handled by the Caliper host. As a result, each host is a part of the star topology and performs the measurements and evaluations indicated in Figure 4.38.

In performance analysis, the proposed system is evaluated using simulation settings and evaluation methods. The effects of changing parameters like block size, endorsement policy, and block creation time are also examined. The data is presented in terms of performance delay, throughput, network capturing. Graph plots are used to show different scenarios with different configurations.

4.7 Simulation configuration

The Hyperledger calliper tool is a benchmarking tool for blockchain networks. Fabric, composer, sawtooth, iroha, and other hyperledger frameworks are among those that can be used. In this research, the calliper tool was used to test and execute the system's performance and various characteristics, including latency, throughput, CPU utilization, memory consumption, disc write/read, network I/O, and metrics for system evaluation. The assessment is used to alter the setup parameters, such as block size, block time, endorsement policy, channel, resource allocation, and ledger database. Configurations for the simulation computer systems is as follows:

- Intel core i5 processor (with 3-4 MB cache)
- 8GB RAM
- Minimum 320 GB Hard Disk Space
- 1 Gbit/s network

Hyperledger is an open-source program, can run on any platform like windows, MacOS and Linux. In our study Ubuntu 20.04 and windows10 operating system used. In the deployment phase study examine distinct scenario related to the execution of the transaction. The following are some of the observations that are taken into consideration for comprehension:

4.8 Basic experiment

Many observations are taken into account when assessing and evaluating the hyperledger platform of blockchain technology.

The first experiment is carried out using various inputs and involves five rounds of writing 1000 transactions into the ledger network at various rates of transactions per second consider as 50, 100, 150, 200, 250, and 500.

The transaction time reflects the performance of the blockchain network. In the network's atypical setup, Figure 4.39 illustrates multiple lines containing the time taken to successfully execute transactions.

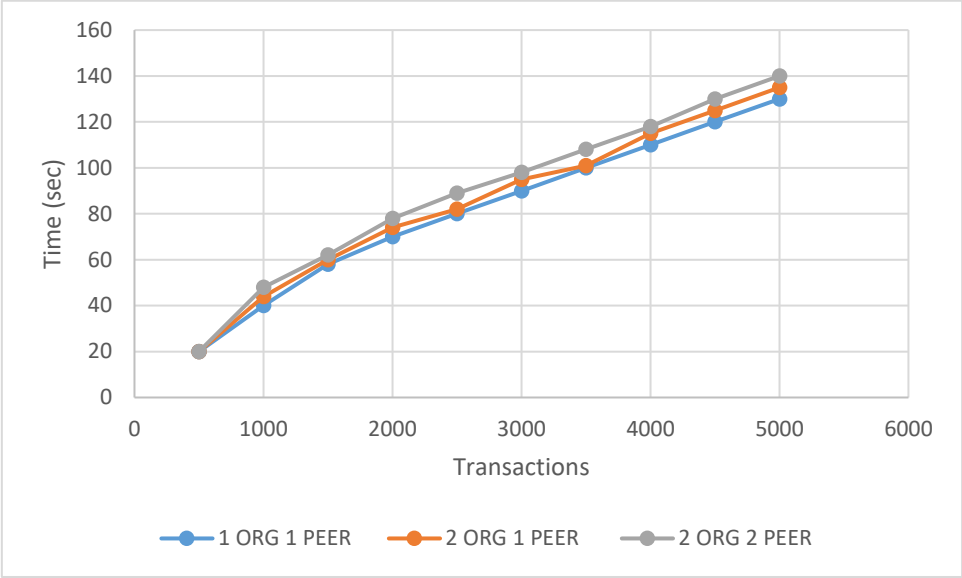


Figure 4.39: Time is taken to successfully execute transactions

1org1peer, 2org1peer, and 2org2peer represent different transaction performances. The results are calculated across five rounds, with each round consisting of 1000 transactions at various tps rates. It takes 140s for the 1org1peer to reach 5000 transactions. 2org1peer reaches 3000 transactions in 140s, but 2org2peer only reaches 2000 transactions in 140s. As a result, it's evident that as the number of organizations and peers grows, so does the amount of time it takes to complete transactions.

Transaction latency is calculated using a mathematical formula. Assume T_L stands for transaction latency, which is the time it takes to use the network. C_T is the transaction's confirmation time, which varies depending on the network threshold N_T. As shown in Table 4.4, in the blockchain network an S_T is the submit time for a transaction.

Transaction latency $T_L = (C_T * N_T) - S_T$

Table 4.4 Basic measurements

Parameters	Configurations
Transactions	1000 per round
Mode of Transactions	Read/ Write and config
Rounds	5
Rate	70 to 250 tps
Varied factor	----

Fig 4.40, fig 4.41, fig 4.42, fig 4.43 and fig 4.44 depicts the average latency of performance testing using the benchmark tool caliper report. Latency is displayed in seconds in this diagram. It represents the delay of communication and the success rate of writing transactions. 1org and 1peer offer significantly lower latency, 2org 1peer and 2org 2peer, on the other hand, lower throughput to 20 and 10 tps, respectively. This results in larger latency and communication gaps, allowing for better performance.

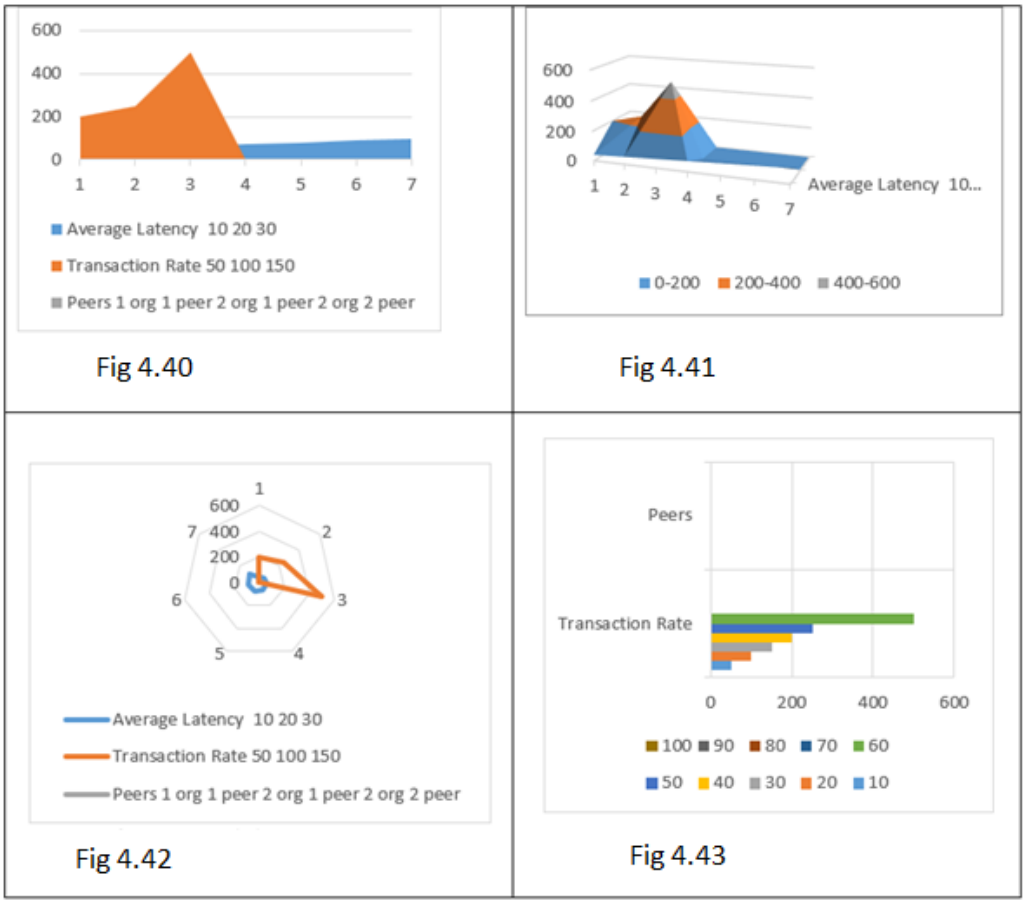


Figure 4.40, 4.41, 4.42, 4.43 The average latency of performance testing using caliper report

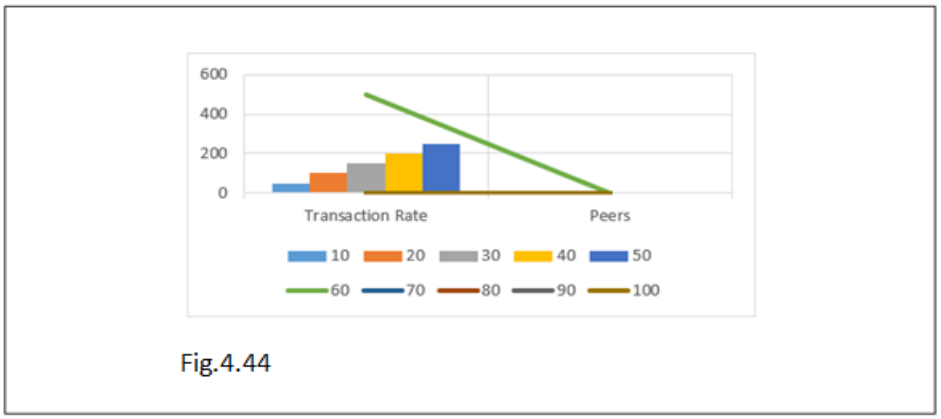


Figure 4.44 The average latency of performance testing using caliper report

4.9 Experiment with varying blocks

The optimization of the network is carried out in this experiment. Changing the block formation time measurement in the hyperledger calliper for EHR system produces different results. The arrangement of the caliper used in the experiment is shown in Table 4.5.

Table 4.5 Varied Block Time Measurements

Parameter	Configuration
Transactions	1000 per round
Transactions mode	Write
Rate	50 to 250 tps
Network size	2Org 2Peer
Varied Factor	Block Time
Endorsement Policy	2 of : {signed-by: {0, 1}}
Round	5

The transaction delay of the 2 org 2peer network architecture. In order to achieve the lowest feasible latency, the optimization criteria were taken into consideration. After increasing the endorsement policy block creation time, the calliper results default to block time. The result shows a 1.5x reduction in network latency, which helps to improve the performance of the EHR system. The minimal latency for a transaction rate of 50 is roughly 27 seconds, down from 52 seconds. There are 37s for 250 tps, which is a decrease from the 50s. This is a system performance that can be improved by changing the hyperledger network configuration.

Five rounds of reading/writing the transaction into the network of the ledger with 1000 transactions in each round at few rates of 100, 150, 200, 250,300 transactions per second.

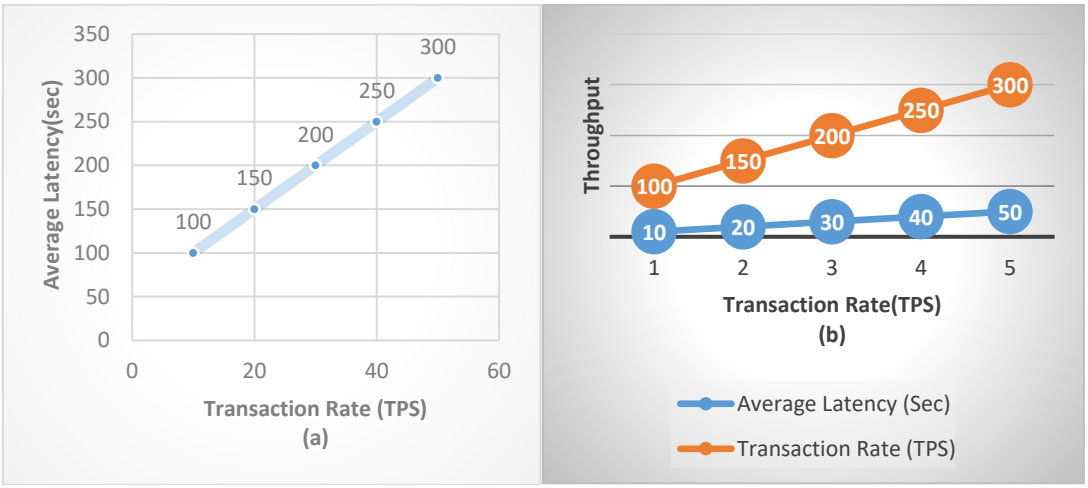


Figure 4.45: Transaction latencies with varying block time (a), (b) Transaction throughput with varying block time.

Figure 4.45 depicts transaction throughput (b). It shows how the network's policy affects block time, resulting in higher throughput and performance in terms of transaction committing time and success rate. Combining optimization increased overall throughput by 1.75x for 50 to 250 tps.

The read transaction mode reads the received transaction at a set interval of time. Table 4.4 shows the read transaction's setup. To increase the system's performance, the network's endorsement policy and block time for transaction reading have been altered. The optimization of the blockchain with varying block timings for building aids the reading or querying of transactions.

Figure 4.46 depicts the optimized performance in terms of transaction rate and latency. In terms of optimization, the system's latency has been reduced by 40%, which is a good outcome for total network performance. The default 250ms block time has a 9s average latency, whereas changing the policy and block time by 2s only has a 4s latency. The default block time for a max tps of 250 is 13s, but with the altered setup, the read latency drops to 6s.

Table 4.6: -Varied block time measurement with reading mode.

Parameter	Configuration
Rounds	3
Transactions	1000 per round
Transactions mode	Read
Rate	100, 200, 250 tps
Network size	2Org 2Peer
Varied Factor	Block Time
Endorsement Policy	2 of : {signed-by: {0, 1}}

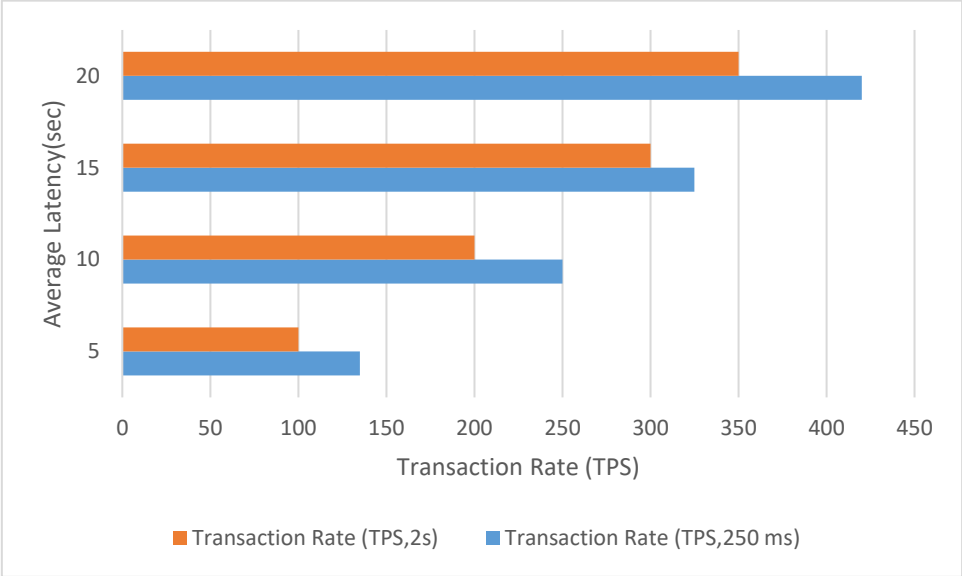


Figure 4.46: Optimized performance in terms of transaction rate and latency

4.10 Comparative analysis of consensus algorithms in blockchain

This section addresses the parameters that should be considered while considering blockchain consensus algorithms. The type of blockchain, transaction rate, scalability, and adversary tolerance model are all factors to consider. Latency, throughput, bandwidth, and experimental setup assaults, communication model, communication complexity mining, energy usage, consensus category, and Finality of the consensus has been recognized as critical parameter for comparing the various blockchain consensus algorithms.

In implement phase of our study, we used two consensus mechanisms. POW and plugged PBFT in Hyperledger fabric. In a comparative analysis, it has been observed that POW is good but only suitable for cryptocurrency transactions. Another limitation of using POW is, it consumes high power for executing transactions. PBFT is the best approach that we used for secure E-Healthcare data using Hyperledger fabric. Table 4.7 shows performance using PBFT consensus mechanism.

In our study, we utilized the Hyeprledger caliper tool to evaluate the performance. The proposed scheme enhances the performance of blockchain with the proposed algorithms, and the latency may also be reduced using the proposed technique, according to the results. This demonstrates that, like the steam engine and the Internet, Blockchain has the capacity to bring about profound change for humanity's advancement.

- Transaction throughput
- Transaction latency (minimum, maximum, average)
- Resource consumption (CPU, Memory, Network IO, …)

Table 4.7: -Performance metrics using PBFT.

Type	Name	Memory (avg)	CPU (avg)	Traffic In	Traffic Out	Disk Write
Docker	peer1.org1.example.com	266.0 MB	15.70%	3.1MB	512.25KB	7.4MB
Docker	Peer0.org1.example.com	205.2 MB	24.25%	5.2MB	3.5MB	7.4MB
Docker	Peer0.org2.example.com	202.0 MB	27.95%	6.2MB	4.6MB	7.4MB
Docker	peer1.org2.example.com	224.1 MB	15.25%	4.1MB	498.2KB	8MB
Docker	orderer.example.com	56.9 MB	4.05%	3.9MB	16.52MB	5MB

Applications can be created, distributed, and run using the open-source Docker platform. In order to swiftly release software, Docker enables you to divide your applications from your infrastructure. Hyperledger used built in docker images for create distinct peers. Experiment contains five different peers as shown in Table 4.7. Using PBFT consensus mechanism average memory used by the different peers is fluctuates according to hosting process of Hyperledger caliper and a network configuration file including information on the machine being tested and network connection specifications. Org endure for organization, org1 and org2 are organization 1 and organization 2 respectively that connected with the peer of networks. In the PBFT

performance metrics every time when network peer hosted with any one of the organization memory, CPU, traffic in, traffic out and disk write reports generated using Hyperledger caliper. In peer1.org1.example .com average memory used 266.0 MB but after hosted next peer peer0.org1.example .com and peer0.org2.example .com peer1 hosted again and now it uses less memory from first time hosting that is 224.1 MB. peer0.org1.example .com and peer0.org2.example .com hosted one after other in continuous approach so these occupied memory 205.2 MB and 202.0 MB respectively, CPU utilization for both is 24.25% and 27.95%. In the case of traffic in and out that are circumstances where nodes connected and transfer data over the network. As per the transaction results varies, in our experiment five rounds of transactions fired in the system from different peers and organizations as measured in the KB and MB. In peer1 for organization 1 traffic in 3MB and traffic out is 512.25 KB disk write used for transactions are 7.4 MB. In peer0.org1.example.com 5.3MB traffic in and 3.5MB traffic out disc write 7.4 MB.

Many distributed blockchains, including Ethereum and Bitcoin, are permissionless, allowing every node to take part in the consensus process that organises and groups transactions into blocks. These systems rely on probabilistic consensus techniques as a result, which finally guarantee ledger consistency with a high degree of probability problem called fork but are still susceptible to divergent ledgers. Contrarily, Hyperledger Fabric operates. It has an orderer node, also referred to as an "ordering node," which performs this transaction ordering and, along with other orderer nodes, creates an ordering service. Any block approved by the peer is certain to be final and accurate because Fabric's design depends on deterministic consensus procedures. In contrast to many other distributed and permissionless blockchain networks, ledgers cannot fork [125]. Orderer.example.com acts as a service metric utilized 56.9 MB memory 4.05% of CPU, traffic in and traffic out was respectively3.9MB and 16.25 MB. Disk write is 5MB for handling the transactions.

The following algorithms are presented in relation to them.

4.8.1 Blockchain Type- Public, private, and consortium blockchain are the three categories. The membership control in the consensus algorithm is determined by the blockchain type. This must be taken into account when analyzing consensus algorithms to determine what type of membership is assumed in the design. The sort of blockchain to use depends on the nature of the business application.

4.8.2 Scalability – In today's climate, scalability is a must when dealing with massive data. When the number of nodes is increased, more transaction blocks are handled, resulting in scalability. ELASTICO and proof of trust are both scalable. Implicit consensus and proof-of-work aren't scalable. Other algorithms that are used in comparisons have not yet been evaluated for scalability.

4.8.3 Adversary tolerance model- The adversary model determines the percentage of the blockchain network that can sustain failure or attack without compromising consensus. The suggested method for blockchain consensus includes a threshold value for this attacker scenario. A higher enemy threshold value is preferable. ELASTICO outperforms the other algorithms in terms of adversary control.

4.8.4 Performance related parameters- Some existing consensus techniques have not been tested experimentally. Only theoretically, using soundness proofs, are they compared. However, a quantitative examination of the performance and security of these consensus methods is also required. For each of the consensus algorithms, the three fundamental performance elements that must be focused on are latency, throughput, and bandwidth. Other algorithms, with the exception of ELASTICO, are not experimentally assessed in terms of these performance factors.

4.8.5 Communication model and complexity- The sender waits for the recipient to acknowledge the request in synchronous communication. Asynchronous communication eliminates the requirement for the sender to wait for a response from the recipient before continuing the conversation. PoW, PoT, Ripple, and implicit consensus can be explored for real-time applications that cannot afford delays. If an application is going to have a lot of read operations, the synchronous model should be used because it responds quickly. The synchronous communication paradigm is assumed in the design of ELASTICO and the leader free consensus method. Compared to ELASTICO and PoT, the leader free consensus algorithm has a linear and lower communication cost. The rest of the algorithms' communication costs are yet to be studied in the literature.

4.8.6 Attacks – Ripple is vulnerable to the Sybil attack, in which a single attacker creates many IP addresses, virtual machines, and user identities to control multiple network nodes. Leaderless consensus and PoT are safe from this attack. The algorithms are not assessed or analysed in terms of the number of probable security threats in a blockchain network. In terms of security assaults, it's critical to review the algorithms.

4.8.7 Energy consumption- The term "energy consumption" describes how much energy is used. The amount of power or energy that the hardware consumes in the blockchain network, infrastructure is used. The almost all of the consensus's energy consumption algorithms hasn't been put to the test.

4.8.8 Mining and consensus category- It specifies how the mining operation in the blockchain network is carried out. It has a lot to do with how the verification process works. For networks with a large number of nodes, proof-based consensus is optimal. On the other side, vote-based consensus works best with a small number of nodes. If the network has a high number of nodes, ELASTICO, PoW, PoPF, and implicit consensus are the best options. In that situation, the remainder of the consensus procedures (which are more complicated) would be the best fit.

4.8.9 Consensus finality- The term "finality" in blockchain refers to the fact that a transaction has been completed and will not be reversed. It's a crucial factor to consider while creating a blockchain consensus mechanism. The two types of consensus finality are probabilistic finality and absolute finality. In probabilistic finality, the risk of a block reversing reduces as it moves deeper into the chain. In absolute finality, however, a transaction is completed instantly when it is added to the blockchain. ELASTICO, PoPF, and implicit consensus are recommended consensus versions if absolute consensus finality is desired.

4.11 Comparative analysis of proof of work and PBFT

Proposed work implemented using proof of work and PBFT, PBFT consensus mechanism is used in Hyperledger fabric that is used for final implementation of proposed work. Comparison between proof of work and PBFT has been done according to our implementation. Comparison of consensus mechanism proof of work and PBFT as per implemented experiment. The values mentioned in the table – are collected from spyderIDE profiler when proof of work has implemented and collected from Hyperledger caliper tool in PBFT mechanism. From the values reported below, PBFT seems to achieve the highest throughput with over 10,000 transactions per second. Comparison done on the basis of properties that are blockchain type that express which type of blockchain used by consensus mechanisms. Trusted model that expresses the model deployed using consensus is trusted. Scalability, a crucial factor in blockchain networks, refers to a network's ability to support higher transaction throughput. Scalability is therefore essential for Blockchain's further development. Scalability property used in comparison which is high scalable in blockchain. Throughput refers to the number of transactions execute in blockchain. Fault tolerance is another property used for comparison because if a distributed system, like a blockchain network, can generate consensus on important issues even in the presence of unreliable or malicious network participants, it is considered to be byzantine fault-tolerant. Last property used for comparative analysis is energy efficient.

Table 4.8: - Comparison of proof of work and PBFT.

Properties	**Proof of Work**	**PBFT**
Blockchain Type	Permissionless	Permissioned
Trust Model	Untrusted	Semi trusted
Scalability	High	Low
Throughput	<10	<10,000
Fault Tolerance	50%	30%
Energy Efficient	No	Yes

There are a variety of characteristics that may be used to assess a consensus algorithm's functionality, performance, and security. But as the execution and deployment phase of study, it has been observed with the results with pluggable PBFT consensus mechanism with

Hyperledger fabric more reliable for transfer secure data as comparison of PoW consensus of bitcoin. Blockchain has the potential to alter the way we think about healthcare applications by allowing for automated data collection, the elimination of third parties, a trustless system, and data protection. The suggested network does not have to worry about single-point failure because it is a decentralized network. The system architecture for healthcare applications using blockchain has been implemented in our study, along with algorithms (Algorithm 1,2,3,4) for user access control. This thesis also includes the implementation of a blockchain that employs EHR, for which we employed the Hyperledger Fabric blockchain.

Deep dive observations for PBFT that express it is better than proof of work. PBFT works on permissioned blockchain where anonymous entries restricted, only those transactions are part of the network which are already validate from the administrator rest all the activities which may be malicious blockchain will kick them out from the network. Proof of work is untrusted whereas PBFT is semi-trusted and more secure. In the compression of transaction through PBFT execute more transaction as compared to proof of work. Proof of work is not energy efficient; it consumes very high power for solve mathematical puzzles on which it works for providing the security to transactions. It is measure by our experiment while using proof of work. PBFT consume less power because energy utilization is reduced as hashing energy is not required to enter the next block.

CHAPTER 5

FINDINGS, CONCLUSION, AND RECOMMENDATIONS

5.1 Findings of the study

This chapter summarizes research findings, recommendation and conclusion of present research titled “Design and implementation of security framework for e- healthcare using block chain technology." The research findings are followed by conclusion and recommendation and it provide important aspects and feedback about four different objectives of research i.e., collect and analyze E-healthcare data of tertiary hospitals of Punjab, model security framework for hospitals having E- health care setup to record data, propose and implement consensus algorithms on E healthcare data and compare proposed algorithm with existing algorithm. Tertiary hospitals of Punjab use E-healthcare system for store transactions. Trillions of transactions proceed hourly E-healthcare system, sometimes noticed that many third-party vendors like insurance companies, laboratories, and clinician's access one shared data base on whole network from one peer to other peer on the network. The healthcare industry has unique security and privacy risks as a result of additional regulatory obligations to protect patients' medical information. As cloud storage and the use of mobile health devices expand the sharing of records and data in the Internet age, the risk of hostile attacks and the possibility of private information being compromised increases. As health information becomes more accessible via smart devices and people visit multiple doctors, data sharing and privacy are becoming more of a concern. Authentication, interoperability, data sharing, medical information transfer, and issues about mobile health are just a few of the unique problems that the healthcare business faces. Academics, industry, and governments all across the world have recently expressed interest in blockchain technology. It is considered a technological advancement with the potential to disrupt a wide range of application industries, affecting many parts of our lives. The sky-high expectations for its potential have driven a large-scale inquiry into its use in a variety of industries.

Due to the popularity of blockchain, numerous potential blockchain applications in the healthcare industry, such as electronic health record (EHR) systems, have been presented. As a result, we conduct a comprehensive literature evaluation of blockchain techniques built for EHR systems in this research, focusing solely on security and privacy issues. Prior to analyzing

the (possible) applications of blockchain in EHR systems, we introduce necessary background knowledge relating to both EHR systems and blockchain as part of the assessment. A number of research difficulties and opportunities are also identified. In our study we find many problems in electronic health record in the e healthcare system of Punjab is security there are many parameters presented under that constraint like unauthorized access, data confidentially etc. In tertiary hospitals of Punjab many transactions execute online, but there is not any security aspect used for secure transactions.

Different Blockchain concentrates on mean to address recordkeeping challenges, like more prominent patient command over touchy wellbeing data, and the primary discoveries introduced in our review incorporate the significance of acknowledging EHR interoperability through medical care supplier reception of Blockchain and the meaning of open norms. Due to health data exchange, availability, and integration, they could be critical for improving health care services. Furthermore, the usage of Blockchain technology in clinical studies could improve EHR transaction security.

The utilization of blockchain in healthcare frameworks assumes a basic part in this healthcare industry. It can bring about robotized information assortment and check processes, right and accumulated information from different sources which are changeless, alter safe and give got information, with a diminished likelihood of cybercrime. It additionally upholds conveyed information, with overt repetitiveness and adaptation to non-critical failure of the framework. The present issues that the healthcare industry faces are examined in this study. To provide privacy and security for patient data in the EHR system, we suggested a system architecture and algorithm for access control policy for participants. In addition, the implementation of a blockchain-based EHR sharing system is described. The suggested effort eliminates the system's central authority as well as a single point of failure. Immutable ledger technology ensures system security since no user can alter the ledger. The performance of the proposed system is tested using the caliper by configuring block size, block formation time, endorsement policy, and recommended optimization for evaluation metrics like as latency, throughput, and network security for better results. The proposed system’s performance is increased by 1.95x and its latency is reduced by 2.0x by optimizing its performance. This demonstrates the blockchain’s utility and importance in a variety of fields, demonstrating that it has the potential to be the next revolutionary technology to replace present healthcare systems.

5.2 Conclusion

- During the assessment of existing system, it had been observed that major purpose of e healthcare system is of data entry and record keeping

  During in-depth interviews of hospital administrators it had been observed that hospitals that are using E healthcare mostly they are using it for data entry and record keeping as when question related to data analysis is asked from hospital administrators 43.7 percent said that they use basic data analysis to fetch information related to total patients visits weekly and monthly , patients visit doctor wise weekly and monthly and disease wise data analysis they are doing in order to find out which area is infected with what type of disease and 47.9 percent said that they are using data analysis mostly as reporting tool but it was not there routine task to analyze data ,When any higher official ask then they make report for them and 8.4 percent said that they are not using any type of analysis and only third party and policymakers are analyzing data they are into collection phase only .Those who replied that they are analyzing data for different purposes most of them are using Microsoft excel as reporting tool to create graphs and present data to their peers whenever required ,Few of them said about usage of tableau and power BI but not at very advance stage .The system they are using for data entry have some features which can create different graphs and charts of different attributes with which they are analyzing data and that graphs are sufficient for them as they said for data analysis .

- While accessing the existing e healthcare model of tertiary hospitals of Punjab. It had been seen that mostly client server architecture is used for online transactions.

  Maximum of the hospitals used online system for registration of patients. Transaction directly sent to data base after data entry, there is no security provided on the transactions. Due to which data travelled from different transactions is not secure due to use of client server architecture. Common security issues in e healthcare in particular confidentiality, authorization, integrity, data theft immense problem in traditional healthcare system of Punjab.
- Data availability, privacy and security main issues found in client server architecture.

After gathering information from respondent's study found shortcoming in existing system for perform transactions and storing data. It had been analyzing for healthcare system of Punjab from data collected and discussion with administration officers that, in Punjab client server architecture is used for making transactions, data from one node to other node is directly send without any encryption, due to which each record is simply travelled with the clear information that is easily available for all of the sources in the data base even though it is accessed by the others in clear format.

- Proposed research used blockchain technology for secure e healthcare system of tertiary hospitals of Punjab.

  Blockchain is a very promising technology that allows for a distributed, safe, and private environment between peers without the use of a reliable third party. Blockchain is capable for encrypt data in the transaction using secure hash algorithm SHA-256 used for cryptographic security. For exchange information over the network in hospitals we have implemented a secure blockchain network.

- Consensus mechanism is back bone of transaction security in blockchain.

  We have implemented proof of work and PBFT consensus mechanisms. In execution it has been observed after implementation that PBFT is best consensus mechanism for secure transactions in E- healthcare system.

In conclusion, research work meets its objectives of design and implementation of security framework for e- healthcare using blockchain technology, the semantic representation ensures that health data from various sources can be smoothly combined and shared when needed. The study effort uses standardized medical vocabulary and universal identifiers to define the semantic EHR's essential information. The patient can engage in the utilization of his or her own health data thanks to the EHR framework. The EHR is easily accessible to health-care providers for the primary aim of providing efficient and ongoing patient care. After implementation blockchain security framework in e healthcare. All transactions are recorded on the Blockchain. Every transaction's date, time, participants, and amount are recorded in the register. Each node in the network has a complete copy of the Blockchain, and the transactions are confirmed by the Bitcoin miners who keep the ledger using cryptographic principles. These principles also ensure that these nodes agree on the current state of the ledger and every

transaction in it automatically and constantly. If someone tries to tamper with a transaction, the nodes will be unable to establish a consensus and thus refuse to accept the transaction into the Blockchain.

Blockchain has the potential to alter the way we think about healthcare applications by allowing for automated data collection, the elimination of third parties, a trustless system, and data protection. The suggested network does not have to worry about single point failure because it is a decentralized network. The system architecture for healthcare applications using blockchain is proposed in this study, along with algorithms for user access control. This thesis also includes the implementation of a blockchain that employs EHR, for which we employed the Hyperledger Fabric blockchain. As results of this study shows, blockchain has a ton of potential for altering the customary medical services industry. While endeavoring to totally incorporate blockchain innovation with existing EHR frameworks, nonetheless, various examination and functional obstacles remain. From that point onward, we found an assortment of conceivable review subjects, for example, IoT, large information, AI, and edge registering. We trust that this exploration will help in better comprehension of the turn of events and sending of cutting edge EHR frameworks that will help our general public.
The semantic model used in this study makes integration easier without imposing requirements on stakeholders. Consolidating EHR data can aid in the creation of illness registries for improved public health. For analysis and research, the unified data would necessitate big data approaches. Data from wearable sensors and smart phones can be easily linked into the EHR for real-time analysis.

In terms of transparency, historically, the prevailing philosophy for protecting health-related data in the healthcare industry has been to keep records out of the hands of anyone who isn't directly involved in the patient's care. The Blockchain privacy approach makes data records generally available, but the patients to whom they pertain are either anonymous or private. The goal of this study was to determine the scope of blockchain's application in the healthcare industry. The findings were utilized to synthesize existing information on block chain's implementation in the healthcare industry, as well as past and current topical trends in academic research in this field. Future research directions have been offered using a synthesized framework created by combining ideas from existing constraints, recommendations, and emerging gaps in current knowledge discovered throughout this evaluation.

Based on the findings we believe that Blockchain technology could be a future suitable solution for common problems in the healthcare field, such as EHR interoperability, establishing sharing trust between healthcare providers, auditability, privacy, and allowing patients to choose who has access to their health data. However, because a patient's health data is personal, highly sensitive, and vital information, further research, trials, and experiments are needed to verify that a secure and established system is developed before adopting Blockchain technology on a broad scale in healthcare. Decentralization, immutability, transparency, and traceability are some of the qualities of blockchain that make it a feasible sharing and storing tool in the healthcare domain. Scalability difficulties, interoperability, a lack of technical competence, security, and authorization are all concerns to blockchain technology's use in the healthcare profession. As there is a void in research directing healthcare organizations to use blockchain design types such as public, private, and hybrid, it is critical to present evidence relating to distinctions between each blockchain design in future work.

Following are the wider scope of implementing blockchain in healthcare:

- For recordkeeping blockchain technology provide a secure way for transaction with the help of consensus mechanism.
- Blockchain provide digital version of patient's paper-based records, which can be accessed from anywhere on the network.
- Using blockchain patient data management sharing process is free from attacks and hacker.
- In tertiary hospitals, numerous branches working on one patient record. By implement blockchain numerous branches of hospitals securely works on patients records with transparency.

5.3 Recommendations

Security is a significant issue in the healthcare industry. Somewhere in the range of 2009 and 2017, a larger number of 176 million patient records were uncovered in information breaks. The culprits took charge card and banking data, as well as wellbeing and genomic testing records. Our study propose framework which is having ability to keep an incorruptible, decentralized and transparent log of all patient data that makes it a important for security applications. Our study proposes Blockchain application that optimized specifically for the

healthcare industry, helping protect patient health data when transporting it. This study proposes decentralized nature of the environment of patient information that can be rapidly and proficiently referred to by specialists, clinics, drug specialists, and any other person associated with treatment. Along these lines, the blockchain can prompt quicker analyze and customized care plans.

- **Implement Blockchain to secure E healthcare in tertiary hospital of Punjab**

Blockchain is now one of the most secure data protection solutions available. Rapid improvements in digital technology have resulted in new data security challenges. Organizations must employ robust authentication and cryptographic key vaulting techniques to secure their data. To secure E healthcare data and their transaction blockchain is superlative tool that should be implemented.

- **Use of Consensus Mechanism for implementing Transactions**

Blockchain is a distributed decentralized network that enables immutability, privacy, security, and transparency, as we all know. Despite the lack of a central authority to validate and verify transactions, the Blockchain considers each transaction to be completely secure and verified. This is only feasible because of the consensus protocol, which is an essential component of any Blockchain network.

A consensus algorithm is a method through which all peers in a Blockchain network reach a consensus on the current state of the distributed ledger. Consensus algorithms achieve blockchain network resilience and create trust amongst unknown peers in a distributed computing environment in this way. In essence, the consensus protocol ensures that every new block added to the Blockchain is the one and only version of the truth that all nodes in the Blockchain agree on. The Blockchain consensus protocol has several specific goals, including reaching an agreement, collaboration, co-operation, equal rights for all nodes, and each node's mandatory participation in the consensus process. As a result, a consensus algorithm seeks to identify a common ground that benefits the entire network.

Our research work recommendation PBFT consensus mechanism with Hyperledger fabric for providing security to the transactions in tertiary hospitals of Punjab. The next block

generation's miner is chosen using this consensus algorithm. The main goal of consensus mechanism in healthcare transaction to provide security on different peer.

- **Providing Security and privacy in healthcare transactions in tertiary hospitals of Punjab**

There are numerous transactions performed every second in in a healthcare system of Punjab. To secure these transactions our study designs a security framework to provide security and privacy in healthcare transactions through blockchain technology. In our study we identified that there are different types of and completed transactions stuck on different networks or on health care system, research work recommendation blockchain technology with consensus mechanism for secure transactions from patients, doctors, clinicians and laboratory.

There are inventive uses of Blockchain in medical services because of intrinsic encryption and decentralization. It upgrades the security of patients' electronic clinical records, advances the adaptation of wellbeing data, further develops interoperability among medical services associations, and helps fake battle medications. Different medical services fields can change with Blockchain innovation; regions like medical services, advanced arrangements permitted by keen agreements comprise one of Blockchain's most basic applications.

In the future scope of our study, research can be carried out in advancement of IoT (internet of things) and AI (artificial intelligence) integration using blockchain technology. The Internet of Things (IoT) and artificial intelligence has recently emerged, bringing with it a whole new class of applications and increased efficiency for existing service sectors. The healthcare industry is one major service that is attempting to profit from IoT. These Healthcare IoT applications face additional obstacles due to application-specific needs, as well as device connectivity and communication capabilities. Artificial intelligence integrated with IOT can be used to improve electronic healthcare records. Mobile applications can be connected to AI based data driven systems through IOT, using this technique data collected from sensors and AI techniques can be used for data analysis, reporting, decision making using blockchain based secure networks. Moreover, healthcare efficiency is very important aspect in developing nations where healthcare facilities are not appropriate in number as prescribed by WHO guidelines. Data envelopment analysis is non parametric technique to assess efficiency of organization and many researchers are presently working on to assess healthcare efficiency using DEA using slack based models. Furthermore, there is an increasing demand for people to have access to

and control over their data as patient involvement in healthcare rises. Electronic health records (EHRs) could be managed effectively using blockchain, a secure, decentralized online ledger, which has the potential to enhance health outcomes. Data envelopment analysis in future can be used by policy makers and administrators to evaluate performance of blockchain technology specifically in healthcare sector to optimize system performance and to compare the performance of blockchain systems with various consensus models.

REFERENCES

[1] Shekh Jahid, Zuber Farooqui, "Temporal Blockchain Approach based Secure Ehealth Framework", International Journal of Computer Applications, Volume 174 – No. 28, April 2021.

[2] Ozair FF, Jamshed N, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. Perspect Clin Res. 2015 Apr-Jun;6(2):73-6. doi: 10.4103/2229-3485.153997. PMID: 25878950; PMCID: PMC4394583.

[3] Kaddoura, Sanaa & Grati, Rima. (2021). Blockchain for Healthcare and Medical Systems. 10.4018/978-1-7998-5839-3.ch011.

[4] "Indian Medical Services", https://indiamedicalservices.org/ (Accessed Sep. 2021)

[5] Pal, DK & Pal, D. & Tiwari, R. & Kasar, Pradeep & Sharma, Arvind & Verma, S. & Gautam, P. & Jain, Y. & Bansal, M.. (2007). Functioning of the Sub Health Centers (SHCs) in Mandla District.

[6] Luxon L. Infrastructure - the key to healthcare improvement. Future Hosp J. 2015 Feb;2(1):4-7. doi: 10.7861/futurehosp.2-1-4. PMID: 31098066; PMCID: PMC6465866.

[7] T. D. McFarlane, B. E. Dixon, and S. J. Grannis, ‘‘‘Client registries: Identifying and linking patients,’’ *in Health Information Exchange: Navigating and Managing a Network of Health Information Systems*, B. Dixon, Ed., 1st ed. Indianapolis, IN, USA: Elsevier, 2016, pp. 163–182.

[8] "National Institution for Transforming India", http://social.niti.gov.in/hlt-ranking (accessed Jun. 5, 2020).

[9] "Primary Health Centers", https://pib.gov.in/PressReleasePage.aspx?PRID=1656190 (accessed Sep. 20, 2020)

[10] "HealthFrog", https://www.healthfrog.in/hospital/list/punjab (accessed Jun. 5, 2020)

[11] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ *J. Gen. Philosophy Sci.*, vol. 39, no. 1, pp. 53–67, 2008, doi: 10.1007/s10838- 008-9062-0.

[12] Bahuguna P, Mukhopadhyay I, Chauhan AS, Rana SK, Selvaraj S, Prinja S. Sub-

national health accounts: Experience from Punjab State in India. PLoS One. 2018 Dec 10;13(12):e0208298. doi: 10.1371/journal.pone.0208298. PMID: 30532271; PMCID: PMC6287852.

[13] "EHR (electronic health record) vs. EMR (electronic medical record)", https://www.practicefusion.com/blog/ehr-vs-emr/

[14] Tsai, Flora. "Security Issues in E-Healthcare ". Journal of Medical and Biological Engineering. (2010). 30.

[15] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst. 2017 Aug;41(8):127. doi: 10.1007/s10916-017-0778-4. Epub 2017 Jul 21. PMID: 28733949; PMCID: PMC5522514.

[16] National Research Council (US) Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the Record Protecting Electronic Health Information. Washington (DC): National Academies Press (US); 1997. 4, Technical Approaches to Protecting Electronic Health Information. Available from: https://www.ncbi.nlm.nih.gov/books/NBK233433/

[17] Ismail Keshta, Ammar Odeh, "Security and privacy of electronic health records: Concerns and challenges", Egyptian Informatics Journal, Volume 22, Issue 2,2021,Pages 177-183,https://doi.org/10.1016/j.eij.2020.07.003.

[18] H. Wang, Y. Song, Secure cloud-based EHR system using attribute-based cryptosystem and blockchain, J. Med. Syst. 42 (8) (2018).

[19] Zarour M, Alenezi M, Ansari MTJ, Pandey AK, Ahmad M, Agrawal A, Kumar R, Khan RA. Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett. 2021 Apr 16;8(3):66-77. doi: 10.1049/htl2.12008. PMID: 34035927; PMCID: PMC8136763.`

[20] Pai, M.M.M., Ganiga, R., Pai, R.M. et al. Standard electronic health record (EHR) framework for Indian healthcare system. Health Serv Outcomes Res Method 21, 339–362 (2021). https://doi.org/10.1007/s10742-020-00238-0

[21] Raposo VL. Electronic health records: Is it a risk worth taking in healthcare delivery? GMS Health Technol Assess. 2015 Dec 10;11:Doc02. doi: 10.3205/hta000123. PMID: 26693253; PMCID: PMC4677576. C. Agbo, Q. Mahmoud, and J. Eklund,

‘‘Blockchain technology in health- care: A systematic review,’’ Healthcare, vol. 7, no. 2, p. 56, Apr. 2019.

[22] H. Jin, Y. Luo, P. Li, and J. Mathew, ‘‘A review of secure and privacy- preserving medical data sharing,’’ IEEE Access, vol. 7, pp. 61656–61669, 2019.

[23] B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 699-703, doi: 10.1109/ICACCS.2019.8728483.

[24] Number of register doctor in india from 2010 to 2020, https://www.statista.com/statistics/605347/india-registered-doctors-medical-council/

[25] Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for healthcare 4.0 environment: opportunities and challenges. Comput Electr Eng 2018;72:1–13.

[26] Y. Yuan and F. -Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421-1428, Sept. 2018, doi: 10.1109/TSMC.2018.2854904.

[27] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. Habits: Blockchainbased telesurgery framework for healthcare 4.0. 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). 2019.p.1–5. https://doi.org/10.1109/CITS.2019.8862127.

[28] “A timeline and history of blockchain technology”, https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

[29] Savva Shanaev, Arina Shuraeva, Mikhail Vasenin and Maksim Kuznetsov,” Cryptocurrency Value and 51% Attacks: Evidence from Event Studies”, The Journal of Alternative Investments Winter 2020, 22 (3) 65-77; DOI: https://doi.org/10.3905/jai.2019.1.081

[30] Mahajan UV, Wafapoor V, Mahajan OA, Anderson WS. Use of Patients' Protected Health Information to Solicit Hospital Funds: How did This Practice Come About? J Patient Exp. 2022 Jun 7;9:23743735221106604. doi: 10.1177/23743735221106604. PMID: 35694011; PMCID: PMC9185007.

[31] Sudhakara, H & T., Rajendra Prasad. (2016). “Healthcare Expenditure in India -An Analysis, “ Shanlax International Journal of Economics., vol. 5, dec 2016

[32] J. Brogan, I. Baskaran, and N. Ramachandran, ‘‘Authenticating health activity data using distributed ledger technologies,’’ *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jan. 2018.

[33] Bhukta, Dr. Ashok and Patra, Sudhakar, Pattern of Healthcare Expenditure in India (October 7, 2019). Available at SSRN: https://ssrn.com/abstract=3465791 or http://dx.doi.org/10.2139/ssrn.3465791

[34] Mushtaq MU. Public health in british India: a brief account of the history of medical services and disease prevention in colonial India. Indian J Community Med. 2009 Jan;34(1):6-14. doi: 10.4103/0970-0218.45369. PMID: 19876448; PMCID: PMC2763662.

[35] Chirantan Chatterjee, Vasanthi Srinivasan. Ethical issues in health care sector in India, IIMB Management Review, Volume 25, Issue 1, https://doi.org/10.1016/j.iimb.2012.11.004.

[36] Burt T, Sharma P, Dhillon S, Manchanda M, Mittal S, Trehan N. Clinical Research Environment in India: Challenges and Proposed Solutions. J Clin Res Bioeth. 2014 Nov 1;5(6):1-8. doi: 10.4172/2155-9627.1000201. PMID: 25590017; PMCID: PMC4290669.

[37] Loraine Kennedy, Kim Robin et Diego Zamuner, “Comparing State-level policy responses to economic reforms in India”, https://doi.org/10.4000/regulation.10247

[38] Singh, Pritpal; Farhan, Mohd; Asif, Mohammad,” An Empirical Study on Association of Operational Efficiency and Customer Satisfaction in Tertiary Hospitals in Punjab.”, Indian Journal of Public Health Research & Development . Sep2019, Vol. 10 Issue 9, p295-301. 7p.

[39] Pankaj Bahuguna,Indranil Mukhopadhyay,Akashdeep Singh Chauhan,Saroj Kumar Rana,Sakthivel Selvaraj,Shankar Prinja, “Sub-national health accounts: Experience from Punjab State in India”, PLOS ONE, December 10, 2018, https://doi.org/10.1371/journal.pone.0208298

[40] Bahuguna P, Mukhopadhyay I, Chauhan AS, Rana SK, Selvaraj S, Prinja S (2018)

Sub-national health accounts: Experience from Punjab State in India. PLoS ONE 13(12): e0208298. https://doi.org/10.1371/journal.pone.0208298

[41] Mohan P, Kumar R. Strengthening primary care in rural India: Lessons from Indian and global evidence and experience. J Family Med Prim Care. 2019 Jul;8(7):2169-2172. doi: 10.4103/jfmpc.jfmpc_426_19. PMID: 31463225; PMCID: PMC6691438.

[42] Gupta R, Tanwar S, Tyagi S, Kumar N. Tactile-internet-based telesurgery system for healthcare 4.0: an architecture, research challenges, and future directions. IEEE Netw2019;33(6):22–9.https://doi.org/10.1109/MNET.001.1900063.

[43] L. Zhou, L. Wang, and Y. Sun, ‘‘MIStore: A blockchain-based medical insurance storage system,’’ *J. Med. Syst.*, vol. 42, p. 149, Aug. 2018.

[44] S. Badr, I. Gomaa, and E. Abd-Elrahman, ‘‘Multi-tier blockchain framework for IoT-EHRs systems,’’ *Procedia Comput. Sci.*, vol. 141, pp. 159–166, Jan. 2018.

[45] Vora J, Italiya P, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Ensuring privacy and security in e-health records. 2018 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE; 2018. p. 1–5.

[46] K. Mannaro, G. Baralla, A. Pinna, and S. Ibba, ‘‘A blockchain approach applied to a teledermatology platform in the sardinian region (Italy),’’ *Information*, vol. 9, no. 2, p. 44, Feb. 2018.

[47] S. Amofa, E. B. Sifah, K. O.-B. O. Agyekum, S. Abla, Q. Xia, J. C. Gee, and J. Gao, ‘‘A blockchain-based architecture framework for secure shar- ing of personal health data,’’ *in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2018, pp. 1–6.

[48] H. Jiang, H. Peng, and S. Dian, ‘‘A design of medical information sharing model based on blockchain technology,’’ *IOP Conf. Ser.*, Mater. Sci. Eng., vol. 428, Oct. 2018, Art. no. 012006.

[49] Y. Du, J. Liu, Z. Guan, and H. Feng, ‘‘A medical information service platform based on distributed cloud and blockchain,’’ *in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Sep. 2018, pp. 34–39.

[50] C. Ananth, M. Karthikeyan, and N. Mohananthini, ‘‘A secured healthcare system using private blockchain technology,’’ *J. Eng. Technol.*, vol. 6, no. 2, pp. 42–54, 2018.

[51] G. Srivastava, A. D. Dwivedi, and R. Singh, ‘‘Automated remote patient monitoring: Data sharing and privacy using blockchain,’’ 2018, arXiv:1811.03417. https://arxiv.org/abs/1811.03417

[52] S. Rahmadika and K.-H. Rhee, ‘‘Blockchain technology for providing an architecture model of decentralized personal health information,’’ *Int. J. Eng. Bus. Manage.* vol. 10, Jan. 2018, Art. no. 184797901879058.

[53] M. M. Hassan, ‘‘Blockchain and big data to transform the healthcare,’’ *in Proc. Int. Conf. Data Process. Appl. (ICDPA)*, 2018, pp. 62–68.

[54] T. T. Thwin and S. Vasupongayya, ‘‘Blockchain based secret-data sharing model for personal health record system,’’ *in Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA)*, Aug. 2018, pp. 196–201.

[55] Patel MM, Tanwar S, Gupta R, Kumar N. A deep learning-based cryptocurrency price prediction scheme for financial institutions. JISA 2020;55:102583. https://doi.org/10.1016/j.jisa.2020.102583.

[56] Jindal A, Aujla G, Kumar N. Survivor: a blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment. Comput Netw (1976) 2019;153. https://doi.org/10.1016/j.comnet.2019.02.002.

[57] O. Hejlesen, ‘‘How to use blockchain for diabetes health care data and access management: An operational concept,’’ *J. Diabetes Sci. Technol.*, vol. 13, no. 2, pp. 248–253, Mar. 2019.

[58] M. Hanley and H. Tewari, ‘‘Managing lifetime healthcare data on the blockchain,’’ in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Oct. 2018, pp. 246–251.

[59] P. B. Nichol and W. Dailey, ‘‘Micro-identities improve healthcare interop- erability with blockchain: Deterministic methods for connecting patient data to uniform patient identifiers,’’ *ResearchGate*, Berlin, Germany, Tech. Rep., 2016.

[60] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, ‘‘On the design of a blockchain-based system to facilitate healthcare data sharing,’’ *in Proc. 17th IEEE*

Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (Trust- Com/BigDataSE), Aug. 2018, pp. 1374–1379.

[61] A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, ‘‘Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden,’’ *in Proc. IEEE SmartWorld*, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Oct. 2018, pp. 257–262.

[62] Z. Shae and J. J. Tsai, ‘‘On the design of a blockchain platform for clinical trial and precision medicine,’’ *in Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 1972–1980.

[63] Shae Z, Tsai JJ. On the design of a blockchain platform for clinical trial and precision medicine. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2017. p. 1972–80.

[64] T.-T. Kuo and L. Ohno-Machado, ‘‘ModelChain: Decentralized privacy- preserving healthcare predictive modeling framework on private blockchain networks,’’ 2018, arXiv:1802.01746. [Online]. Available: https://arxiv.org/abs/1802.01746

[65] S. Kim and D. Kim, ‘‘Design of an innovative blood cold chain manage- ment system using blockchain technologies,’’ ICIC Express Lett. B, Appl., *Int. J. Res. Surv.*, vol. 9, no. 10, pp. 1067–1073, 2018.

[66] PengCheng Wei , Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, Neeraj Kumar, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, 102 (2020) 902–911

[67] T. Heston, ‘‘A case study in blockchain health care innovation,’’ *Int. J. Current Res.*, vol. 9, no. 11, pp. 60587–60588, 2017.

[68] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ‘‘MedRec: Using blockchain for medical data access and permission management,’’ *in Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[69] D. Ichikawa, M. Kashiyama, and T. Ueno, ‘‘Tamper-resistant mobile health using blockchain technology,’’ *JMIR Mhealth Uhealth*, vol. 5, no. 7, p. e111, Jul. 2017.

[70] L. Castaldo and V. Cinque, ‘‘Blockchain-based logging for the cross- border exchange of ehealth data in Europe,’’ *in Security in Computer and Information Sciences (Communications in Computer and Information Science)*. Cham, Switzerland: Springer, 2018.

[71] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, ‘‘Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,’’ *J. Med. Syst.*, vol. 42, no. 7, p. 130, 2018.

[72] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, ‘‘How blockchain could empower eHealth: An application for radiation oncology,’’ *in Data Management and Analytics for Medicine and Healthcare (Lecture Notes in Computer Science)*. Cham, Switzerland: Springer, 2017.

[73] A. Ekblaw and A. Asaf, ‘‘‘MedRec: Medical data management on the blockchain PubPub,’’ PubPub, *Tech. Rep.*, 2016.

[74] Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Bheem: A blockchain-based framework for securing electronic health records. 2018 IEEE Globecom Workshops (GC Wkshps). IEEE; 2018. p. 1–6.

[75] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-W. Liao, ‘‘Governance on the drug supply chain via groin blockchain,’’ *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, p. 1055, May 2018.

[76] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, ‘‘Blockier: A blockchain-based platform for healthcare information exchange,’’ *in Proc. IEEE Int. Conf. Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 49–56.

[77] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, ‘‘BMPLS: Blockchain- based multi-level privacy-preserving location sharing scheme for telecare medical information systems,’’ *J. Med. Syst.*, vol. 42, p. 147, Aug. 2018.

[78] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, ‘‘MedBlock: Efficient and secure medical data sharing via blockchain,*’’ J. Med. Syst.*, vol. 42, no. 8, p. 136, 2018.

[79] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, ‘‘Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control,’’ *J. Med. Syst.*, vol. 40, p. 218, Oct. 2016.

[80] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, ‘‘A decentralizing attribute-based signature for healthcare blockchain,’’ *in Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–9.

[81] S.-J. Lee, G.-Y. Cho, F. Ikeno, and T.-R. Lee, ‘‘BAQALC: Blockchain applied lossless efficient transmission of DNA sequencing data for next generation medical informatics,’’ *Appl. Sci.*, vol. 8, no. 9, p. 1471, Aug. 2018.

[82] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," in IEEE Access, vol. 6, pp. 72469-72478, 2018, doi: 10.1109/ACCESS.2018.2881246.

[83] M. F. Alhamid, and M. Guizani, ‘‘Blockchain-based mobile edge com- puting framework for secure therapy applications,’’ *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[84] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, ‘‘BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,’’ 2018, arXiv:1811.03223v1. [Online]. Available: https://arxiv.org/abs/1811.03223v1

[85] M. Sankayya, and B. Balusamy, ‘‘Securing e-Health records using keyless signature infrastructure blockchain technology in the cloud,’’ *Neural Comput. Appl.*, vol. 32, no. 3, pp. 639–647, Feb. 2020.

[86] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery and R. Deters, "MediChainTM: A Secure Decentralized Medical Data Asset Management System," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1533-1538, doi: 10.1109/Cybermatics_2018.2018.00258.

[87] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, ‘‘A case study for blockchain in healthcare: ‘MedRec’ prototype for electronic health records and medical research data,’’ *in Proc. IEEE Open Big Data Conf.*, 2016, p. 13.

[88] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ‘‘MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,’’ *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[89] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, ‘‘BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,’’ *Information*, vol. 8, no. 2, p. 44, Apr. 2017.

[90] A. Roehrs, C. A. Da Costa, and R. Da Rosa Righi, ‘‘OmniPHR: A distributed architecture model to integrate personal health records,’’ *Information*, vol. 14, no. 2, p. 44, Apr. 2020.

[91] A. Dubovitskaya, Z. Xu, S. Ryu, and M. Schumacher, ‘‘Secure and trustable electronic medical records sharing using blockchain,’’ *in Proc. AMIA Annu. Symp.*, 2018, p. 650.

[92] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, ‘‘Blockchains everywhere A use-case of blockchains in the pharma supply-chain,’’ *in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.

[93] M. Benchoufi, R. Porcher, and P. Ravaud, ‘‘Blockchain protocols in clinical trials: Transparency and traceability of consent,’’ F1000Research, vol. 6, p. 66, Jan. 2017.

[94] Bingqing Shen, Jingzhi Guo, and Yilong Yang, “MedChain: Efficient healthcare data sharing by blockchain”, Appl. Sci. 2019, 9, 1207; doi:10.3390/app9061207

[95] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

[96] T. Mikula and R. H. Jacobsen, ‘‘Identity and access management with blockchain in electronic healthcare records,’’ *in Proc. 21st Eur. Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706.

[97] Vahdat S, Hamzehgardeshi L, Hessam S, Hamzehgardeshi Z. Patient involvement in health care decision making: a review. Iran Red Crescent Med J. 2014 Jan;16(1):e12454. doi: 10.5812/ircmj.12454. Epub 2014 Jan 5. PMID: 24719703; PMCID: PMC3964421.

[98] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, ‘‘Blockchain-powered parallel healthcare systems based on the ACP approach,’’ *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018.

[99] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, ‘‘Blockchain-based data

preservation system for medical data,'' *J. Med. Syst.*, vol. 42, p. 141, Aug. 2018.

[100] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, ''Applying software pat- terns to address interoperability challenges in blockchain-based health- care apps,'' *Tech. Rep.*, May 2017.

[101] Marko Hölbl ,Marko Kompara, Aida Kamišalić andLili Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare", Symmetry 2018, 10(10), 470; https://doi.org/10.3390/sym10100470

[102] M. S. Hossain, ''Spatial blockchain-based secure mass screening frame- work for children with dyslexia,'' *IEEE Access*, vol. 6, pp. 61876–61885, 2018.

[103] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 468-477, doi: 10.1109/CCGRID.2017.8.

[104] D. Steffan Norberhuis, ''MultiChain: A cybercurrency for cooperation,'' *Delft Univ. Technol.*, Delft, The Netherlands, Tech. Rep., 2015.

[105] E-Estonia Webpage. (2019). Healthcare. Accessed: Jan. 31, 2019. [Online]. Available: https://e-estonia.com/solutions/healthcare/e-health- record/

[106] Ahto Buldas, Risto Laanoja and Ahto Truu, "Keyless signature infrastructure and PKI: hash-tree signatures in pre- and post-quantum world", International Journal of Services Technology and ManagementVol. 23, No. 1-2, February 7, 2017

[107] Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst. 2018 Jun 28;42(8):140. doi: 10.1007/s10916-018-0995-5. PMID: 29956061.

[108] V. Patel, ''A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,'' *Health Inform.*, J, vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[109] M. A. Uddin, A. Stranier, I. Gondal, and V. Balasubramanian, ''A patient agent to manage blockchains for remote patient monitoring,'' *Stud. Health Technol. Inform.*, vol. 254, pp. 105–115, Apr. 2018.

[110] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, ‘‘A pro- posed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment,’’ *J. Med. Syst.*, vol. 42, no. 8, p. 156, 2018.

[111] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 415-420, doi: 10.1109/INFCOMW.2016.7562112.

[112] AL Alkeem, E., Shedada, D., Yuen, C.Y., Zemerly, M., and .J, Hu., 2017,’New Secure healthcare system using the cloud of things’, *Cluster Computing*, 20(3), 2211-2229.

[113] Greenhalgh T, Hinder S, Stramer K, Bratan T, Russell J. Adoption, nonadoption, and abandonment of a personal electronic health record: case study of HealthSpace. BMJ 2010;341:c5814

[114] Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005), ‘Can 1000 Electronic medical record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs, *Health Affairs*, **24**(5), 1103-1117

[115] Heart, T., Ben-Assuli, O. and Shabtai, I. (2017), ‘A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy’, *Health Policy and Technology*, 6(1), 20–25

[116] Flora S. Tsai (2010),’ Security Issues in E-Healthcare’, *Journal of Medical and Biological Engineering*, 30(4): 209-214

[117] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[118] S. Raval, “Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology.” *O’Reilly Media*, Inc. Sebastopol, California (2016).

[119] Jayneel Vora, Parth Devmurari , Sudeep Tanwar, Sudhanshu Tyagi ,“Blind Signatures Based Secured E-Healthcare System”, 978-1-5386-4599-4/18©2018 IEEE

[120] Zhao, H., et al., 2017. Lightweight backup and efficient recovery scheme for health blockchain keys. In: Autonomous Decentralized System (ISADS), *2017 IEEE 13th International Symposium* online. https://doi.org/10.1109/ISADS.2017.22. IEEE

[121] Thomas McGhin, Kim-Kwang Raymond Choo , Charles Zhechao Liu, Debiao He, "Blockchain in healthcare applications: Research challenges and opportunities", *Journal of Network and Computer Applications* 135 (2019) 62–75

[122] An overview of Hyperledger foundation, https://www.hyperledger.org/wp-content/uploads/2021/11/HL_Paper_HyperledgerOverview_102721.pdf

[123] T. Crain, V. Gramoli, M. Larrea, and M. Raynal, "(leader/randomization/signature)-free byzantine consensus for consortium blockchains," arXiv preprint arXiv:1702.03068, 2017.

[124] Z. Ren, K. Cong, J. Pouwelse, and Z. Erkin, "Implicit consensus: Blockchain with unbounded throughput," arXiv preprint arXiv:1705.11046, 2017.

[125] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-oftrust consensus protocol for enhancing accountability in crowdsourcing services," IEEE Transactions on Services Computing, 2018.

Appendix A

A1: List of hospitals

Sno.	Hospital Name	Place	Contacted person
1	V.K. Hospital	Jalandhar	Mr. Manpreet Singh
2	Raman Hospital	Jalandhar	Dr. Jeevan Soni
3	Raja Hospital and trauma care	Jalandhar	Mr. Sandeep vasal
4	German Hospital	Jalandhar	Dr. Rajjat Kumar
5	Kapoor Bone & Children Hospital	Hoshairpur	Dr. Davinder Singh
6	Thind Eye Hospital	Mukerian	Dr.V.P.Singh
7	Kidney Hospital	Amritsar	Dr. Saroj Lumb
8	Apolo Hospital	Bhatinda	Dr.Gurkirat Kaur Gill
9	Tyagi Hospital	Patiala	Dr. Manoj Harish
10	Navnoor Hospital	Mohali	Dr. Vishal Bhambri
11	Bhai Jaita Ji Civil Hospital	Ludhiana	Mr.Anupinder Singh
12	Mata Nanki Hospital	Ludhiana	Dr Vijay Thakur
13	Life Line Hospital	Chandigarh	Dr Monika
14	Dogra Nursing Home & Endoscopy Centre	Mohali	Mr. Pradeep
15	Fortis Hospital	Anandpur Sahib	Dr.Dhraj puri
16	Ek noor Hospital	Mohali	Dr. Amit Thakur
17	Indus Health Care	Jalandhar	Dr. Vinayak
18	Joshi Hospital	Jalandhar	Dr. Amandeep
19	Apax Super Speciality Hospital	Bhatinda	Mr. Saurabh
20	Max Super Speciality Hospita	Dasuya	Dr.Rajesh Bagga
21	Agam Hospital	Mukerian	Dr. Ravinder
22	Guru Nanak Hospital	Patiala	Dr. Kulwinder
23	Centre For Sight-Patiala	Mohali	Dr. Paramjit
24	Liberty Hospital	Talwara	Dr. Manmohan singh
25	Satya Sai Cheritable Hospital	Zirakpur	Dr. Amit Kumar
26	J.P. Hospital	Zirakpur	Dr. Sandeep
27	Osmed Healthcare Multispecialty Hospital	Mohali	Dr. Anjali
28	Max Super Speciality Hospital	Ludhiana	Dr. Amanveer kaur
29	Sigma New Life Hospital	Ludhiana	Dr.Sahil
30	Toor Hospital	Sangrur	Ms.Navneet
31	Singla Surgical Hospital	Sangrur	Dr. Manmeet

32	Sibia Healthcare Pvt Ltd	Patiala	Dr.Aman ubhi
33	Malhotra Hospital	Hoshiarpur	Dr.Shashi
34	Vidya Memorial Kanvel Hospital	Dasuya	Colonel Arvinder Singh
35	Hunjan Bone And Joint Hospital	Hoshiarpur	Mr.Amrit pal
36	B.J.S.Bal Memorial Hospital	Gurdapur	Dr. Gurwinder
37	Public Hospital	Amritsar	Ms.Palwinder
38	Dr Kundan Lal Hospital	Bhatinda	Dr.Dilbagh singh
39	Aashirwad Hospital	Gurdaspur	Dr.Ajay
40	Sukhmani Hospital	Doraha	Dr Kulwinder
41	Sanjivni Hospital	Chandigarh	Dr. Ashish Agrawal
42	Landmark Hospital	Patiala	Dr. Arun walia
43	Guru Nanak Hospital	Ludhiana	Mr.Shalendra
44	Puri Nursing Home	Hoshiarpur	Dr.Vineeta Gupta
45	Sadbhavna Medical & Heart Institute	Tanda	Dr. Minakshi saini
46	Pathak Hospital	Patiala	Dr. Nitin
47	Centre For Sight-Patiala	Mukerian	Dr.kaml Dhillaon
48	Waves Hospital	Tanda	Dr Ajit saini

A2. List of people contacted for validating content of Questionnaire

Sno.	Doctor	Place	Designation/Specialization
1	Dr. Sunita bhalla	Gurdaspur	Assistant Civil Surgeon
2	Dr. Monika Sharma	Hoshiarpur	Gynae
3	Dr. Vishesh Kumar	Garhshankar	Eye specialist
4	Dr. Saroj Lumb	Garhshankar	Gynae
5	Dr. Sashi	Dasuya	Gynae
6	Dr. Vishesh Kumar	Chandigarh	ENT
7	Dr. Arvind Kumar	Nawanshehar	ENT
8	Dr. Gopal Sharma	Chandigarh	Neurosurgeon
9	Dr. Sanjeev	Chandigarh	Neurosurgeon
10	Sukhdev Singh	Hoshiarpur	Civil Surgeon
11	Dr. Ajay Bagga	Nawanshehar	Civil Surgeon
12	Dr. Monika	Chandigarh	Medicine
13	Dr. Sukhjinder Singh	Nawanshehar	ENT
14	Dr. Rajjat	Ludhiana	Eye specialist
15	Dr. Shivanki Sinha	Jalandhar	Neurosurgeon
16	Dr. Gopal Das	Chandigarh	Medicine
17	Dr. Manish	Balachor	ENT
18	Dr. Manoj Kumar	Balachor	Gynae
19	Dr. Tyagi	Balachor	Gynae
20	Dr. Vivek Saini	Roopnagar	Medicine
21	Dr. Kanchan Sharma	Batala	Medicine
22	Dr. Gurpreet Kaur	Gurdaspur	Medicine

A3. Questionnaire for E health care setup assessment

My Name is Prikshat Kumar; I am currently pursuing PHD from Lovely Professional University, Punjab. I am conducting research study on DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE. Please respond to following questions. All responses will be kept impersonal for purpose of research only.

Topic:

DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR E-HEALTHCARE USING BLOCKCHAIN TECHNOLOGY.

Name of Hospitals _____

Hospital administrator Name _____

District _____

Qualification of Administrator

- Graduate _____
- Post graduate ____
- Doctorate ____

1. Are you using E- healthcare system?

   - Yes _____
   - No _____

2. If answer to question 1 is Yes: What is major purpose of Using E-Healthcare system?

   - Data entry
   - Data Access to patients
   - Data Access for Administration
   - Data storage

- Easing process flow
- Data analysis

3. Do you use online application for patients' registration process?

   - Yes _____
   - No _____

4. Do you use mobile application for patients' registration process?

   - Yes _____
   - No _____

5. Can patient initiate registration process before visiting Hospital?

   - Yes _____
   - No _____

6. Does E token is provided to patients after registration?

   - Yes _____
   - No _____

7. Is E token can be Reused after one visit?

   - Yes _____
   - No _____

8. If Reused for How many days it is valid?

_____

_

9. Is Registration of patients linked With Aadhaar card number?

- Yes _____
- No _____

10. Is walk in entries for e healthcare system allowed.

- Yes _____
- No _____

11. Does verification process is followed for verifying patients' information.

- Yes _____
- No _____

12. Does Attribute concept is used to store data of patients.

- Yes _____
- No _____

13. Access granted to some other framework for data registration inside the organisation.

- Yes _____
- No _____

14. Access granted to other framework for data registration outside organisation.

- Yes _____
- No _____

15. Do you have system in Hospital that protects our electronic health records?

- Yes _____
- No _____

16. Doctors having access to patients' data.

- Yes _____
- No _____

17. Paramedical staff having access to patients' data.

- Yes _____
- No _____

18. Patients have access to their own recent medicinal history

- Yes _____
- No _____

19. Data classified according to transaction.

- Yes _____
- No _____

20. Any system to track transactions and detect security incidents.

- Yes _____
- No _____

21. Do you have any secure path for executing transactions?

- Yes _____
- No _____

22. Basic security controls for securing data.

- Yes _____
- No _____

23. What do you think is it required to improve transaction paths?

- Yes _____
- No _____

24. Any difficulty in transaction processing?

- Yes _____
- No _____

25. Is mapping of storage area for transactions is done?

- Yes _____
- No _____

26. Is any training provided to you for accessing e healthcare system?

- Yes _____
- No _____

27. How security provided to transactions.

---

28. Is there any backup and recovery plan used in the system?

- Yes _____
- No _____

29. Have any third party approached you to provide their services for managing data?

---

30. What kind of security issues you face in our e healthcare system?

---

31. Has your data ever been breached?

---

32. If yes, how do you know?

---

33. Have ever any insurance company contacted you for patients' data?

---

34. Are Medical labs are approaching you for patients' data?

---

35. How do you dispose of electronic patient health information?

---

36. Are you analyzing data of patients?

---

37. If yes which tool you are using for analysis?

_____

38. Is there is any third part involved in analysis?

_____

39. What do you think: Is E Healthcare is improving efficiency of Hospitals?

- Yes
- No

40. What are various challenges nowadays hospitals are facing related to E -Healthcare setup?

_____

LOVELY PROFESSIONAL UNIVERSITY

Centre for
Research Degree Programmes

LPU/CRDP/PHD/EC/20200225/000998
Dated: 01 Apr 2022

Prikshat Kumar Angra
Registration Number: 41800137
Programme Name: Doctor of Philosophy (Computer Applications)

Subject: Letter of Candidacy for Ph.D.

Dear Candidate,

We are very pleased to inform you that the Department Doctoral Board has approved your candidacy for the Ph.D. Programme on 04 Dec 2019 by accepting your research proposal entitled: "Design and implementation of security framework for e- healthcare using blockchain technology" under the supervision of Dr. Pritpal Singh.

As a Ph.D. candidate you are required to abide by the conditions, rules and regulations laid down for Ph.D. Programme of the University, and amendments, if any, made from time to time.

We wish you the very best!!

In case you have any query related to your programme, please contact Centre of Research Degree Programmes.

Head

Centre for Research Degree Programmes

Appendix B1: Analyzing Efficiency and Slack of Tertiary Hospitals of Punjab: A Case of Data Envelopment Analysis

Singh Pritpal, Angra Prikshat

International Journal of Current Research and
Review
Year: 2021, Volume: 13, Issue: 10
First page: **(295)** Last page: **(301)**
Print ISSN: 2231-2196. Online ISSN: 0975-5241.
Article DOI : 10.31782/IJCRR.2021.131022

Abstract

Introduction: Data envelopment analysis is an operational research-based method for estimating the efficiency of the general execution of hierarchical units of hospital considering the availability of various data sources in form of inputs and outputs.

Objective: This research focuses on analyzing operational efficiency and finding slack in the input of tertiary hospitals of Punjab. Demand for health services is increasing but the availability of health services are still a big issue. In the present circumstance, it has turned out to be difficult for hospitals in Punjab to guarantee increasingly productive methods for administrations. Under the current conditions, it is fundamental to discover the fitting asset blend and its use.

Methods: VRS-DEA model of data envelopment analysis is applied on data collected from 1st January 2018to 31st December 2018 for hospitals inputs and outputs to analyze efficiency and find slack of 48 tertiary hospitals of Punjab of three different sizes toward to output.

Results: This research indicates that smaller hospitals have an efficiency more than large size and mid-size hospitals as smaller size hospitals average efficiency is .80. The mean efficiency of medium size hospitals is .75and large hospital is .71. Only 4hospitals are working at the constant return to scale and working efficiently and 44 are inefficient as these 44 hospitals are suffering huge slack in Inputs. Mean Slack of 27.31%, 18.5%, 9.5%observed in large size, Medium size and small size hospitals in the number of patients attended.

Conclusion: Hospital authorities must benchmark efficiency with the best performing hospitals in that area. Data envelopment analysis must be used to distinguish the hospitals on basis of efficiency and policymakers can use this as a tool to evaluate the performance of public hospitals and set key performance indicators for allocating fund to these hospitals.
Key Words: Data envelopment analysis, Input slack, Efficiency, Return to scale, Performance indicators, Operational research.

INTRODUCTION

This research focuses on studying the operational efficiency of tertiary hospitals of Punjab. A study to find association was conducted with the help of analysis of data envelopment technique, which is used to find out the efficiency of tertiary medical hospitals considered for the study. Data envelopment analysis focuses on finding efficiency through input /output-based model which follows linear mathematical formulas.1,2 As the demand for healthcare services in India is increasing because of many reasons which include awareness for a preventive health checkup, Increasing population, Complexity of disease and availability are major contributors to this. Demand for health services is increasing but the availability of health services are still a big issue.2 Among health service providers in specialized care, the Private sector in Punjab is at the forefront and covering most of the area and population for providing health services. But still according to world health statistics report India is performing below average with 9 beds for 1000 patients which is very below the global average. Govt. hospitals in form of community health centres and civil hospitals also started improving their infrastructure to provide health services at a specialized level but still bed to patient ratio is not improving from last many years as compared to the global average which is a matter of concern.3,4 A considerable amount of money invested by government bodies and private sector to improve infrastructure to improve performance of services provided to people and to increase the availability of services to all but as a population of the country is huge that much infrastructure is not enough. In that case, it will become very important for hospitals whether private or government to optimally utilize their existing resources, Data envelopment analysis is a technique that is formulated to find operational efficiency in form of logical and scale efficiency of the organization and to decide their benchmark and operate according to benchmark or if there is no benchmark then set the benchmark.5 Health and healthcare services are too different aspect which needs to be distinguished, Health is related to person and healthcare services does not only involve providing hospital services but also to provide

preventive services and post medical checkup services also. In the present circumstance, it has turned out to be difficult for hospitals in Punjab to guarantee increasingly productive methods for administrations. Under the current conditions, it is fundamental to discover the fitting asset blend and its use. So also, it is important to distinguish sources of relative cost wastefulness – specialized and allocate both.5,6 The centre point of this study is on surveying the hospitals in efficiency terms, for example, the perfect measure of inputs to deliver a given degree of output. The other inspiration driving this investigation has been to see how to address the issue of benchmarking in hospitals.

Organizational Structure of health Sector in Punjab

Punjab, both the public and the private division assume a vital job in providing medicinal services administrations. It is the Department of Health and Family Welfare under the Public part which is in charge of preventive health services benefits in Punjab. There is a four-level structure of medicinal services conveyance framework in the State. This contains Sub Health Centers (SHCs)/dispensaries at the base giving the fundamental human services administrations to a population of 3000-5000 individuals. Above it, there is Primary Health Centers (PHC) serving a population of 20000-30000 individuals.6 It likewise fills in as a referral unit to six subcentres. Above Primary Health Centers there are Community Health Centers (CHC) which serves a population of 80,000 to 1.20 lac and a referral unit to four PHCs. This entire extent of SHCs, PHCs and CHCs goes under essential level healthcare where administrations are constrained. To help primary human services administration there are secondary level medicinal services.The information in Table 1 beneath demonstrates that since the 1990s, there was no impressive measure of increment in the hospital framework in Punjab.

Table 1: Broad wise category Health centres during 2016 in Punjab

	Hospitals		Primary Health centre		Subsidiary health centre		Community health centre		Ayurveda Institutions	
District	1991	2016	1991	2016	1991	2016	1991	2016	1991	2016
Gurdaspur	16	3	47	40	127	120	6	1515	51	52
Amritsar	33	7	49	36	178	98	6	4	43	22
Tarn taran	.	2	-	19		59	-	9	-	22
Kapurthala	7	3	10	13	60	50	5	4	26	26
Jalandhar	25	3	36	28	161	110	6	11	45	32
S.B.S.Nagar	-	2	.	17	-	49	.	3	-	24
Hoshiarpur	16	4	41	32	1 22	93	6	3	57	44
Rupnagar	8	2	23	I1	78	34	5	3	35	22
S.A.S.Nagar	.	2	-	13	.	51	.	5	.	25
Ludh iana	27	5	35	33	1 56	120	6	2	37	36
Firozpur	17	4	38	34	1 00	85	6	8	39	38
Faridkot	17	3	40	8	1 18	20	6	3	26	9
M ukısar	-	3	-	17	.	45	-	s	.	1 1
Moga		I	-	22	.	53	-	5	-	7
Bathinda	I S	4	38	20	1 16	70	6	9	39	27
Mansa	-	2	.	14	.	38	-	4	-	1 2
Sangrur	18	4	41	32	1 17	73	6	6	43	31
Bamala	.	I	.	1 1	.	36	.	4	.	12
Paıiala	19	·6	44	28	132	72	6	10	S I	32
Fatehgarh Sahib	.	2	-	14	-	28	-	4	.	1 0
Punjab	203	62	442	444	1473	1308	70	130	493	495

Source: Statistical abstract of Punjab 2016 Director, Health and family welfare, Punjab

MATERIALS AND METHODS

Research Question

This research focuses on analyzing the operational efficiency of hospitals and finding slack in the input of tertiary hospitals of Punjab to set the benchmark for inputs as comparable to outputs using data envelopment analysis.

Ethical Approval

Ethical approval of this study is taken from the senior medical officer of each district for selecting their hospital data into the study and for private hospitals data is collected after taking due permission from an administrative officer of the hospital where data is not present online on their website

Study design

Data was collected from 48 hospitals in form of inputs and outputs decided for calculating efficiency from 1st January 2018 to 31st December 2018 and the selection of hospitals was made from the list of the hospitals being run by doctors registered with the Indian Medical Association. Government and private tertiary level hospitals with bed strength of more than 40

were chosen for study from the Jalandhar, Hoshiarpur, and Amritsar and Ludhiana districts of Punjab. Hospitals are selected based on quota sampling. Quota sampling is done on basis of the size of the hospital, according to the objective of this research different sized hospitals are required and three different sizes of tertiary hospitals are considered i.e. 16 Small sizes hospital having bed strength between 40 and 70, 16 medium sizes between 70 to 100 and 16 large size hospitals having bed strength more than 100.

Data analysis

Envelopment study of data is a linear mathematical programming-based method for estimating the efficiency of the general execution of hierarchical units of hospital considering the availability of various data sources in form of input and outputs. DEAOS free online \\tool was used for calculating efficiency. This study introduces the input /Output technique and uses a manual proportion of effectiveness, i.e.: how relative efficiencies can be settled around the centre on inefficient units set.7,8 Efficiency is usually considered in the range of [0, 1]. Efficiency requires a typical arrangement of loads to be applied to overall units and loads is given to each input as per the DEA model. 9,10

Inputs and outputs Variables from the hospital for data envelopment analysis

Inputs data collected is in form of number of beds, number of doctors, Nurses, Outpatient department hours per week of working, laboratory hours per week and paramedical staff supporting major staff doctors and administrative staff. Outputs for calculating efficiency are Outpatient visits, Inpatients and laboratory cases, Maternal and child healthcare all these are types of cases treated and the number of cases. Basically for efficiency calculation input and output are required. Data of some of the hospitals are collected through secondary sources and for some hospitals data is collected by visiting hospitals and meeting administrative officers of hospitals after taking due permission from SMO of the district. Outpatient and inpatient are two very important parameters to calculate efficiency in previous studies efficiency is calculated on basis of these two only, But in this study laboratory cases and maternal and child healthcare is also included which gives proper efficiency of variable return to scale which is technical efficiency. All the outputs are in form of the number of cases treated. Data is collected from hospitals from annual book release and by directly visiting the hospitals. The study includes the outputs efficiently arranged. Those can be isolated into faculty, resources, or assets and administrations.

RESULTS

In first stage efficiency of hospitals were analyzed, data envelopment analysis was utilized to analyze and evaluate the efficiency of the hospital and in the second stage, slack values were analyzed (Table 2).

Table 2: Comparison of the efficiency of large, medium and small size hospitals

Parameter	Efficiency
Mean	0.76
Std. Dev.	0.16
Hospitals (Small Size) (n=16)	
Mean	0.8
Std. Dev.	0.15
Hospitals (Medium Size) (n=16)	
Mean	0.75
Std. Dev.	0.16
Hospitals (Large Size) (n=16)	
Mean	0.71
Std. Dev.	0.15

Slack Value in Large size Hospital

Slack values are value which is added to inequality constraint to convert into to equality .Slack values of large size hospitals mostly working at either increasing return to scale or diminishing return to scale all the values are derived from data envelopment analysis of data collected .hospitals can employ even 19 per cent fewer doctors to achieve the same output of outpatients. .With the same number of inputs they can cater to a large number of outpatient's (i.e. 65000) (Table 3).

Table 3: Mean Slack value of large size hospitals

DMU(Hospital)	Efficiency score	I/O	Present quantity	Target	Difference (PQ-T)	Percentage Difference
LARGE SIZE HOSPITAL						
	0.71	Doctors	31	25.1	-6	--19.58064516
				144	-16	-10
		Beds	160			
		Nurses	44	41	-3	-6.81818182
		Equipment's	24	23	-1	-4.16666667
		paramedical staff	16	16	0	0
				65000	14000	27.45098|04
		Outpatient visits	51000			

Slack Value in Medium and Small Size Hospital

Hospital administrators have three options to them for optimally utilizing wasteful assets use: Expanding network of hospital. Decreasing hospital inputs; or Hospital organization process changes in medical hospitals.11,12All together for the wasteful medical hospitals to have gotten moderately productive, as a gathering, they would have expected to build their outpatient division visits more than (18.05%) and in small size hospitals patient visits can be increased to 9.5% (Table 4 and 5).

Table 4: Mean Slack value of medium Size Hospital

DMU(Hospital)	Efficiency score	I/O	Present quantity	Parameter Target	Difference (PQ-T)	Percentage Difference
Medium Size Hospital	0.75	Doctors	14	12	-2	-14.2857143
		Beds	76	70	-6	-7.89473684
		Nurses	34	30	-4	-11.7647059
		Equipment	23	16	-7	-30.4347826
		paramedical staff	16	16	0	0
		Outpatient visits	27000	32000	5000	18.5185185

Table 5: Mean Slack value of Small Size Hospital

DMU(Hospital)	Efficiency score	I/O	Present quantity	Target	Difference (PQ-T)	Percentage Difference
Small Size Hospital						
	0.80	Doctors	13	11	-2	-15.3333333
		Beds	45	34	-11	-24.4444444
		Nurses	29	23	-6	-20.6896552
		Equipment's	16	12	-4	-25
		paramedical staff	13	13	0	0
			24000	26300	2300	9.58333333

DISCUSSION

Present research indicates that smaller hospitals have an efficiency more than the larger size and mid-size medical hospitals as demonstrated in the above table smaller size hospitals average efficiency is .80. The mean efficiency of medium size hospitals is .75 and the large hospital is .71. As per our outcomes, small size medical hospitals are generally more efficient. The objective of small, medium and big size hospitals are different as some concentrate more on care and quality some on quantity. Big size hospitals will in general increment their physical, innovative and medicinal work limit in request to understand the requirement of far-reaching care. Nature of care may essentially increment in parallel with the addition of these limits. Strangely, huge size medical hospitals are not performing like small and medium-size medical hospitals as far as scale effectiveness. As results estimate large size hospitals don't work at an ideal scale size. , big size hospitals may frame smaller patient consideration units inside their association. Along these lines, large size medical hospitals not just take out the negative impact of their non-ideal scale size, yet besides they make explicit treatment units for patients.

Other than efficiency estimation this DEA model also provided important information about return to scale of hospitals, Outcomes uncovered that all hospitals understudy would result in: *The constant return to scale in 4 (8.33%*) medical hospitals, suggesting that their healthcare administration outputs would increment to a similar extent. This implies hospitals were working at their most gainful scale sizes.14,15

Increasing return to scale in 23 (47.9%) medical hospitals, suggesting that their healthcare administration outputs would increment by a more prominent extent. These medical hospitals subsequently expected to expand their size to accomplish ideal scale, for example, the scale at which there is a steady return to scale in the connection among inputs and outputs.16,17

Decreasing return to scale in 21(43.7%) hospitals, inferring that their healthcare administration outputs would increment by a small extent. medical hospitals would have expected to decrease their size to accomplish ideal scale.18,19

Slack values are valued which is added to inequality constraint to convert into equality. The present study uncovers immense slack in the utilization of assets, for example, specialists, Beds. With better observing, medical hospitals will have the option to serve more patients with existing assets and in the current situation in the healthcare area in India, the ideal use of assets in the segment is vital. in the first stage efficiency of hospitals are calculated and only 4 % of hospitals are working at an efficient scale and 44 % of hospitals are inefficient and now in this stage research is to find out the cause of inefficiency that will cause input slack in Hospitals. In this stage, analysis is applied to find whether these medical hospitals ideally use contributions for human services to give out-persistent and good administrations to the overall population if not what is the actual reason for inefficiency and how much each hospital can contribute to out to reach efficiency.

CONCLUSION

As indicated by research outcomes and findings, small size hospitals are generally more efficient and have higher patient satisfaction as compared to other hospitals. Medical hospital likewise concentrates on the reasons for low efficiency before reconfiguring their entire hospital structure. The organization through decentralized set-up and the small zone level authorities screens these associations and study slack of every hospital. The activity of government is essential in ensuring that finding slack is used effectively. This will require making execution based pointers to screen the slack in the input of hospitals and plan to manage to particularly work on which area. In this research also many slacks are identified in each hospital infrastructure use which can be regulated to other paces if it is surplus. Moreover when an organization is big then management must ensure efficiency consideration. The health care industry can adopt Benchmarking scheme of their services with the best one in the same field to improve efficiency. The reason for benchmarking in medicinal services is to improve effectiveness, nature of care, understanding healthcare and patient satisfaction.

RECOMMENDATIONS

DEA data envelopment analysis can be applied in the organization to solve the proper staffing problem. Utilizing information to examine staff distribution can prompt operational productivity. Information on patient volume can be recorded and medical hospital staff can be suitably designated dependent on the equivalent. The present research demonstrates that smaller medical hospitals have a more significant level of effectiveness than bigger and medium-size emergency hospitals as appeared in the above table smaller size hospitals normal efficiency is .80. So two hundred bed hospitals are more efficient than one 200 bed hospitals. In a country like India here Population is very high small hospitals with more outreach is required. Healthcare operations management is urgent for the effective working of healthcare administrations, particularly when the medicinal services segment is experiencing a lot of changes.

FUTURE SCOPE OF STUDY

This study provides the idea about how to evaluate the efficiency of tertiary hospitals. This methodology can act as a tool to benchmark efficiency for hospital authorities for best in that area. The technique utilized right now i.e. Data envelopment analysis to distinguish the hospitals on basis of efficiency, which can improve their administration. In past, the checking and assessment of these foundations have stayed a significant issue. The administration through decentralized set-up and the area level healthcare specialists can screen these foundations. The job of the government is very basic in guaranteeing that hospital infrastructure is utilized optimally. This will require creating execution based pointers to screen these awards using data envelopment analysis. The procedure recommended right now help healthcare agencies to recognize moderately less efficient medical hospitals. The methodology suggested in this research can be used by the Department of Health and Family Welfare to develop benchmarks for monitoring and evaluating the performance of both public and private hospitals. Based on the findings the steps can be initiated to improve the efficiency of resource use in hospitals. DEA can be applied to compare hospital performance after Electronic Medical record system implementation.

ACKNOWLEDGEMENT

Authors acknowledge the immense help received from the scholars whose articles are cited and included in references of this manuscript. The authors are also grateful to authors/editors/publishers of all those articles, journals and books from where the literature for this article has been reviewed and discussed

Financial Support and sponsorship: Nil

Conflict of interest: No conflict of interest.

Author Contribution:

Dr Pritpal Singh and Prikshat Kumar conceived the idea. Dr Pritpal Singh developed the theory and performed the computations. Prikshat Kumar verified the analytical methods and encouraged Dr Pritpal Singh to investigate and supervised the findings of this work. Both authors discussed the results and contributed to the final manuscript. Dr Pritpal Singh and Prikshat Kumar wrote the manuscript.

REFERENCES

1. Bowlin F. Measuring performance: An introduction to data envelopment analysis (DEA). J Cost Anal 1998;7(2):3-27.
2. Bhat R, Verma BB, Reuben E. An empirical analysis of district hospitals and grant-in-aid hospitals in Gujarat state of India. Health Policy Development Network (HELPONET), 2001;13(2):1-40.
3. Hassan M, Tuckman HP, Patrick RH. Hospital length of stay and probability of acquiring infection. Int J Pharm Health Mark 2010;4(3):24-38.
4. Ghosh B, Bhadia U. A study on the inpatient system in a state hospital of Calcutta. Indian J Commu Med 1990;15(1):135-149.
5. Mogha SK, Yadav SP, Singh SP. Performance evaluation of Indian private hospitals using DEA approach with sensitivity analysis. Int J Manag Eco 2012;11(2):1-2.

6. Singh PP, Farhan M, Asif M. An Empirical Study on Association of Operational Efficiency and Customer Satisfaction in Tertiary Hospitals in Punjab. Int J Manag Eco 2019;10(9):295-301.
7. Oussofiane A, Dyson RG, Thanassoulis E. Applied data envelopment analysis. Eur J Oper Res 1991;5(2):1-15.
8. Jat TR, Sebastian MS. Technical efficiency of public district hospitals in Madhya Pradesh, India: A data envelopment analysis. Glob Health Act 2013;(6:2):17-42.
9. Jat TR, Sebastian MS. Technical efficiency of public district hospitals in Madhya Pradesh, India: A data envelopment analysis. Glob Health Act 2013;(6:2):17-42.
10. Sheikhzadehl Y, Roudsari AV, Vahidi RG .Public and private hospital services reform using data envelopment analysis to measure technical, scale, allocative, and cost efficiencies. Health Promot Perspect 2012;2(2);28-41.
11. Singh Z. Aging: The triumph of humanity-are we prepared to face the challenge? Indian J Public Health 2012;5(6):189-195.
12. Davey S, Raghav SK, Muzammil K, Singh JV, Davey A, Study on the role of rural health training centre (RHTC) as a supporting component to a primary health care system for NRHM programme in district Muzaffarnagar (UP). Int J Res Med Sci 2014;2(6):53-61.
13. Austin MJ, Shawcross DL. The outcome of patients with cirrhosis admitted to intensive care. Curr Opin Crit Care 2008;14(2):202-7.
14. Charif I, Saada K, Benajah D, Abkari ML. Predictors of IntraHospital Mortality in Patients with Cirrhosis. J Gastroenterol 2014;14(4):141-8.
15. Wong F, Bernardi M, Balk R, Christman B, Moreau R, GarciaTsao G, et al. Sepsis in cirrhosis: report on the 7th meeting of the International Ascites Club. Gut 2005;54(5):718-25
16. Viasus D, Garcia-Vidal C, Castellote J, Adamus J, Verdaguer R, Dorca J, et al. Community-acquired pneumonia in patients with liver cirrhosis: clinical features, outcomes, and usefulness of severity scores. Med. 2011;90(2):110-8.
17. Alsherif A, Darwesh H, Badr M, Eldamarawy M, Shawky A, Emam A. SOFA Score as a Predictor of Mortality in Critically Ill Cirrhotic Patients. Life Sci J 2013;10(2):178-181.
18. Hamza RE, Villyoth MP, Peter G, Joseph D, Govindaraju C, Tank DC, et al. Risk factors of cellulitis in cirrhosis and antibiotic prophylaxis in preventing recurrence. Anna Gastroent 2014;2:28.

19. Jalan R, Fernandez J, Wiest R, Schnabl B, Moreau R, Angeli P, et al. Bacterial infections in cirrhosis: a position statement based on the EASL Special Conference 2013. J Hepatol 2014;60(6):1310-24.
20. Maiwall R, Kumar S, Chaudhary AK, Maras J, Wani Z, Kumar C, et al. Serum ferritin predicts early mortality in patients with decompensated cirrhosis. J Hepatol 2014;61(1):43-50.

B2. Cloud Security Issues and Challenges

Prikshat Kumar Angra , Dr.Kavita, Dr.SahiVerma, AnupLalYadav

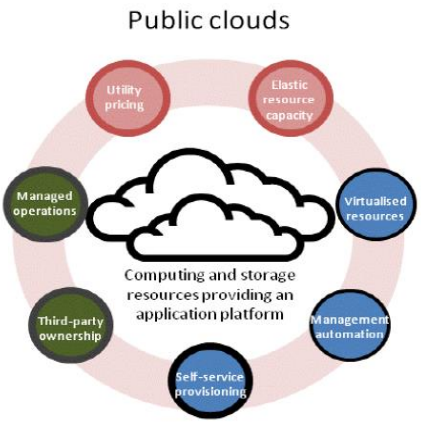
International Journal of Control and Automation
Year: 2019, Volume: 12, Issue: 4
First page: **(151)** Last page: **(156)**
ISSN: 2005-4297.

Abstract

It provides a direct blaze to the shared pool of comfortable attached resources.These resources are used to access information with the help of service providers. Resources are provided in the form of IT-based capabilities.In this paper cloud computing security obstructions are discussed related to cloud and its services.Cloud security can be improved with the help of many technologies that may use to secure data some times and also secure sometimes working of service providers.We have presented a review from different papers according to which many security issues are discussed.We explain trusted data sharing in which our data is easily accessible from different devices with the help of cloud services.For secure data access Service level Agreement(SLA) protocol helps for transparent communication between the end user and cloud.

Keywords: Security, Cloud Computing,Service level agreement.

Introduction Cloud computer is a technology which can be executed by different design, and resources of other technology with distinct configurational approaches. Some cloud resources models are Infrastructure As a Services (IaaS), Platform As a Services (PaaS), and Software As a Services (SaaS). There is a free and open source software which is used to develop the cloud platform called Heroku. That supports many languages like JAVA, Node.js, Scala, Python and PHP, it can also be integrated with data services. Cloud computing generally described either build on the host mode, or on services that cloud present if has. While discussing about deployment model, we can classify cloud as: Public, Private, Hybrid, Community Cloud and based on a services the cloud model is charity: IaaS, PaaS, SaaS, or storage, Database, Information, Process etc.



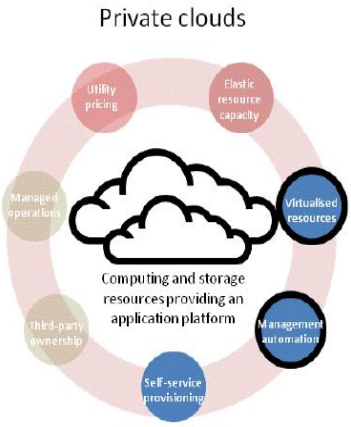


Figure 1:Public cloud [23] **Figure 2:Private Cloud[23]**

Cloud computing data security is the major challenge now a day to minimize the risks. These threats are directly like open cloud, distribute upload, and environment. Cloud computer is everywhere now because of some advantages like flexibility, accessibility and capacity as compare to other storage methods. The main seek of this study is to secure the client data over the cloud and ensuring the client that the data which has been uploaded by you is safe a secure. Security is the main part of the cloud computing and it can be divided in to two main parts, Firstly, Security issued by the cloud provider and secondly Security excude faced by their customers. Customer has trust on cloud provider that's why they put data over this storage with trust; this is main reason the need of security. There are several algorithms has already been used like AES (Advance Encryption Standard) and this algorithm is symmetric block cipher. In cloud computing, the users are unaware the location of their confidential data, because the cloud service providers only manage the data centres at distributed location. The importance of this study is to address the basic requirement of the client like Authentication, integrity, transparency, confidentiality, availability etc.

Related Work

A Venkatesh et al[1] in their paper has demonstrate that make sure that data is stored on cloud storage by secure process but data securiy is major threat in cloud storage.To eliminate this, privately,uprightness,availability should be compressed in a Cloud Service Provider (CSP)'s Service- Level Agreement (SLA) to its customers.Dr. N.K.Joshi et al[2] in their paper has

demonstrate that One of the main problem is the data security and privacy of information stored and processed at the cloud service grant systems.User's all data may be store on different locations for either problemliberalilsm or because the service is provided through different service providers.Prabal Verma et al[3] in their paper has demonstrate that Security in cloud computing is still in conception and required more inspect,cloud computing has been utilized and used in showing environments.This paper grant an overview of cloud computing, its power and categories.Victor Chang et al[4] in their paper has explain that review, thinking and essentials in the (Cloud Computing Adoption Framework) CCAF to protect informationsecurity.CCAF multi-layered security could provide the additional protection for all 10 PB of data in 125 hours when the Data Center was under the security cause and slash. Data security in the Cloud is an important issue for Cloud adoption.Zhangjie Fu et al[5] in their paper has explain the standard theory of encryption makes the properuse of the data difficult.So it is tough to find the given set of keyin encrypted data set.Solution of this is use different cloud servers for encrypted retrieval and make hand outall on findrightness and regularity. For exceed correctness,develop the idea hierarchy to deliver the search perameters.Jong-Hoon Lee et al[6],in their paper has demonstrate that when the normal security systems arevirtualized in cloud party line, we build the SIEM design for cloud-based security utility Security Information and Event Management (SIEM) engine performs the data analysis super each user, it must see the retrieved data for each user.It also find out the gained data for each user.DIAO Zhe et al [8],in their paper has demonstrate that cloud storage fusion made very rapid, and cloud storage security technology is facing unprecedented issues.To achieve the security of cloud storage completely, academia,industry and government departments need to work together.

Deployement and Service Models

The cloud deployment model derivates in four types:-

(a)Private cloud model:-The infrastructure operated by only one organization and according to their private use.These are made by the organization for working of their own critical applications with no interferance of other organization.This service is only accessed by owners of the cloud.

(b)Public cloud model:-This kind of cloud storage is used by the general purpose users for uploading and downloading the data.Service supplier has all over ownership of cloud storage

with their own attitude and model.Various cloud service provider areMicrosoft, Amazon EC2 and Google App Engine etc.

(c)Community cloud:-A cloud is togetherbuild by organization and equal cloud infrastructure is shared by them.

(d)Hybrid cloud model:-This kind of cloud infrastructure is combination of 2 or additional clouds it may be public,private or community.It is used for optimizing the resources of an organization.

Figure 3:Deployment Model[22]

Cloud service model is differentiate to 3 main parts-SaaS(Software as a Service),PaaS(Platform as a Service) and IaaS(Infrastructure as a Service). 1)SaaS Software as a service provides different types of softwares that are used to develop and host different web applications developed in high level programming and frameworks.All our hardware devices like mobiles,data servers and data base etc. 2)PaaS Platform as a service gives different platforms used to develop application.Platforms are operating systems we use to develop application. 3)IaaS All fundamental computing resourses like storage,server network etc.are used to provide services to the end user's with proper relation with software and platform they need.Amazon EC2 is an example of IaaS.

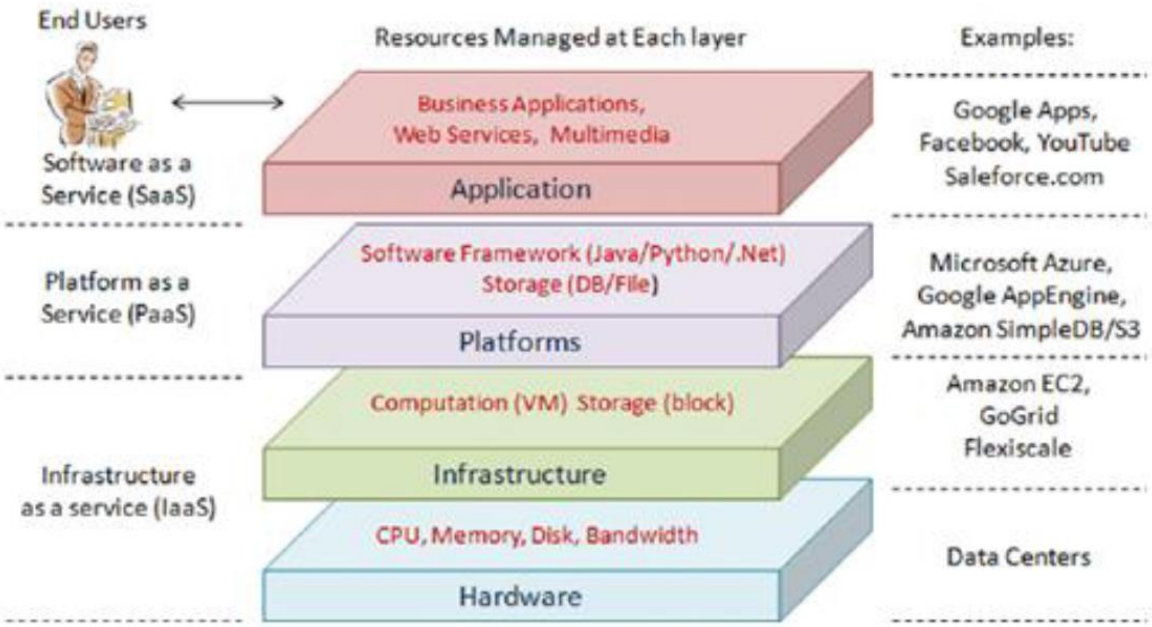


Figure 4:Service Model Architecture[21]

Major Security Issues In Cloud Computing

There are manyissues and challenges that should be taken in to premier for gain full benefit from this new design.Some of major concern are

1)It is difficult to maintain the cohesion to ensure the auditability of dynamic data molten nature of cloud computing service model.

2) There should be a common standard that all the service provider used for store end user valueable information. 3)Userknow they are safe and updated with required application.

4) Violation of law of data attach by government.

Conclusion

Uses of cloud computing reduce operating cost for companies and increasing efficiency of working.We have presented issues connected to security in cloud computing.After that the problems related to security in cloud computing model how can be exceed is discussed.The ongoing working on Service level agreement (SLA) is outlined in this paper. Also we have shown a solution to provide security for user's information reside on private clouds since safe information stored on cloud nature is a consequentialfact that prevents number of peoples from

using the cloud.The need for future work on account ability mechanism in public and private clouds,to provide clear service that can be trusted by every user is also highlighted in this paper that's why we working for secure access of data from the cloud service providers.

Reference

1. A Venkatesh *1, Marrynal S Eastaff 2,"A Study of Data Storage Security Issues in Cloud Computing,"International Journal of Scientific Research in Computer Science, Engineering and Information Technology,January-February-2018

2. ShivamSharma,Dr. N.K.Joshi,"CLOUD COMPUTING SECURITY CHALLENGES AND

SOLUTIONS,"February 2018

3. PrabalVerma 1 , Aditya Gupta 2 , Rakesh Singh Sambyal 3,"Security Issues and Challenges in Cloud Computing: A Review,"CSEIT411832 | Published - 25 April 2018 | March-April-2018

4. Victor Chang, MuthuRamachandran,"Towards achieving Data Security with theCloud Computing Adoption Framework,"1939-1374 (c) 2015 IEEE

5. ZhangjieFu,Lili Xia Xingming Sun Alex X. Liu,GuowuXie,"Semantic-aware Searching overEncrypted Data for Cloud Computing,"1556-6013 (c) 2018 IEEE

6. Jong-HoonLee,YoungSooKim,Jong Hyun Kim,Ik Kyun Kim,"Toward the SIEM Architecturefor Cloud-based Security Services,"2017 IEEE

Bih-Hwang Lee,ErvinKusumaDewi, Muhammad Farid Wajdi,"Data Security in Cloud Computing Using AES Under HEROKU Cloud,"2018 IEEEE

8. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan"Study on Data Security Policy Based On Cloud Storage,"2017 IEEE

9. David S. Linthicum,"Emerging Hybrid Cloud Patterns,"2016 IEEE

10. Mohamed Al Morsy, John Grundy and Ingo Müller,"An Analysis of the Cloud Computing Security Problem,"

11. Syed NoorulhassanShirazi, Antonios Gouglidis, Arsham Farshad, and David Hutchison,"The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective,"NOVEMBER 2017 IEEE

12. Gentry Craig. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University; 2009.<http://crypto.stanford.edu/craig/craig-thesis.pdf>[retrieved 21.04.11]

13. Microsoft. Microsoft Windows Azure.<http://www.microsoft.com/windowsazure/>

14. RongChunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011

15. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

16. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput.,vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

17. J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," J. Commun.Netw., vol. 14, no. 6, pp. 682–691, Dec. 2012.

18. Office of Management and Budget. 2016. Strengthening Federal Cybersecurity. Meeting Our Greatest Challenges: The President's Fiscal Year 2017 Budget. Fact Sheet. Last accessed May 31, 2016.https://obamawhitehouse.archives.gov/omb/budget/key-issue-fact-sheets

19. ShaluMall, Sushil Kumar Saroj,"A New Security Framework for Cloud Data,"Procedia Computer Science 143 (2018) 765–775

20. RongChunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011.

21. JafarMuzeyinWorku,"DEFINING AN EFFECTIVE SECURITY POLICY FOR COMPANIES USING CLOUD COMPUTING,"23 July 2017

22. Intel. Intel Dam Cloud.<https://www.intel.com/content/dam/>

23. Global Dots<https://www.globaldots.com/cloud-computing-types-of-cloud/>

B3. A Study to Create Secure E-Healthcare Framework using Blockchain Technology: A Case of Tertiary Hospitals of Punjab

Prikshat Kumar Angra , Dr. Pritpal Singh

Pacific Business Review (International)

Year: 2021, Volume: 14, Issue: 6
First page: **(10)** Last page: **(16)**
ISSN: 0974-438X(P).

Abstract

Blockchain technology enables a decentralized and distributed state without the need for a central authority. Because of the use of cryptographic standards, exchanges are still reliable and dependable. Blockchain technology has recently become popular and has made inroads into a variety of industries, owing to the popularity of cryptographic forms of currency. The need for a more persistent oriented way to deal with human services systems and to interface different processes, as well as increasing the accuracy of electronic social insurance records, is one area where blockchain innovation has colossal potential (EHRs). A study of cutting-edge blockchain research in the field of human services is currently underway. The aim is to highlight the future applications of the technology as well as the challenges and implications of blockchain research in the medical field. First, some background information is presented, followed by a description of the current philosophy in use. Exploratory analysis, probe gathered information including properties, and aftereffects writing finitude assessments are among the study's outcomes. In the end, analysis leads to discussion. According to findings, blockchain technology research in the human services sector is growing, with the technology being used primarily for knowledge sharing, health record management, and access control. There are many transactions conducted in the electronic health records (EHR) system, and the data travelled in the transactions is stored on many peers across the network. The study incorporates a security mechanism that is used to provide security in the transactions of the electronic health records (EHR) system. The aim of this study is to create a protection system for electronic health records (EHR) and to use blockchain technology to enforce a consensus mechanism. A

consensus algorithm was used to secure e-healthcare data obtained from Punjab's tertiary hospitals. To protect healthcare data, the Python programming language is used to enforce a proof of work consensus process. We used 10000 data base rows with 7 attributes data from tertiary hospitals in Punjab for our study, which shows that blockchain is a revolution in providing protection in healthcare data.

Keywords: Distributed Systems; Healthcare; Exploratory; Blockchain

Introduction

Since there are many peers in healthcare where transactions are performed and data is accessed, this research focuses on implementing blockchain technology to provide protection to healthcare data. The enormous value growth of digital forms of money and enormous speculations of investment in blockchain new businesses have largely guided the premium and advancement of this innovation. The demand for blockchain innovation is expected to develop until 2021, according to estimates. As of now, there are approximately 1500 crypto coins that were created just a few years after the introduction of bitcoin. Bitcoin was the first computerized cryptocurrency. It ensures that exchanges are carried out in a localized manner, eliminating the need for a confided in focal point. There is no compelling need to discover someone's personality when open keys are used. Diggers, who receive coins for their fractional work to verify and exchanges (installations) in the Bitcoin blockchain, are an essential part of the Bitcoin arrangement. More information about Bitcoin can be found for those who are interested.

Electronic health care increases the social, health benefit and reduces medical errors. Electronic health record (EHR) is an electronic version of patient's medical records that are conserve using database technologies. Electronic Health Record is electronic patient's health information which is produced by more Care Delivery Organization. The EHR provides the complete record of the patient, which is supported by the different Care Delivery Organization via the interface. Health information like prescriptions, lab reports, patient's medical history etc. With EHRs, patient’s wellbeing data is accessible in one spot, when and where it is required. Suppliers approach the data they need, at the time they need it to settle on a choice. Solid admittance to finish persistent wellbeing data is fundamental for protected and successful consideration.

The blockchain enables substance transactions without the need for a (trusted) third-party. Validators (commonly known as excavators) take the place of outsiders and authorise transfers in a decentralized manner. This is done through a dispersed agreement—the capacity to come to an agreement on something among disparate groups who don't trust one another. In the cryptographic money environment, this computational problem is known as the twofold payment question, which certifies that a certain amount of an advanced coin has not yet been spent without the approval of a trusted outsider (usually a bank) who monitors all exchanges and client adjustments.

As opposed to referenced papers, this work presents an exploratory survey & examination cutting edge blockchain inquire about in the yard of social insurance. The point of our paper is additionally demonstrating chance utilization blockchain in social insurance furthermore, viewing the difficulties & chance bearings of blockchain look into. Our methodical survey just incorporates investigate that presents another solution, algorithm, strategy, approach, or engineering for the yard of social insurance. Survey findings, inactivity potential utilizations of blockchain, outer large distributions are avoided.

Literature Review

The advantages of a dispersed database hold the guarantee of overseeing information in the social insurance industry. Because of the multifaceted nature as far as the partners engaged with the human services organize, a monstrous measure of information must be moved in reverse and advances. The use of blockchain gets significant in managing the need of an assortment of included gatherings to access a similar sort of data. Clinical treatment forms areorganized while considering the additional worth made by blockchain. A pilot venture, in light of the Ethereum stage, which is known as the Gem Health Network, gives distinctive human services master viders full access to reatment data. Such a biological system handles the issues of simultaneous openness, in this way restricting the opportunities for carelessness brought about by obsolete information. Furthermore, operational expenses brought about from keeping up past various databases can be diminished. The sys-tem grants parental figures to follow patients' clinical data on a frequent premise, just as to survey the memorable association between clinical specialists and patients, which consequently improves the straightforwardness and nature of the whole clinical condition.

A dispersed agreement convention characterizes how a system figures out which companion will get ready and seal the most up to date hinder with still unsubstantiated and non-designed information. The most straightforward route is to decide it haphazardly, however such a methodology isn't successful as far as system life span and can even be perilous for the system, since companions could choose to assault the entire system.

The PoW agreement convention is utilized in bit-coin mastermind. Its uses figuring energy as a segment to choose the picked peer. The rivalry betwixt peers depends on hashing unverified exchanges. Along these lines, a companion's possibility of being picked is in relation to its computational force.

The PoS agreement convention depends on the benefits a companion has. A companion's possibility of being picked to affirm another square is with respect to its advantages. Practically speaking, acknowledged include a friend store a predefined least count advantage. Opposition right now not founded on the computational intensity of the companions, which means there is negligible vitality utilization in contrast with the PoW. In any case, such a methodology is like an investor company, where the rich have a bit of leeway.

Blockchain—Distributed LedgerTechnology

Each trade finished by a center point is set apart before it is imparted to the framework for afterward attestation. The propelled checking of a trade utilizing the private key engages confirmation and gives decency trade. The first is a result of the way solitary customer having particular secret key can sign the trade furthermore, a result way that a bumble during transmission of the information realizes the disappointment disentangling. The essential assignments of a blockchain hub are:

- interfacing with the blockchain arrange
- putting away cutting-edge record
- tuning in to exchanges
- passing on legitimate exchanges into the system

Variety of blockchain

By and large, there are various sorts of block chains relying upon oversaw information, on the client's ability to access certain knowledge and what tasks he or she may perform This include the following:

- open permission less,
- cartel,
- snobbish

Everyone has access to and can see all of the details in the free permission less blockchain. Regardless, a few bits of the blockchain may be encoded to compensate for the lack of meaning in a particular part. In an open permission less blockchain, anyone can enter the blockchain and act as a simple hub or an excavator without any approval (hub). These kinds of blockchains are normally given a monetary impetus, for example, in digital currency systems.

Blockchain in Healthcare

To improve medical usefulness, the focus should be on data management, which can benefit from the ability to link different systems and improve EHR precision. Blockchain technology can be used to help calm down solutions and development networks around the board, pregnancy and any hazard information the executives just as to help find a good pace, regulating of clinical activities. Social protection organizations are changing to enable a patientdriven approach. Block-chain based social protection automated-system may upgrade safety & dependability of person's information from person's authority over their therapeutic administrations data sets. Those systems could in like manner help combine tolerant data, enabling the exchanging of clinical records across various restorative administrations establishments.

Taking care of the clinical data of patients is significant in human administrations. These data are very delicate also, right now a practical objective for advanced assaults. It is essential to make sure about each fragile datum. Right now, and finding a good pace of patients' human administrations data is another usage section may benefit by bleeding core current day promotion. Block-chain advancement is hearty against assaults and disappointments, and

deliver various simulations for get to control. Right now way, block-chain gives a better than average structure to human administrations data.

Healthcare information necessitates a high level of security and confidentiality. The term "privacy" applies to people who have the legal authority to authorize or reveal personal details to others. This necessitates collaboration between healthcare providers and regulators, as well as the creation of agreed-upon policies and procedures. The first step in deciding who should have access to confidential patient information is to consider privacy. Numerous security standards, such as HIPAA, COBIT, and DISHA, have been established in response to this problem, and have been used to protect patients' health information. Healthcare providers must also priorities confidentiality in order to protect the privacy of their patients' health details. Thisinvolves maintaining patient information access control, securing patient data from unauthorized users, and modifying and destroying stored data, among other things. As the scale of healthcare data expands, security measures to protect the data are needed. As a result, the US and other countries have established security standards and regulations to safeguard their healthcare data.

In e healthcare distinct security requirement are mentioned in table 1.1. Every security concept takes place numerous transactions in e healthcare. In common cloud based architecture data as directly send to the system is stored in the data base. But using blockchain we can secure data in e healthcare system.

Table 1.1 Users Security Requirements in E healthcare

S. No.	Security concept	Requirements
1	Registration	Verify the authenticity of user
2	Non-repudiation of user action	It is required in e -healthcare that verification one user transaction never deny other user's transaction
3	Non-repudiation of emergency access	E healthcare gives emergency access to users (doctors, patient), due to provide secur ity to one side transaction other transaction not denied
4	Verify user actions	It access user's identity and allowed access
5	Access in transactions	To check the privileges only to the authorized users, allow users to make transactions to the system.

Research Mathodology

Electronic Health Record is electronic patient's wellbeing data which is created by more Care Delivery Organization. The EHR gives the total record of the patient, which is upheld by the distinctive Care Delivery Organization through the interface. This interface having many pathways to get data. Health information like patients registration, approval of their appointments, medical history of patient, doctor's prescription, and progress notes etc. stored directly into data base from different GUI (Graphical User Interfaces). The Electronic Health Record (EHR) with patient's data is viewed as exceptionally delicate in Healthcare association. Delicate data to patients in medical services must be overseen with the end goal that it is free from any and all harm from unapproved access. Electronic Health Record is electronic patients prosperity information gives the absolute record of the patient, which is maintained by the unmistakable Care Delivery Organization through the interface. The NationalAlliance connects the sharing of Electronic health records between different providers for health Information Technology.

In tertiary hospitals of Punjab, trillions of transactions executed on the network in seconds. Using blockchain technology we create and implement security framework on e healthcare system of Punjab using consensus mechanism. In our study we implements proof of work algorithm for secure e healthcare records.

Proof of Work

The prover (requestor) and verifier are two separate parties (nodes) in a Proof of Work (PoW) mechanism (provider). The prover completes a resource-intensive computational task with the aim of achieving a goal and then presents it to a verifier or a community of verifiers for validation. The central concept is that the asymmetry in resource requirements between proof generation and validation acts as an inherent barrier to any device misuse. Within this aim, the idea of PoW was first presentedy Dwork and Naor in their seminal article in 1993. They proposed that PoW be used to prevent email spamming. According to their plan, an email sender will be expected to complete a resourceintensive mathematical puzzle and attach the solution to the email as proof of completion. The email recipient can only approve an email if the solution can be checked successfully.

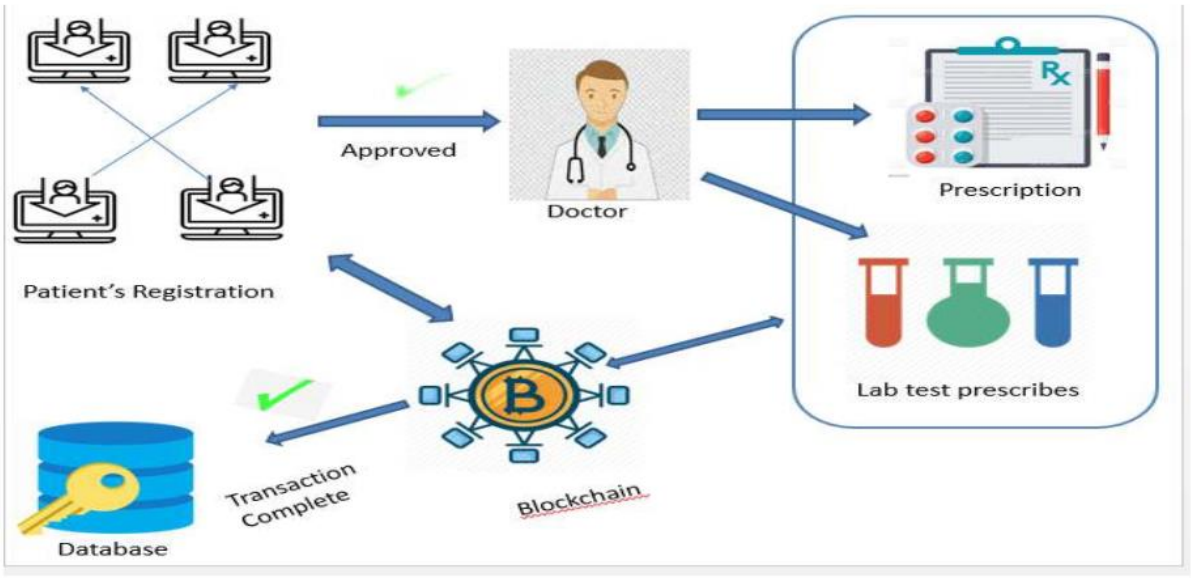


Figure 1:- Implement Blockchain in E-healthcare

Patient's register themselves after successfully registration there details are send to doctor after appointment approval. When doctor got details of patients day wise, according to schedule there patients visit to hospital for their treatments. Doctor gives prescription and lab test according to case. There are different transactions done in this complete work. Our research is emphasis to secure these transactions using blockchain technology.

We are using python for create blockchain in healthcare. Our study is to examine e-Healthcare security challenges in order to address the emerging needs of a national digital healthcare solution. New security concerns arise in transmitting and processing of electronic medical records, personal healthcare records, and patient billing records, as well as public health alerts, across many parties with varying security, privacy and trust levels. Blockchain has numerous potential for healthcare. HER systems are used to maintain electronic healthcare records. Our research is to secure e-healthcare using blockchain technology. In figure-1 we gives an idea that clearly defines our work.

For secure data transaction in blockchain in both patient and doctor side we implement consensus algorithm proof of work. AProof of Work algorithm (PoW) is how new Blocks are created or mined on the blockchain. The goal of PoW is to discover a number which solves a problem. The number must be difficult to find but easy to verify-computationally speaking-by anyone on the network. This is the core idea behind Proof of Work.

In our study we using python to create blockchain. We processing blockchain with proof of work consensus algorithm. Healthcare as an industry has unique requirements associated with security and privacy due to additional legal requirements to protect patients' medical information. The aim of this study is to identify and analyses the security threats that exist for Electronic Health Records health care system. Proposed system secure transactions using blockchain technology using consensus mechanism, records in e healthcare system is encrypt using cryptography and then transfer from one peer to another peer.

Conclusion

Our examination explored flow block-chain investigate slants inside social insurance. The blockchain innovation instant federalized system viewed extraordinary potential for use in medicinal services, due to the touchy idea of information being prepared and overseen. The point examination recognizes the flow status of block-chain research and technology in social insurance. To accomplish this goal, we have characterized look into questions and utilizing the predefined approach. These were then additionally dissected.

Our discoveries demonstrate that blockchain advancement research and its work in human administrations is extending. EHR are now protected using blockchain reason behind that is all transaction in healthcare are secured using consensus algorithm. Moreover, frequently specialized insights regarding the utilized blockchain components aren't give such as, blockchain stage, accord calculation, blockchain type or the utilization of brilliant agreements. Especially, keen agreements could be increasingly utilized as they empower the mechanization of procedures inside a blockchain stage. Most research could likewise give a model usage or if nothing else talk about some execution subtleties of their recommendations.

References

- Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media: Newton, MA, USA, 2015.
- Singh, S.; Singh, N. Blockchain: Future of financial and cyber security. In Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016; pp. 463–467.
- Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Commun. Surv. Tutor. 2016, 18, 2084–2123.

- Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.
- Park, J.; Park, J. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry 2017, 9, 164.
- Yin, S.; Bao, J.; Zhang, Y.; Huang, X. M2M security technology of CPS based on blockchain. Symmetry 2017,9, 193.
- Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology Engineering Management Conference (TEMSCON), Santa Clara,CA, USA, 8 June 2017; pp. 137–141.
- Conoscenti, M.; Vetro, A.; Martin, J.C.D. Blockchain for the Internet of Things:Asystematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
- Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 2016, 11, e016347.
- Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H.Acritical review of blockchain and its current applications. In Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113.
- Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
- Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In Advances in Computers; Elsevier: Amsterdam, The Netherlands, 2018.
- Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc.2017, 24, 1211–1220.
- vAngraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology: Applications in Health Care.Circ. Cardiovasc. Qual. Outcomes 2017, 10, e003800.

- Mackey, T.K.; Nayyar, G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin. Drug Saf. 2017, 16,587–602. Giungato, P.; Rana, R.; Tarabella,A.; Tricase, C. Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. Sustainability 2017, 9, 2214.
- Engelhardt, M. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol. Innov. Manag. Rev. 2017, 7, 22–34.
- Alhadhrami, Z.;Alghfeli, S.;Alghfeli, M.;Abedlla, J.A.; Shuaib, K. Introducing blockchains for healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, 21–23 November 2017; pp. 1–4.
- Sater, S. Blockchain Transforming Healthcare Data Flows. SSRN Electr. J. 2018.\
- Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry.Computer 2017, 50, 18–28.
- Raval, S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, 1st ed.; O'Reilly Media, Inc.:Sebastopol, CA, USA, 2016.
- Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; Alex, R.; Costa, C.A.; Righi, R.R. OmniPHR: A distributed architecture model to integrate personal health records. J. Biomed. Inform. 2017, 71, 70–81.
- Sleiman, M.D.; Lauf, A.P.; Yampolskiy, R. Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System. In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden,7–9 October 2015; pp. 332–336.
- Aumasson, J. Serious Cryptography: A Practical Introduction to Modern Encryption; No Starch Press: San Francisco,CA, USA, 2017.
- Ferguson, N.; Schneier, B. Practical Cryptography, 1st ed.; John Wiley & Sons, Inc.: New York, NY, USA, 03.
- Greenspan, G. Blockchains Vs Centralized Databases; MultiChain: London, UK, 2016.
- Lewis, A. A Gentle Introduction to Blockchain Technology. Bits on Blocks. 2018. Available online: https:// bitsonblocks.net/2015/09/09/gentleintroduction-blockchain-technology/
- Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here.Paper presented at the e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference.

- Chen L, Lee WK, Chang C-H, Raymond Choo K-K, Zhang N. Blockchain based searchable encryption for electronic health record sharin.Fut Gener Comput Syst 2019;95:420–9
- Dwork, Cynthia and Naor, Moni “Pricing via processing or combatting junk mail”. Annual International Cryptology Conference, 139–147, 1992

Appendix C: Conferences Attended

Year	International Conferences Attended	Paper Presented
2019	Business Agility in Volatile times	Data sharing between healthcare system and IOT devices a review study
2021	Business Resilience & Reinvention in the VUCA world	A study to create Secure E healthcare framework using blockchain technology: A case of tertiary hospitals of Punjab
2022	Emerging Trends and latest Research in Computer Science-2022	Blockchain-based electronic healthcare record system for healthcare applications: A case of tertiary hospitals of Punjab
2022	Industry 5.0 Human Touch, Innovation and Efficiency	Lightweight Blockchain for E-healthcare security: A case of tertiary hospitals of Punjab
2022	International E-Conference on Advanced Electric Vehicle Drives ICAEVD – 2022, NIT	Design and Implement of Security Framework For E-Healthcare using Blockchain Technology
2022	International Conference on Blockchain for Business: Embracing Digital Disruptions (BBEDD Conference 2022)	Opportunities of Blockchain in Healthcare: Trial application situations to assess the performance of client/server and blockchain