DATA SECURITY FOR INTERNET OF THINGS USING CRYPTOGRAPHY

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

by

DHARMINDER SINGH

11501055

Supervisor

Ms.AMBICA VERMA

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

June 2017

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M. Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE545 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0287

Supervisor Name : Gauri Mathur **UID :** 11400 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Dharminder Singh	11501055	2015	K1518	08872408007

SPECIALIZATION AREA : Programming-II **Supervisor Signature:** _____

PROPOSED TOPIC : Internet of things(IoT)

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	5.20
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	5.20
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	5.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	5.80
5	Social Applicability: Project work intends to solve a practical problem.	5.20
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	5.60

PAC Committee Members		
PAC Member 1 Name: Janpreet Singh	UID: 11266	Recommended (Y/N): Yes
PAC Member 2 Name: Harjeet Kaur	UID: 12427	Recommended (Y/N): Yes
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 4 Name: Vikas Verma	UID: 11361	Recommended (Y/N): NO
PAC Member 5 Name: Dr. Ramandeep Singh	UID: 14105	Recommended (Y/N): NO
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: **Data security for Internet of Things using cryptography**

Overall Remarks: Approved (with major changes)

PAC CHAIRPERSON Name: 11011::Rajeev Sobti **Approval Date:** 22 Nov 2016

ABSTRACT

The internet of things (IOT) has gained the popularity over the past decade and has found their applications in the various domains. The popular applications of the IOTs focus upon the home security, healthcare, weather, smart city traffic, etc. The IOTs are equipped of the small sensors for the collection of the data, which is processed in event-based or time-based paradigms according to the nature of the data on arrival. In both of the paradigms, the data is first received upon the aggregation node, which collects all of the data from the IOT nodes in the given network. The collected or aggregated data is further analyzed for the discovery of the desired patterns or parameters to observer the specific properties or variations. The security of IOT raises the major concerns as the IOTs are equipped with the limited resources based sensor nodes. Hence, these sensors must be provided with the light and efficient security algorithm for the enforcement of data privacy and user integrity in the given network. The two major security paradigms for IOTs are authentication & encryption mechanisms, which have many variants. In this thesis, the work has been carried over the enhancement of the proposed security model by designing the authentication model with set of algebraic equations. The multi-column based complex key generation is designed around the algebraic equations, specifically cubic and quartic equations.

The authentication keys and data encryption is another security paradigm of the proposed model, which utilizes the advanced encryption standard (AES), which has been used for the implementation of the high security protocols. The performance of the proposed model has been analyzed under the different scenarios with variable number of nodes (50, 100 and 150) with decreasing transmission range of 75, 50 and 25 respectively. The proposed model has been recorded with minimum projected resource readings at 1.09, 5.49 and 10.96 percent in the scenarios with 50, 100 and 150 nodes respectively, whereas the maximum readings are 1.95, 9.81 and 19.63 percent for similar scenarios. The maximum value of entropy has been recorded at 2.98, 3.39 and 3.29 for proposed model against the 2.26, 2.53 and 2.39 existing model, which shows the robustness of the proposed security model for IOTs. The minimum values of entropy are recorded between 1.99 and 2.16 for proposed model against the existing range of 1.61 and 1.77 for the entropy, which again shows the similar trend to the latter analysis. Hence, it shows the clear improvement of proposed model against the existing model in all experiments.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled "DATA SECURITY FOR INTERNET OF THINGS USING CRYPTOGRAPHY" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Ms.AMBICA VERMA. I have not submitted this work elsewhere for any degree or diploma. I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate
DHARMINDER SINGH
11501055

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "DATA SECURITY FOR INTERNET OF THINGS USING CRYPTOGRAPHY", submitted by DHARMINDER SINGH at Lovely Professional University, Phagwara, India is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor
Ms.AMBICA VERMA
Date:

Counter Signed by:

1) Concerned HOD:

HoD's Signature:_____

HoD Name:_____

Date:_____

2) Neutral Examiners:

External Examiner_____

Signature:_____

Name:_____

Affiliation:_____

Date:_____

Internal Examiner_____

Signature:_____

Name:_____

Date:_____

ACKNOWLEDGEMENT

This thesis is the culmination of my journey of Masters which was just like climbing a high peak step by step accompanied with encouragement, hardship, trust, and frustration. When I found myself at top experiencing the feeling of fulfilment, I realized though only my name appears on the cover of this dissertation, a great many people including my family members, well-wishers, my friends, colleagues and various institutions have contributed to accomplish this huge task. First and foremost, I offer my sincerest gratitude to my supervisor, Ms.Ambica Verma, who has supported me throughout my thesis with his patience and knowledge whilst allowing me the room to work in my own way. I attribute the level of my Master's degree to his encouragement and effort and without him this thesis, too, would not have been completed or written. One simply could not wish for a better or friendlier supervisor. I acknowledge the people who mean a lot to me, my parents, Jagraj Singh and Swarnjeet Kaur, for showing faith in me and giving me liberty to choose what I desired. I salute you all for the selfless love, care, pain and sacrifice you did to shape my life. Although you hardly understood what I researched on, you were willing to support any decision I made. I would never be able to pay back the love and affection showered upon by my parents. Also, I express my thanks to my sister Rupinder Kaur for her support. I thank the Almighty for giving me the strength and patience to work through all these years so that today I can stand proudly with my head held high.

DHARMINDER SINGH

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Introduction to Wireless Sensor Network

Internet of things (IoT) combines the certain number of sensor node for incorporation of the network. Internet of Thing (IoT) network is created such that it gives continuous data and investigation of low level information in threatening condition. [1] The IoT sensor nodes speak with each other without physical system through radio flag. [3] The remote systems function as transmission media among a few gadgets. Internet of things gadgets are self-controlled and can adapt to the wireless network scenarios automatically. The hubs of remote system are made out of limited memory, sensor, a radio handset and adequate power source, for example, battery. IoT is an extraordinary kind of ad-hoc network system. [16]

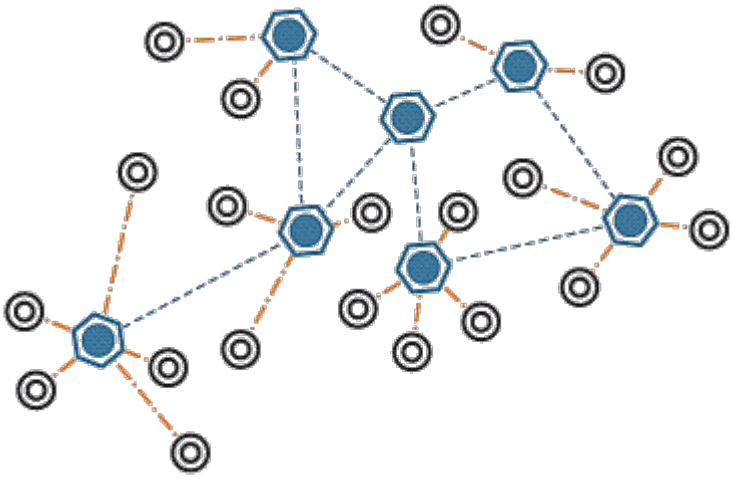

Figure 1.1: An example of wireless sensor network (WSN) [23]

The correspondence or data given by IoT is required to have information respectability, the information which is exchange by the sender is not temper or changed on the way from sender to collector. [2] In the remote system time synchronization is normal with the end goal that there is nonattendance of deferral in parcels when it is exchange between two hubs. Classified data is

foreseen in remote system it signifies specific data must be kept from endowed outsider. [6] The hubs of remote sensor arrange is conveyed in ill-disposed condition so it is energy preservation capability against attacks. IoT are imperiled to security assault inferable from communicate nature of transmission medium. [1, 5-7]

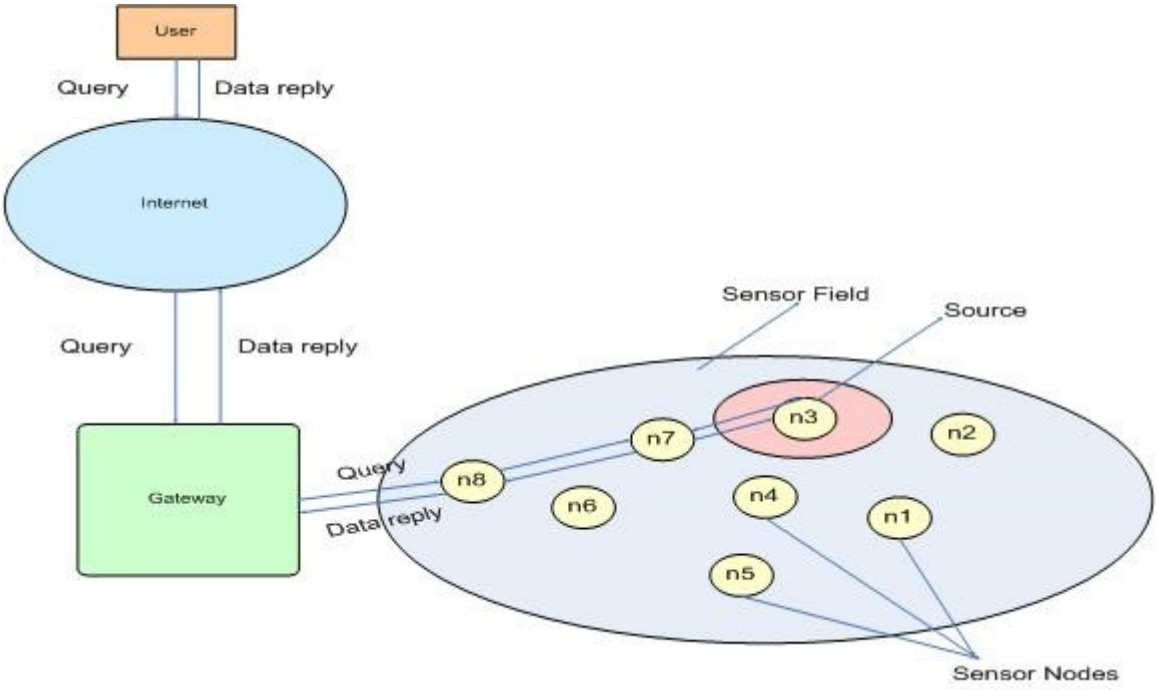

Figure 1.2: Internet Protocol (IP) based Wireless Sensor Networks [13]

A Internet of Things network is an accumulation of IoT sensor nodes, which develops a system utilizing radio correspondence in a self-governing and circulated way. [5] Nodes are dispersed over a particular field, and can gather and transfer data about nature, keeping in mind the end goal to give fine-grained perceptions of a marvel. [14] A sensor hub is ordinarily outfitted with at least one sensors that are utilized to catch occasions from the earth, a simple advanced converter, a radio handset, a focal preparing unit with constrained computational capacities, a little measure of memory and a battery control supply. Sensor gadgets work together with each other so as to perform fundamental operations, for example, detecting, correspondence and information preparing. [21]

Real applications utilizing IoTs include: natural observing, human services, mind-set based administrations, situating and creature following, amusement, coordinations, transportation, home and office, modern and military applications. Non-nosy and non-troublesome ecological checking enables researcher to consider delicate natural life territories, for instance the smaller scale atmospheres on Great Duck Island, Maine. Medicinal services applications empower individuals with certain restorative conditions to get consistent observing through sensors. Military applications

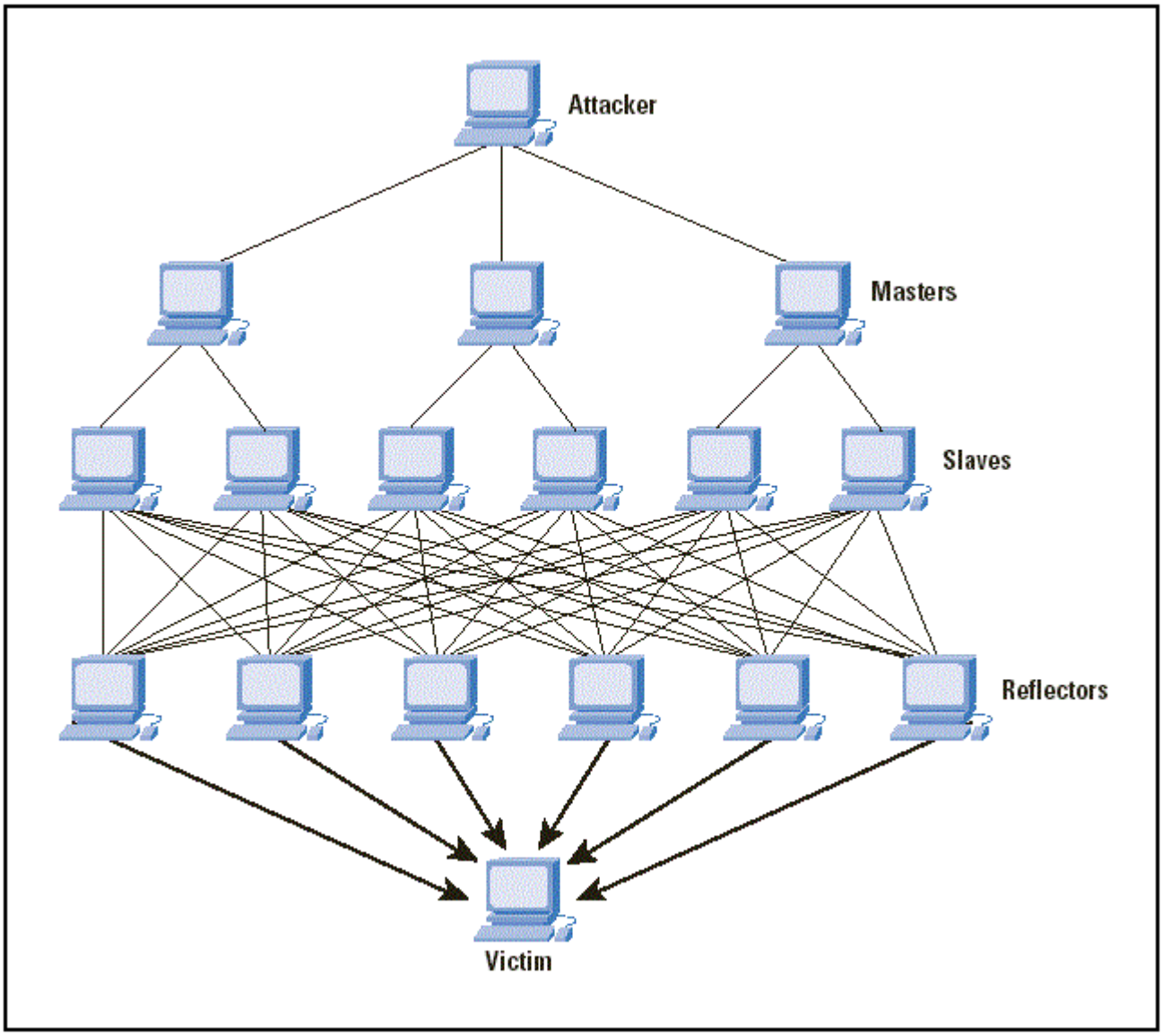

Figure 1.3: An example of hierarchical DDoS attack [6]

incorporate observation, target following, counter-expert sharpshooter frameworks and war zone checking, in which data is proliferated to officers and vehicles required in battle. [21-23] The innovative headways in remote correspondence and microelectronics have brought about a developing enthusiasm for the field of remote sensor systems. A sensor arrange includes sending a variety of sensors for appropriated observing of constant occasions. [26] The sensor systems have constrained vitality, as the IoT sensor nodes are battery controlled. The IoT sensor nodes additionally have constrained memory and computational ability and can be conveyed in remote ranges or unfriendly territory. There has been an expanding utilization of sensor systems forever basic applications, for example, checking patients in healing centers and military applications. [8] These applications make it imperative to have a decent security framework for sensor systems. The arrangement of these systems in military applications and the constrained power and memory, make the outline of

a security convention extremely difficult. [7,11] In this paper security issues in Directed dissemination are tended to. Coordinated Diffusion is a novel steering convention for sensor systems. A look-into conceivable assaults and counter measures is given. The paper is finished up with a short investigation on the conceivable countermeasures to forestall such assaults. [2]

1.2 WSNs and Health-Care Monitoring Network

Social insurance is dependably a major worry, since it includes the personal satisfaction a given individual can have. It is constantly preferable to keep an ailment over to treat it, so singular observing is required as an intermittent action. The maturing populace of created nations show a developing cut of government's financial plan, and introduces new difficulties to social insurance frameworks, to be specific with elderly individuals living on autonomous senior lodging. Customarily, wellbeing observing is performed on an occasional check premise, where the patient must recall its manifestations; the specialist plays out some check and defines a demonstrative, at that point screens understanding advancement along the treatment, if conceivable. In any case, a few side effects just show themselves in day by day exercises, where an individual may feel some torment or inconvenience. Human services uses of remote sensor systems permit in-home help, shrewd nursing homes, clinical trial and research expansion. In-home human services winds up plainly compulsory for sicknesses like Parkinson or Alzheimer, giving memory improvement through drug updates, mental incitement through sounds or pictures of question's area, control over home machines, medicinal information query, and crisis circumstances. Such approach may prompt a multi-layered design, with lightweight portable PCs and savvy sensors in conjunction with all the more intense computational gadgets. Before portraying and reviewing restorative applications for human services, this segment concentrates on a few difficulties and general angles that describe this sort of advances.

1.2.1 Challenges

Human services applications introduce a few difficulties: low power, restricted calculation, material limitations, persistent operation, heartiness and adaptation to internal failure, versatility, security and obstruction, and administrative prerequisites. The power challenge is available in practically every territory of utilization of remote sensor systems, yet restriction of a keen sensor embedded on a man still stances significantly additionally challenge, albeit progressing research tries to give control remotely. Another test as far as power originates from the operational warmth. For example, at times it is impractical to chill off the sensor by permitting contact with the earth. A commonplace

soluble battery, for instance, gives around 50 watt-hours of vitality. This may mean not as much as a time of ceaseless operation for every hub in full dynamic mode. By and by, for some applications, it will be important to guarantee that a system can stay operational with no substitutions. Calculation is specifically restricted because of the constrained measure of energy. Ordinarily, biosensors are not anticipated that would have an indistinguishable computational power from traditional Internet of Things hubs. Since correspondence is indispensable and impression is little, little power stays for calculation. An answer can be information combination, which involves a few hubs pooling their data together for expanded computational power handling and precision. Additionally, it might be normal that for a few applications, for example, blood glucose checking, the capacity to transmit information to an outer gadget will be required for encourage information handling. A few sensors may have differing capacities that speak with each other and convey one community information message. Material requirements is another issue for remote sensor systems application to medicinal services. A biosensor must be in contact with human body, or even on it. In the event that the biosensor is inside a pill, the decision of development materials must be cautious, particularly on batteries. Likewise compound responses with body tissue and the transfer of the sensor is of most extreme significance. In numerous applications, it is conceivable to dispose of at least one brilliant sensors without the requirement for any administrator intercession. Ceaseless operation must be guaranteed along the lifecycle of and openings. The regularly inspiration for aggressor is advantage from information. Aggressor openings extend from physical get to, remote correspondence, assaults on coordination and self-design, up to organize perceivability. Administrative necessities should dependably be met, significantly more with medicinal applications. There must be some confirmation that these gadgets won't hurt; even model gadgets should meet the strict guidelines of patient security before any human testing should be possible. The remote information transmission must not hurt human body and the incessant working and power usage of these gadgets should likewise be kind. Plan for security must be a key component of biomedical sensor advancement, even at the soonest arranges. Sensible confirmation of plan viability will be required notwithstanding for model gadgets.

1.3 Cloud Integration of Health-Care Monitoring WSNs

Internet of Things (IOT) normally comprises of an accumulation of sensors with their own energy supply, remote correspondence, information stockpiling, and information preparing ability. In an average sensor organize, every sensor hub has a microchip with constrained handling capacity, a little measure of memory for flag preparing and has restricted vitality supply and transmission

capacity. Every sensor hub discusses remotely with a couple of other nearby hubs inside its radio correspondence go. Data gathered by and transmitted on a sensor arrange depicts states of physical conditions—for instance, temperature, moistness, or vibration. Uses of sensor systems are boundless and can differ fundamentally in application prerequisites. Test applications include: Traffic checking, Habitat observing, Forest fire recognition, Natural catastrophe counteractive action, Healthcare checking and so forth. Distributed computing is the utilization of registering assets (equipment and programming) that are conveyed as an administration over the system (chiefly the Internet). Cloud has bounteous preparing power, expansive measure of capacity which can be scaled by application needs. Present day innovation is being moved to Cloud based stage as it is suited for long haul information stockpiling. The proposed framework concentrates on gathering of patient's indispensable wellbeing parameters and creates caution to overseers, specialists so that quick move can be made if there should be an occurrence of crises. The information is then put away in Cloud with the goal that information can be gotten to through Internet from anyplace whenever. Sensors are utilized to gather wellbeing information from patients. Rather than appending sensors to therapeutic supplies, wearable sensors are connected to human body which persistently screen the pulse rate, pulse, fall discovery, and so on. These IoT sensor nodes help in persistent wellbeing observing of post agent patients at healing center and elderly patients at home condition with continuous updates of therapeutic records. The information are distributed through web servers. Medicinal services experts, analysts and patients can get to the long haul physiological information by means of the Internet. A protected cloud server enables confirmed clients to get to constant patient data. Noncontact electrocardiogram (ECG) estimation strategy has picked up fame nowadays inferable from its noninvasive elements and accommodation in day by day life utilize. This paper presents versatile distributed computing for a human services framework where a noncontact ECG estimation technique is utilized to catch biomedical signs from clients. Social insurance benefit is given to consistently gather biomedical signs from numerous areas. To watch and break down the ECG motions continuously, a cell phone is utilized as a versatile observing terminal. Likewise, a customized medicinal services right hand is introduced on the cell phone; a few social insurance elements, for example, wellbeing status outlines, pharmaceutical QR code filtering, and updates are incorporated into the portable application. Wellbeing information are being synchronized into the social insurance distributed computing administration (Web server framework and Web server dataset) to guarantee a consistent medicinal services checking framework and whenever and anyplace scope of system association is accessible. Together with a Web page application, therapeutic information are effortlessly gotten to by restorative experts or relatives. Website page execution assessment was directed to guarantee insignificant Web server dormancy. The framework exhibits

better accessibility of off-site and up-to-the-minute patient information, which can help identify medical issues early and keep elderly patients out of the crisis room, consequently giving a superior and more thorough social insurance distributed computing administration

1.4 Security and Security Issues in WSN

The security of Internet of Things (IOT) can be traded off from various perspectives. [23] A remote end client getting to base station data can be kept from doing as such in an assortment of ways. Correspondence between the base station and IoT sensor nodes can be blocked. This can be proficient by simple sticking of signs or by computerized sticking as DoS (Denial of Service) assaults that surge the system, base stations or both. Directed DoS assaults on key hubs in the IOT can likewise piece correspondence of huge parts of the system with the base station. Correspondence between base stations and other IoT sensor nodes can be averted by setting up erroneous directing data with the goal that movement goes to the wrong goal or circles. One approach to do this is to parody the base station and beguile hubs into rerouting all bundles to the caricature base station rather than the genuine base station. [23, 24] Another method for breaking security is to decimate the base station itself. This can be proficient by checking the volume and bearing of parcel activity toward the base station so that the area is in the long run uncovered. [7] Destruction can likewise be proficient by tuning in to the RF signs to limit and triangulate the area of the base station. A third risk is listening in. This is made less demanding by remote bounce to-jump correspondence. Listening stealthily can be utilized to track and derive the area of the base station for demolition. There are numerous different strategies to rupture the IOT security. [18]

Assault on IOT can be happening in various techniques. IOT is inclined to security assaults which are submissive in character. [7] The most natural security assaults on IoT sensor nodes is Monitor and Eavesdropping in this assault the adversary could without much of a stretch discover the data content by snooping the data. [12-13] Security of IOT is the most noticeable issue. The Security assaults which occur on remote system are of unmistakable sorts. False steering Information is a Routing Attacks in Sensor Networks the programmer change the directing information of steering conventions through malignant code. [12-13] Wireless system is likewise undermined by Sybil Attacks through this assault a delicacy of single hub is made and speaks to its various personalities to different hubs in remote system. [9] In wormhole assault the foe hold data from one area in the system transmit into another area and on the other hand retransmit into the system. Specific Forwarding is a dynamic assault in this sort of assault the programmers assaults the specific

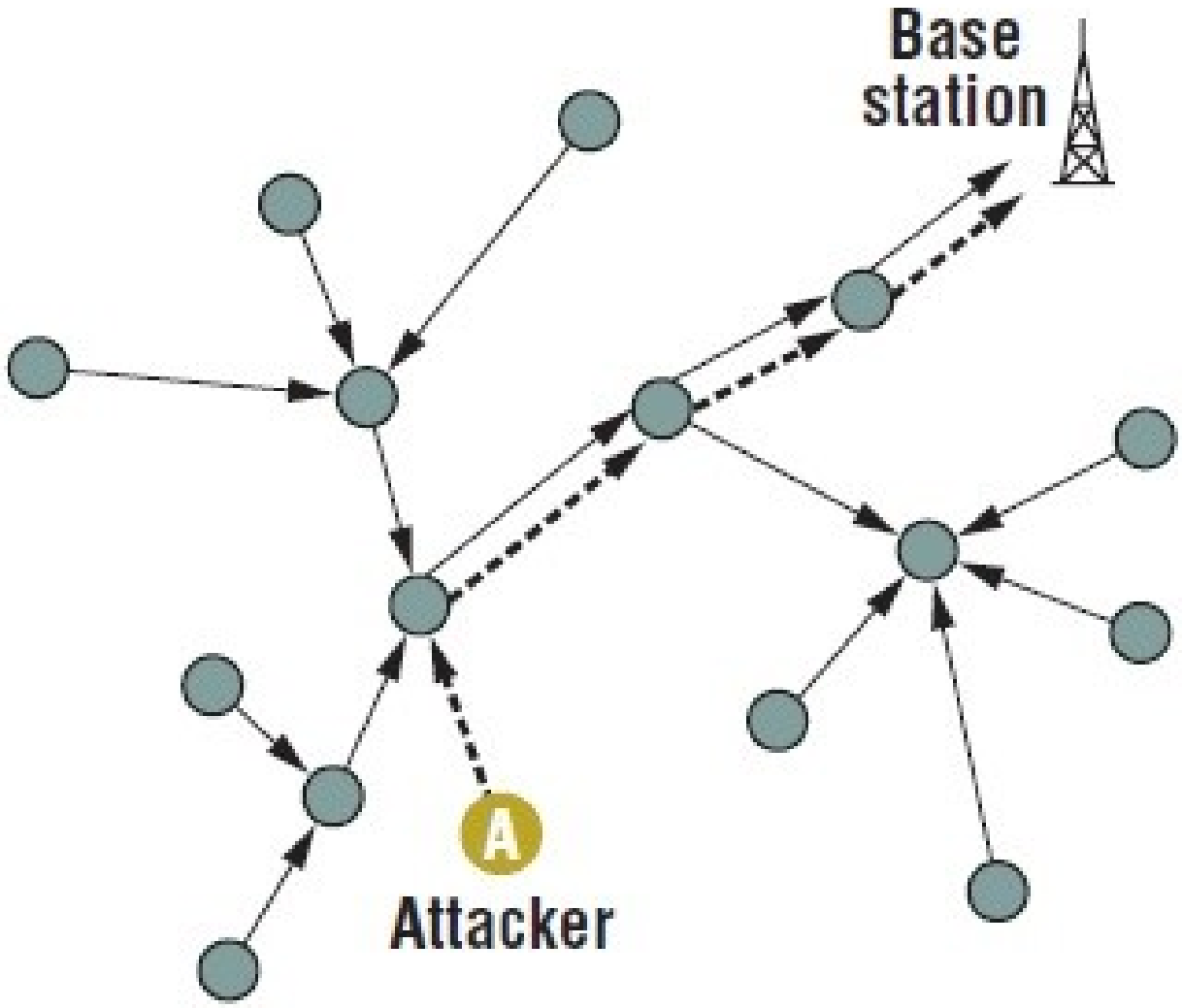

Figure 1.4: Attacks on wireless sensor network [13]

hub and contaminate with the vindictive data the irresistible hub act like a typical hub in organize this hub does not forward the parcels or information to next hub it just which make them act like a fizzled hub. [34]

1.5 Requirement of Cryptography Key Exchange in Cloud Based WSNs for Health-Care Monitoring

A Internet of Things (IOT) is an accumulation of IoT sensor nodes, which develops a system utilizing radio correspondence in a self-sufficient and appropriated way. Hubs are appropriated over a particular field, and can gather and hand-off data about the earth, keeping in mind the end goal to give fine-grained perceptions of a wonder. A sensor hub is ordinarily outfitted with at least

one sensors that are utilized to catch occasions from the earth, a simple computerized converter, a radio handset, a focal preparing unit with constrained computational abilities, a little measure of memory and a battery control supply. Sensor gadgets work together with each other so as to perform fundamental operations, for example, detecting, correspondence and information preparing. Real applications utilizing IOTs include: ecological checking, social insurance, state of mind based administrations, situating and creature following, amusement, coordinations, transportation, home and office, mechanical and military applications. Non-meddling and non-troublesome natural checking enables scholars to contemplate touchy untamed life living spaces, for instance the smaller scale atmospheres on Great Duck Island, Maine. Medicinal services applications empower individuals with certain restorative conditions to get steady checking through sensors. Military applications incorporate observation, target following, counter-expert rifleman frameworks and front line checking, in which data is spread to troopers and vehicles required in battle. The mechanical headways in remote correspondence and microelectronics have brought about a developing enthusiasm for the field of remote sensor systems. A sensor organize includes sending a variety of sensors for circulated checking of constant occasions. The sensor systems have constrained vitality, as the IoT sensor nodes are battery fueled. The IoT sensor nodes likewise have restricted memory and computational ability and can be sent in remote territories or aloof landscape. There has been an expanding utilization of sensor systems forever basic applications, for example, checking patients in healing facilities and military applications. These applications make it critical to have a decent security framework for sensor systems. The arrangement of these systems in military applications and the restricted power and memory, make the plan of a security convention exceptionally difficult. In this paper security issues in Directed dissemination are tended to. Coordinated Diffusion is a novel directing convention for sensor systems. A look-into conceivable assaults and counter measures is given. The paper is finished up with a concise examination on the conceivable countermeasures to anticipate such assaults. The security of Internet of Things (IOT) can be traded off from multiple points of view. A remote end client getting to base station data can be kept from doing as such in an assortment of ways. Correspondence between the base station and IoT sensor nodes can be blocked. This can be proficient by simple sticking of signs or by computerized sticking as DoS(Denial of Service) assaults that surge the system, base stations or both. Directed DoS assaults on vital hubs in the IOT can likewise piece correspondence of extensive parts of the system with the base station. Correspondence between base stations and other IoT sensor nodes can be averted by setting up mistaken directing data with the goal that movement goes to the wrong goal or circles. One approach to do this is to parody the base station and betray hubs into rerouting all bundles to the ridiculed base station rather than the genuine base station. Another

method for rupturing security is to annihilate the base station itself. This can be proficient by observing the volume and heading of bundle movement toward the base station so that the area is in the long run uncovered. Devastation can likewise be proficient by tuning in to the RF signs to limit and triangulate the area of the base station. A third risk is listening in. This is made simpler by remote jump to-bounce correspondence. Listening stealthily can be utilized to track and derive the area of the base station for obliteration. There are numerous different strategies to break the IOT security. Amid the periods when the IOT hubs are in working condition, they require secure cryptographic keys for secure proliferation of the delicate data. Effective key administration and conveyance plot assume a critical part for the information security in IOTs. Existing cryptographic key administration and circulation procedure for the most part devour higher measure of vitality and put bigger computational overheads on Wireless Sensor Nodes. The cryptographic keys are utilized on various correspondence levels of IOT interchanges i.e. neighbor hubs, group heads and base stations. A compelling corporate key administration and appropriation strategy is required to keep up the security of the remote sensor systems.

Chapter 2

REVIEW OF LITERATURE

2.1 Body Area Networks for Health Monitoring

Rosenthel et al. [**21**]had taken efforts to provide advantage of cloud computing for biomedical informatics (BMI) community for sharing medical data and applications. This paper aimed to help the biomedical community such as laboratories, funding agencies, and hospital management to understand the advantages and access capabilities of particular cloud. The main requirement to shift towards cloud technology was in hi-tech laboratories that share information outsides such as investigation associations at cheaper compute resources ranging from computational operation to archival storage. Labs engaged in expensive research computations required machines with fast interconnection among processors, while international medical repositories such as SwissProt and GenBank need vast storage. Among these edges are biomedical consortia that require storing medical data and applications and exchanging among its participants. The various qualitative benefits are less to manage, scalable, superior resilience, homogeneity. But the various challenges encountered were against the security of data stored in cloud such as risk due to hackers, nontechnical outsourcing risks etc.

Rolim et al. [**20**] proposed a system for automating the task of collecting patient's crucial health data through sensor network attached to legally authorized medical devices and storing this data to medical centre's "cloud" for handling, executing, and sharing. The patient's body was implanted with sensor nodes equipped with software for collecting, encoding, and transmission of patient information through wireless medium to the medical cloud server. The proposed Exchange Service was an intermediate between local and remote services. The Exchange Service model was required to receive collected information from sensors and then to forward and store it to appropriate storage servers hosted by cloud.

Sebastian et al. [**12**] worked upon development of remote patient monitoring (RPM) system

supporting universal serial bus plug-in. This research was mainly carried out as an educational tool for poor child charity under the" One Laptop per Child" scheme. All those sensors were based on reduced platform technology and low-cost materials were used. Those sensors were also reliable to work in extreme conditions such as open environment and mishandling by children. The RPC range included in this architecture was of net-book computing devices class and mobile processor running at sub-gigahertz speeds was used. Still, this architecture was capable of hosting most popular operating systems such as MS Windows XP, Solaris & Linux and while consuming 1/5 to 1/10 of the energy power consumption of a normal processor and processing power was also reduced to one-third. The results showed success in power consumption and bandwidth consumption graphs. As there was no option for scalability so there was strong need to develop a mechanism for resource utilization.

Pandey et al. [**19**] developed a prototype system for analysing ECG signal by collecting ECG data in real-time from patients. An implanted wireless ECG sensor collecting patient's data forwards it to handheld via Bluetooth technology. A 3G data network in the mobile device uploads the patient information to the ECG analysis Web Service, hosted on Cloud server. After performing numerous analyses on data, the results are uploaded back to patient's historic record from where authorised persons such as patient, doctor, hospital staff etc. can access it from anywhere. Monitoring of patient was repeated on timely basis i.e. hourly, daily, weekly or monthly. The authors demonstrated the case study in two phases: Initially the computing nodes (VMs) were 25 and there was no scalability of adding more resources with the increased workload. In this setup the response time steadily increased from 30s to 90s when the user requests increased from 80 to 2000. In setup 2, a dynamic resource allocation policy was adopted by with scalability of upto 50 VMs. The response time noted was lower using dynamic allocation policy Setup-2 than that by the Setup 1 for high computational load.

Akm et al. [**1**] proposed a distributed, energy efficient electronic health platform called mHealthMon in which distributed P2P network was created among mobile patients to access patient data collected by sensor from cloud computing-based storage. The basic objective was to satisfy QoS of mHealthMon by modelling each module such as: patient equipped medical sensors, heterogeneous cloud services and wireless communication medium. Empirical measurement based regression theory was applied in developing computational capability of mobile applications. Empirical parameters based mathematical network model was applied for modelling environment interfaces as in WiMAX, WLAN and cellular network. This mHealthMon architecture performed at least 2 times better results for time and energy saving as compared to non-parallel offloading techniques alike MAUI and Clone Cloud

Wan et al. [24] conducted a study on high packet drop and poor network performance because of environmental obstacles. So the authors proposed the use of IEEE 802.15.6 MAC protocol. It was an exclusively designed protocol for WBANs to increase network performance, decrease packet drop ratio and overall energy consumption by connecting the nearby nodes. A public key re-encryption process was used to encrypt content before uploading it to medical cloud data; another user requesting it could download it directly but the content will only re-encrypted to readable form if the user has access rights i.e. private key. The authors highlighted energy-efficient routing protocols, resource allocation methods, semantic interaction models, and information security mechanisms for transmission of essential health data to the cloud in WBAN. There was a demand to work upon the QoS feature to enhance the services of WBAN as it has many limitations due to requirement of large processing power, mobility of patients, and the network coverage area of sensor node.

Almashaqbehet al. [3] proposed real-time remote health tracking system for non-hospitalized patients. This system divided the cloud architecture as local one that contains patients and hospital medical staff, and a global cloud that contains the outer world. The performance parameters to be optimized were congestion reduction, interference and data delivery delay in mobile sensor network. Firstly, data classification and aggregation was employed to optimize the network clogging. Secondly, a dynamic channel assignment strategy was built to distribute available frequency channels to WBANs to handle interference. Thirdly, a delay-aware routing metric was built for multi-hop communication in local cloud to speed up the response process. The simulation environment was ns-2. The simulation results achieved success in optimizing the end-to-end delay, lowering down the increased interference, maximizing the network scalability, and tracking user's mobility.

2.2 Cloud Computing and its application to Health-Care Domain

Hossain et al. [15]termed cloud computing through NIST as a model for pervasive, accessible, demand-driven network access to resources such as network bandwidth utilization, storage, software services etc. from shared pool of computing resources that can be easily available with nominal management attempt. The five key characteristics of cloud model were demand-drive services, high bandwidth network access, Resource pooling, Scalability, Measured service.The service models provide services at software, infrastructure and platform layers e.g. SaaS, PaaS, IaaS. The four deployment models were Private cloud, Hybrid cloud, Community cloud, Public cloud.

Wang et al. [25] discussed that in traditional IT solutions, the IT services were hosted under

complete physical and personnel controls whereas, cloud computing shifted the application and databases phase to large data centre servers on the Internet. This shift gave rise to many software and data security, recovery, and privacy related problems. The authors focused on security of data storage in cloud. The main privacy concern proposed was encryption before data outsourcing and use of authenticated such as Merkle hash tree (MHT) type data structures. To further harden the security of data operations, MHT was integrated with homomorphic- authentication technique. Security of cloud computing was still an area of challenges and require improved security attempts for many years to come.

Fan et al. **[9]**proposed a "Data Capture and Auto Identification Reference" (DACAR) platform for developing eHealth applications equipped with authentication, integrity, confidentiality, authorisation, secure data transmission. It was a hardware and software suite to integrate, capture, store and consume sensitive medical data and supports large scale health services using Cloud infrastructure. Main attributes of the system was Single Point of Contact (SPoC), Data Sharing Strategy, and the Data Buckets. DACAR protocol was implemented in C# and data sharing policy was implemented in Java. Data Bucket hosted over IIS 7 web server supported SQL Server 2008 as back end. The experimental results showed that there was small communication latency and hence it was efficient platform for development of real-time eHealth applications. The future goal was to build a bridge among DACAR and eHealth platforms like Microsoft's Health Vault to secure the sharing of health data on larger scale.

Mohammad et al. **[26]** presented K2C (Key To Cloud) -a scalable and lazy revocation based protocol to share and store data securely in untrusted clouds also. Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption were used for access control, key updation and authorisation. The open source implementation effectiveness was demonstrated over Amazon S3 API. The future research of system was to use proxy re-encryption to improve K2C efficiency and access control protocol by off-loading the task of key distribution to the cloud.

Fitch et al. **[10]** addressed the various concerns of Cloud such as data security, reliability, and availability and the threats such as network outage, data breaches, and exploitations. So the authors developed a novel security solution to cloud storage based on hierarchical colored Petri nets (CPN). They defined Petri net as a directional, connected, and bipartite graph, where each node either represents a place or transition whereas tokens represent information in the places. Transition would be fired only if there was at least single token in each input place. Colored Petri nets, an extension of Petri nets model, denotes different colors to tokens having different values. This CPN model had taken multiple cloud service providers in the form of cloud cluster for data storage. At the primary level, RAID5 technique divided the information into multiple pieces before

storing while keeping distribution parity as a backup resource to information if the provider fails. At the second level, symmetric key encryption played an important role to ensure that non-authorised persons don't have access to the underlying data. This approach had not only taken step towards upholding the confidentiality of the data store, but also guarantees that the failure or compromise of single entity does not affect the security of whole cluster.

2.3 Encryption Standards for Authentication in Health-Care

Smid et al. [**22**] discussed that in 1972, the National Bureau of Standards (NBS) had taken an initiative to develop computer data protection standards. A single basic standard was not efficient for different algorithms to achieve telecommunications interoperability because some applications required an interface standard (i.e. RS-232C interface device for data encryption) while others don't (e.g., secure mail systems). The proposed DES performed both data encryption and authentication. The DES algorithm was the most widely accepted and an earmarked crypto-algorithm for many years.The DES algorithm had led the path for many other security considerations. Despite all functionalities, the major flaw encountered in DES was systematically testing keys till the correct key waslocated. If anyone got keyshe/she could easily calculate both the encryption and its inverse using the function.As the highly secure cryptography had high implementation costs, which attracted less consumerswhich in turn increased the cost of individual equipment's.

Miller et al.[**16**] proposed advancement over DES popularised as Advanced Encryption Standard (AES). AES was symmetric-key encryption standard of U.S. government. AES initially published as Rijndael. AES algorithm had 10 rounds for 128-bit key, 12 rounds for 192-bit key, and 14 rounds for 256-bit key. The AES ciphers had been tested and used worldwide. Till today there is not a single security breach in AES. A theoretical analyzed key attack was that 256-bit AES cipher could be broken with a complexity of 299.5 and 192-bit AES with 2176 complexity but both are infeasible states. 128-bit AES was not distressed by this type of attack.

Om et al. [**23**] presented the performance analysis of data encryption algorithms:DES, 3DES, Blowfish and AES. In this research, the author have presented two main characteristics that identifies and distinguishes each encryption algorithm from another are: the ability of the algorithm to protect the data against attacks, the speed and efficiency of protection. This performance efficiency test was performed using different size blocks of data and on different hardware and software platforms. The results demonstrated that blowfish was the fastest encryption algorithm in consideration

of unauthorised access and speed.

Lee et al. [**11**] presented an implementation architecture exhibiting a latest security equipped, low-power consumption, secure transmission based Bluetooth chip and biomedical sensors equipped fabric belt for body temperature checking and ECG/Heartbeat monitoring. The implementation scenario consists of public key cryptography,polynomial-based encryption, key agreement through a third party, a confident ad hoc routing protocol. The proposed scheme had chosen AES with 128-bits blocks and moved over SAFER+ scheme as SAFER+ was vulnerable to attacks. PDA and Laptopapplications interface was developed using Java platformcreatingan easy to use and portable environment. This only area where the scheme lacks was the need to enhance the system to opt for IPv6-enable sensor networks. Another area of research was biomedical sensor positioning and attacks launched at particular location of elderly or chronic patients when the patient enters that location.

Akinyele et al.[**2**] discussed the ease to offline access mode- the systems should export EMRs securely from the hospital's trust boundary like EMRs maintained by patients store health records to cloud storage e.g. MS HealthVault, Regional Health Information Organizations. Thus thiseradicated the requirement to have a high security access policy to online server to maintain record confidentiality because individual information contents could be stored in encrypted form using different security policies. Therefore, the encrypted records provided the ease to store them at any untrusted locations, like cloud systems, mobile devices, and RHIOs.For the purposed scheme, the authors suggested role-based access control as well as content-based access control. Thus, Attribute based encryption (ABE) could encrypt fields in EMRs to limitread access to data also.

Alshehri et al. [**3**]proposed topractise Ciphertext-Policy Attribute-Based Encryption (CPABE) for encrypting Electronic health records (EHRs)using the identifications or attributes of healthcare provider. To decrypt and access EHRs, the same set of attributes were needed for authentication.Pairing Based Cryptography library was usedfor bilinear mapping on pairing-based cryptosystems.In CPABE scheme, encryption key was shared by healthcare providers and each provider had a unique secret key for decryption. A set of attributes were associated with each secret key according to access policy. A particular ciphertext could only be decrypted using secret key if the attributes of healthcare provider matches the access policy. CP-ABE had complex strategies to denotethat which ciphertexts could be decrypted by which secret key The configuration of virtual machine was1GB RAM, and processor of on 2.26GHz.

Li et al. [**14**] had proposed a patient centric framework to control data access to personal health record. An attribute based encryption technique was leveraged to encrypt each file. The file is encrypted in PHR in order to achieve fine-grained data access control. The authors had

focused on multiple data owner scenario. Lazy-revocation method was used to cut the costs of revocation, because it combined numerous cipher text/key update operations, which resulted in reduced computations per time.

2.4 QRS Detection Algorithms for Heart Monitoring

Pan et al [**18**] had taken an initiative to develop a real-time algorithm for recognition of the QRS complexities on the basis of slope, width and amplitude features of an ECG signal. To reduce/eliminate various types of noises in ECG signal, bandpass filter, having low thresholds and high detection sensitivity, was used. This algorithm effectively, using standard 24 h MIT/BIH arrhythmia database, resulted in 99.3 percent correct detection rate of the QRS complexes inspite of several diverse signal features. The system lacks to detect 0.675 percent of the beats.

Benitez et al. [**5**] proposed robust QRS detection algorithm builtusing the properties of Hilbert transformation. In this method, first derivative of ECG signal and then Hilbert transformation calculated over it locates the R peak of ECG wave. T and P at peak represent high accuracy, as the unwanted effects related to baseline drift motion and muscular noise were minimized. The system's beat by beat evaluation was tested according to ANSI standards for ECG analysis.

Arzeno et al.[**3**] discussed that algorithms (Hamilton-Tompkins and Hilbert transform QRS methods) were computationally efficient for real-time assessment of big datasets supporting high accuracy, reduced intervention and noise but these had largest time error, sometimes attenuated or wide beats due to low signal slope. So to eliminate these drawbacks the authors proposed a mixture of Hilbert transform and squaring function based algorithms to point out irregularities in the signal and then further analyze them. This combination was suggested because Hilbert transform method gives high accuracy and the second derivative of the signal gave uniform magnitude spectrum.

Nakano et al. [**17**] developed a new system for Instantaneous Heart Rate detection using noisy ECG signals. Interval of R-waves extracted using threshold was required for calculating IHR from the ECG. To avoid incorrect detection due to noises,the authors suggested short-time autocorrelation technique comprising three elements: a QSW filter, short-time autocorrelation, and window-length controller. To detect IHR, short-time autocorrelation was calculated over the output signal of QSW filter. Noise tolerance test and accuracy test of IHR was performed over the noise database and the public ECG database. IHR method was based on similarity matching of the wave of the QRS complex so; there would be no threshold calculation.

Kim et al.[**13**] in 2014 presented a hybrid ECG System-on-Chip, that was built adaptive to analog front-end (AFE) and Digital signal processing (DSP) back end. AFE provisions concurrent

3-channel ECG monitoring supporting band-power extraction and impedance measurement. DSP was configured as a 4-way SIMD processor supporting functions like arrhythmia classification and Heart rate variability (HRV) analysis, accurate R peak detection algorithm and motion artifact and was basically configured to support wide range of application. The SoC had inbuilt Bluetooth protocol for communication in a wireless monitoring system. Due to support of SoC to local processing and adaptive sampling, it helped in accurate peak detection and removal of motion artefact which resulted in reduction of power consumption by 20

2.5 Key Authentication and Management Schemes for WSNs

Blom et al.[**7**] proposed a key management solution to symmetric key generation systems (SKGS) in 1985. He explained it by taking an example of network with n users such that each one must have an access to n-1 keys until n is small number. If n becomes a large number it really creates a chaotic situation to store all keys safely. To resolve this issue, suggested a natural solution that each user must be provided a relatively small quantity of secret data using which all keys can be derived. This scheme was well applied to SKGS and results showed the effectiveness of simple and practical implementation. However, as all keys were generated from a single entity i.e. secret data, so dependencies between keys will exist. The main drawback of this scheme was that if some intruder got access to few keys then he might derive the dependency relation between keys.

Du et al. [**8**] proposed an extended pre-distribution key scheme by improving the Blom's key scheme [Blom 1985]. They combined the Blom key method with the random key generation pre-distribution methods. The main motive behind this pre-key distribution scheme was to attain superior resistance against node capture. Suppose all sensor nodes can be placed at vertex position in a graph and edge can only be formed between nodes if they share a secret key so that it may result in complete graph (i.e. all node pairs are connected through edge). Though full connectivity is advantageous, but it is not mandatory in Blom's scheme as connected graph is desirable. The benefit of introducing this connected graph concept is to lessen the quantity of information saved by each sensor node. That scalable and flexible 64-bit secret keys network allows up to N =264 sensor nodes and there was no compulsion of deploying all these sensor nodes at the same time, those nodes can join and leave the network at any time and can form secret keys connection with existing sensor nodes. As all keys are generated pairwise so those can be authenticated directly.

Zhou et al. [**27**] heightened his work in the field of key management based on modified Blom's

symmetric key structure method by performing a number of studies over this. Firstly, an efficient monitoring procedure of compromised nodes was carried out with the help of legitimate neighbour nodes to perform distributed revocation. private shadow matrix concept was presented to mask the key information of legitimate and other innocent nodes and prevent them from revelation. Finally, this scheme was an enhancement over the existing techniques in terms of key management, network security, storage and communication overhead.

Vincent et al. [**28**] discussed about various kinds of attacks occurring due to mobility in network i.e. patients wearing body sensors move freely in environment and executing regular exercises such as jogging and swimming etc. This node mobility moves towards recurrently changing network topology, degrading the link quality, making it simple for intruders to launch various cyber-attacks likedata injection attack and mobile compromise attack. The authors also addressed a number of other unaddressed security and privacy challenges such as privacy attacks and data attacks which should be carefully addressed before it is implemented. Firstly, in most of the cases the PHI names are semantically relevant to its which is not good for its confidentiality and privacy. An efficient alternative introduced was to perform private keyword search over encrypted PHI content.

Xiaodong et al. [**30**] introduced a two phase patient self-controllable multi-level privacy-preserving cooperative authentication scheme which consists of: an attribute based designated verifier signature(ADVS) scheme that provided three level security in five step algorithm: Key Extraction , Verification, Setup, Signature and Transcript Simulation Generation and the corresponding authorized accessible privacy model (AAPM) adversary model. An access tree was set up defining the access rights supporting threshold attributes for persons based on their belonging category. PSMPA scheme especially proved its success over previous schemes for boosting the energy constrained mobile sensor node's proficiency.

Jun et al.[**29**] considerably worked upon the adversary model (AAPM) of the existing work to solve the problem of security when patients traverse among blocks outdoors and perform their regular exercises. A privacy-preserving key management method was developed against time-based and location-based mobile attacks by protecting patient's identity, sensor deployment location etc. It exploited the blinding technique and Blom's symmetric key mechanism for secret sharing. The simulation results proved the efficiency and resistivity against attacks. A mechanism to get rid of patients' selfishness to obtain resistance against mobile compromise attacks was the future requirement of this research.

Chapter 3

PROBLEM FORMULATION

3.1 Problem Formulation

Now a days, the internet of things are being popular in the variety of applications among the world, which is being utilized among the house security, weather, traffic, pollution, etc applications utilized by the various organizations. The security of the IoT data becomes very important in the case of the security critical applications, which includes the home security and military applications upon priority. The existing model is based upon the implementation of the multiple use entity factors using the XOR based encryption algorithm, which is primarily utilized to merge two similar vector built of similar length and byte size. In the existing scheme, the model has been build upon the basis of certificate less cryptography (CBC), which is known as the identity based cryptography (IBC), which creates the combined scheme (CBC-IBC). The existing model utilizes the elliptic curve cryptography which is based upon the XOR encryption, which is associated with the encryption standard performed with the similar length of two vectors, which includes one data vector and another secret key vector. In the existing model, the multiple attributes are the secured using the similar cryptography, which includes the robust security model in the existing model. The exposure to the information is based upon the cryptanalysis attacks in the existing model, which happens due to the lack of authentication layer to protect the user integrity. In this model, the following are the primary shortcomings, which made the security less trustable in the case of existing model:
1. The existing model is based upon the elliptic curve cryptography, which lacks in the security feature of the proposed model to protect against several cryptanalysis attacks overt the cryptographic hashes.
2. Multiple attribute based encryption combine the multiple arguments together, and encrypt them in group, which makes it vulnerable to the several information masquerading attacks.
3. The information lacks the authentication security, which protects the IOT model against the node hijacking attacks in the direct form, which helps to create the robust networks.

3.1.1 Problem Algorithm

The proposed calculation for client information privacy in internet of things (IoT) framework will be a mix of information pressure, encryption and authentication plans. The new half breed client privacy model will guarantee the security level solidifying for the protected information moves in the IoT frameworks. The secrecy of the client sending the information will be accomplished by utilizing the safe key trade between the medicinal services sensors and therapeutic database. The safe key trade model will be refreshed in the proposed show than the current client privacy arrangement in the base paper. The key table for proposed plan will utilize randomized numerical key era capacities. The key table sharing will be performed in the neighbor building condition of the security show. To go up against the information respectability, the encryption calculation will be utilized. The encryption model will guarantee the privacy of the client information by making the information indiscernible amid information transmissions between the medicinal databases and social insurance sensors. Likewise information encryption and pressure plans would be connected to the medicinal services information security component to ensure the client information privacy. The client information privacy will be increment to a level higher by utilizing the information encryption utilizing AES encryption calculation, which will secure the client information privacy more successfully than the typical information transmission. The information pressure will be added to the security component to decrease the information measure which will be expanded utilizing the encryption system. The information measure diminishment utilizing the pressure instrument will encourage the IoT framework to send the information as quick as the plain content information.

3.1.2 Objective

A. To study the security protocols for the security model for internet of things (IoT) networks.
B. To design the proposed model to overcome the shortcomings associated with proposed model
C. To implement the proposed model using the MATLAB simulator with essential input and output parameters
D. To obtain and evaluate the proposed model results from the simulation model.

3.1.3 Facilities Required for Proposed Work

Hardware Requirements

- SYSTEM: Dual Core, 1.70 GHz CPU or above
- HARD DISK: 80 GB

- MONITOR: colour, Any size
- RAM: 2 GB

Software Requirements

- Operating system: Windows 7/8 or Above
- Application: MATLAB v2013a or above
- Coding Language: MATLAB Programming

Chapter 4

EXPERIMENTAL DESIGN

4.1 Overview

The internet of things (IOT) is the network consisted of the small sensor nodes, which is used to obtain the data of specific environment. The IOT networks are considered as the distributed networks, and used to collect the data from the various points in the given environment, which is further aggregated over the aggregation node, which is considered to be the base transceiver station (BTS), sink node, etc. The aggregated data is processed over the centralized processing unit assigned for the purpose, and equipped with the service related application for the analysis of the incoming data. The security of the IOT networks becomes very important for the purpose of privacy and integrity protection, which is considered to be the most important part for the IoT data propagation. The combination of authentication and encryption has been utilized to construct the security solution for the security of IOT network.

4.2 Simulation Environment

The existing model belongs to the certificate les paradigm of the authentication mechanisms, and known as certificate less cryptography (CLC) along with the identity based cryptography (IBC) for the security of the IOT over the authentication layer. The authentication and key aggregation (AKA) based method is being proposed with the robust encryption mechanism of advanced encryption standard (AES) for the implementation of the security of the given IOT network. In this thesis, we have worked upon the generation of the complex keys for the purpose of highly secure authentication protocol, which works on the basis of paired key mechanism (PKM), which utilizes the different keys for the purpose of authentication in the IOT environments. The paired key mechanisms are considered highly secure, as they provide the higher level of security against the guessing attacks, whereas stays weaker against the masquerading, eavesdropping or sniffing

attacks. The paired key mechanisms are made stronger with the incorporation of the encryption method to protect the authentication data against the prior defined attacks. The advanced encryption standard (AES) has been utilized for the purpose of encryption, which is considered to be one of the most secure encryption model and works upon the Rijndael method. The AES encryption has been developed to work upon 128-bit blocks and 128-bit secure key for hiding of the data. It's a symmetric mechanism, which uses the similar keys for encryption and decryption, which are pre-shared among the data sharing resources, and stored manually in the specific applications.

4.3 Simulation Scenario

The simulation scenario is based upon the Internet of Things (IoT) network and its security. The security of the IoT is ensured with the new scheme built over the combination of encryption and authentication algorithms. The proposed model is supposed to increase the level of security of the given IOT network against the information hijacking attempts.

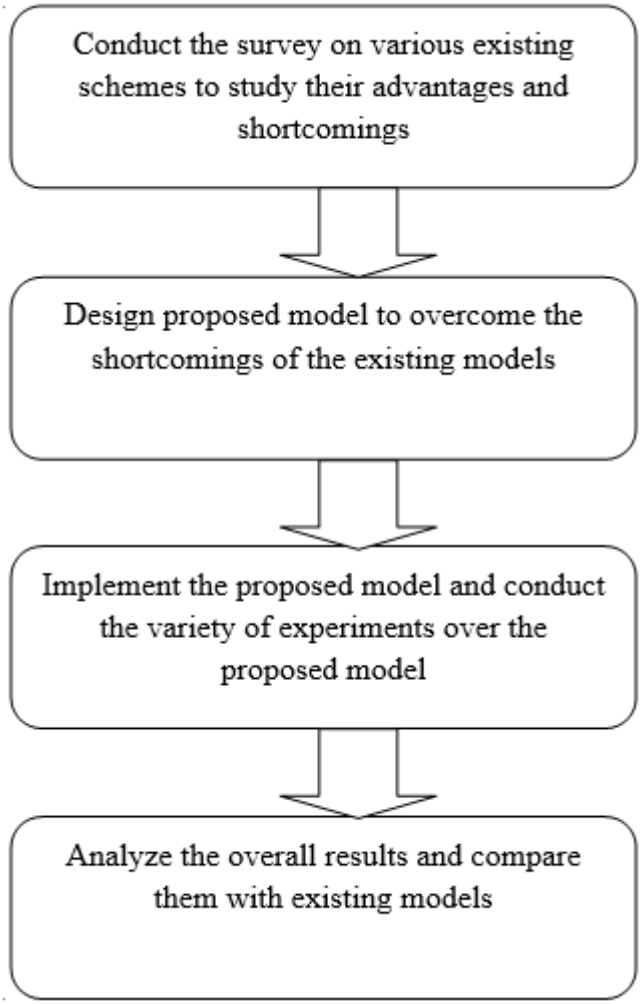

Figure 4.1: Proposed model Design

The proposed model work consists of four major stages as per elaborated in the figure 4.1. The proposed model is based upon the IoT security and began with the study of literature on the various security models on Internet of Things (ioT) networks. The proposed model has been further designed to overcome the shortcomings of the existing models, which is implemented using the MATLAB simulator with dynamic topology, which offers the peer-to-peer relationship. After the experiments are conducted and the results are obtained from the variety of topologies, which helps us to study the proposed model various aspects under the different number of nodes. Finally, the results are compared and analyzed against the existing models to final improvement.

4.4 System Design

The multi-column table based authentication data has been created under the proposed model for the purpose of authentication. Instead of certificate less cryptographic, the advanced encryption standard (AES) has been utilized for the data and authentication key security, which is considered to be more robust and secure than XOR encryption. The authentication model is based upon the complex key generation, which is accomplished using the set of algebraic functions in our scenario. The key chain is created in the communication with the pairs of authentication keys, termed as query key and reply key. The existing encryption scheme is similar to the elliptic curve cryptography (ECC), and carries many disadvantages in common with the ECC scheme, which makes it vulnerable to various attacks over cryptography. The vulnerabilities can be resolved by using the robust and cyclic cipher with higher order of complexity than the existing model, which has been achieved with the use of AES. The authentication procedure is designed over the paired-key mechanism, which combines the multiple columns to create the query and answer keys. For the construction of query key, total 4 coefficients are used out of total 8, which are combined by using the cubic function, whereas for the answer key, total 5 coefficients are used with the quartic function. The following table elaborates the column structure in the given authentication table:

From this table, the first four columns, denoted with symbols (A, B, C and D respectively) are used to construct the query key. Last five columns ranging from 4 to 8 are used for construction of the answer key, which consists of the variables A, B, C, D and E respectively.

Table 4.1: Formation of the Key Table

Columns in Authentication Key Table	Coefficient or Variable Name
1	A
2	B
3	C
4	D,A
5	B
6	C
7	D,A
8	E

4.5 Implementation Details

4.5.1 Cubic Equation

In the algebra, a cubic function is the function to process the input coefficients up to 3rd order

$$f(x) = ax^3 + bx^3 + cx + d \tag{4.1}$$

Where the coefficients are non-zero, or at least one of the coefficients is non-zero.

$$ax^3 + bx^2 + cx + d = 0 \tag{4.2}$$

The initialization can be performed with f(x) = 0, which generally initializes the cubic equation function to process the input coefficients in the next step to return the constructed authentication key. The polynomial theory is utilized in the construction of the cubic function, which is given by the solution known as roots of polynomial up to the Nth order. The four input coefficients denoted with symbols, a, b, c and d are utilized to handle the value provided to the input function. The cubic function utilizes the odd value (3) as the maximum Nth order for the calculation of the equation to produce the final value. The numerical approximation of the input coefficients is performed using the root-discovery mechanism called the Newton's mechanism. The input is accepted in the form of decimals, integers or real numbers, but the complex numbers are not entertained under the cubic equation. The input coefficients with value higher than 0 are acceptable for the purpose of equation processing under the cubic equation based mathematical function. Likely, the solution is produced in the similar form to that of the input coefficients, which may be integer, float, decimal or real number, which depends upon the form or class of the input numbers. The function starts

to compute the values from the base points, conceded zero as the minimum value. There is no capping for the highest value, which can be computed up to any number, which possibly belongs to the one of the input forms. The x in the equation must be a non-zero value in our case, which is computed over the authentication table in the equation 4.1. The following equation describes the cubic function in our case:

$$3ax^3 + 2bx^2 + cx + d \neq 0 \tag{4.3}$$

The solution of the cubic function is computed using the algebraic formula as per given in the following equation:

$$x_{critical} = \frac{-b \pm \sqrt{b^2 - 3ac}}{3a} \tag{4.4}$$

4.5.2 Cubic Equation Implementation

The coefficients are obtained from the authentication key table, which is generated over the first four columns. The selection of rows depends upon the random number generation (RNG) algorithm. The RNG model uses the range between 1 and N, where N is the size of key table rows. The following equation is used to produce the random row id to select the values from the key table:

$$\sigma = x_1...x_n, \sigma x_1...\sigma x_n \tag{4.5}$$

$$P(n,k) = \frac{n.(n-1).(n-2).(n-3).(n-4)...(n-k+1)}{kfactor} \tag{4.6}$$

Where σ is the matrix of possible values, and σx_n denotes the factored values in the matrix for permutation, k factors define the number of possibilities, n denotes the maximum values, k denotes the number of combinations, and P(n,k) gives the permutation result. Hence the row on the permutation value of P(n,k) is obtained from the 4.5, which is further used as the coefficients. The value of row id is assigned to the variable rowed as per the following equation:

$$rowId = P(n,k) \tag{4.7}$$

After the coefficients are selected from the corresponding row in the key table (KT), which is given by the following set of equations:

$$A = K_T(rowId, 1) \tag{4.8}$$

$$B = K_T(rowId, 2) \tag{4.9}$$

$$C = K_T(rowId, 3) \tag{4.10}$$

$$D = K_T(rowId, 4) \tag{4.11}$$

The A, B, C and D coefficients are obtained in the equations between 7 and 10 respectively, which is obtained with respect to random number stored in the rowId. Then the value of x is generated from the first column of the key table as per give in the following equations:

$$x = round(mean(K_T(1 : N, 1)) \tag{4.12}$$

The variable x contains the constant value, which remains similar in all of the cubic function operations, KT denotes the key table, N denotes the number of rows in the key table. Afterwards the mean and round functions are applied in the hierarchical manner in order to create the constant. Then the cubic equation is applied over the given coefficients as per defined in the following equation:

$$Qkey = Ax^3 + Bx^2 + Cx + D \tag{4.13}$$

The Qkey generated in the equation 12 is further sent towards another node, which applies the quartic function to generate the answer key from the last 5 columns, as per explained in the section 4.4.4.

4.5.3 Quartic Equation

In the algebra, a quartic function is the function to process the input coefficients up to 4th order

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e \tag{4.14}$$

Where the coefficients must be nonzero, and the coefficients are acceptable in the various number forms such as real number, integer, float, integer, etc. The polynomial order of 4 is used for the computation of the quartic equation. The major purpose of this equation is to focus on producing the non-zero result as the answer of the equation. The following equation defines the form of the given equation:

$$f(x) = ax^4 + cx^2 + e \tag{4.15}$$

The fourth degree of equation ranges the number of input coefficients to 5 coefficients, which undergoes the various sub-expressions in the quartic equation. The following equation draws the flank for the computation of the key components:

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \tag{4.16}$$

Where value of a or other coefficients must be non-zero. Hence the most acceptable condition would be the one, where all coefficients and variables in the equation are non-zero and defined by a $\neq 0$, b $\neq 0$, c $\neq 0$, d $\neq 0$ and e $\neq 0$.

4.5.4 Quartic Equation Implementation

For the quartic equation, similarity the coefficients are obtained from the authentication key table, which is generated over the last five columns. The quartic function is used on the client node in the authentication link, where the sender acts the server, which produces and provides the query key to the receiver node. The receiver key runs the iteration over the key table for each row in the table, and produces the key using the cubic equation, as per given in the 4.1 and 4.13. Once the cubic function results are matched, the quartic function is applied on the last five elements in the current row of key table, which is explained in the further procedure. After the coefficients are selected from the corresponding rows in the key table (K_T), which is given by the following set of equations:

$$A = K_T(rowId, 4) \tag{4.17}$$

$$B = K_T(rowId, 5) \tag{4.18}$$

$$C = K_T(rowId, 6) \tag{4.19}$$

$$D = K_T(rowId, 7) \tag{4.20}$$

$$E = K_T(rowId, 8) \tag{4.21}$$

The A, B, C, D and E coefficients are obtained in the equations between 16 and 20 respectively, which are obtained with respect to matching row as per defined in the first paragraph of this section. Then the value of y is generated from the first column of the key table as per give in the following equations:

$$y = round(mean(K_T(1 : Nr, Nc)) \tag{4.22}$$

The variable y contains the constant value for quartic equation, which remains similar in all of the quartic function operations, KT denotes the key table, Nr denotes the number of rows in the

key table and Nc denotes the number of columns in the key table, hence the last column in selected in the above 4.22. Afterwards the mean and round functions are applied in the hierarchical manner in order to create the constant. Then the quartic equation is applied over the given coefficients as per defined in the following equation:

$$Akey = Ay^4 + By^3 + Cy^2 + Dy + E \tag{4.23}$$

The answer key (Akey) generated in the 4.23 is further sent towards node on other end, which verifies the answer key and produces the final result.

4.5.5 Advances Encryption Standard (AES)

The advanced encryption standard (AES) has been used to secure the data as well as the authentication keys (Also termed as authentication data). The AES algorithm is based upon the symmetric encryption models and incorporates the multi-round data hidings models in the blocks, which makes is a cyclic block cipher (CBC). The AES scheme is consisted of the various steps altogether for the efficient hiding of the data. The AES algorithm is designed in versatile manner and with many variants, which accepts the different number of encryption rounds and different key lengths.

Phase 1: SBOX Preparation

The s-box plays the vital role in the AES encryption model, which is associated with the sub-bytes and byte-shuffling in the case of mix columns or shift rows steps. The rows and columns are exchanged to create a data mess, which is known as the cipher, and remains the form of scrambled data. The complex scrambling of data with dynamic s-box generation according to the input secure key makes the encryption procedure more complex, and helps to create the secure data to prevent the external information stealing attacks. The following figure shows the example of s-box, and shows the data of a small chunk of the complete s-box matrix.

Phase 2: Encryption Rounds

The number of encryption rounds plays the vital role in the case of advanced encryption standard (AES). The AES algorithm is based upon the symmetric encryption algorithm and incorporates the multiple rounds to hide the information, which makes it stronger and non-attackable ciphering mechanism. The AES model working is depicted in the following figure (Figure 4.3), which shows the input data block and encryption key, which results in the form of cipher text. In this thesis,

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 4.2: Example of S-Box for AES

the 128-bit block cipher has been utilized for the AES algorithm, which is capable of processing 128-bit data in one cycle or round, which accounts for 16 bytes of information. The proposed model utilizes the 128-bit long encryption key (Security key), which is used to hide the data more securely and create a robust block cipher. In this model, the 9-round scheme has been incorporated for the encryption, which includes one additional round. Hence, total 10 rounds of encryption are performed over the data in each encryption cycle.

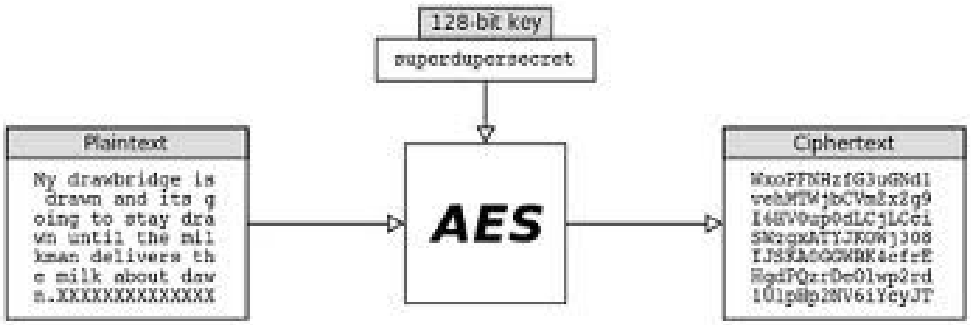

Figure 4.3: The AES algorithm is action for the text encryption

Phase 3: Encryption Key and Key Expression

The 128-bit encryption key has been utilized in the proposed model, which creates a stronger ciphering mechanism under the AES model. The 128-bit encryption key is further expanded to the smaller keys of number equals to the number of rounds. In each round, a different key out of

the expanded key matrix are used to hide the information, which create the robust information security paradigm and hides the data very efficiently. Generally, the symmetric encryption models use the similar key to encrypt and decrypt the data, along with the exactly reversible procedure to reveal the original data from the data hash, which makes it highly secure and less vulnerable to the cryptanalysis attacks. The proposed model is based upon the 10 rounds, which includes 9 data round and 1 final round. Hence, there is a need to 10 sub-keys, which are generated during the key expansion procedure.

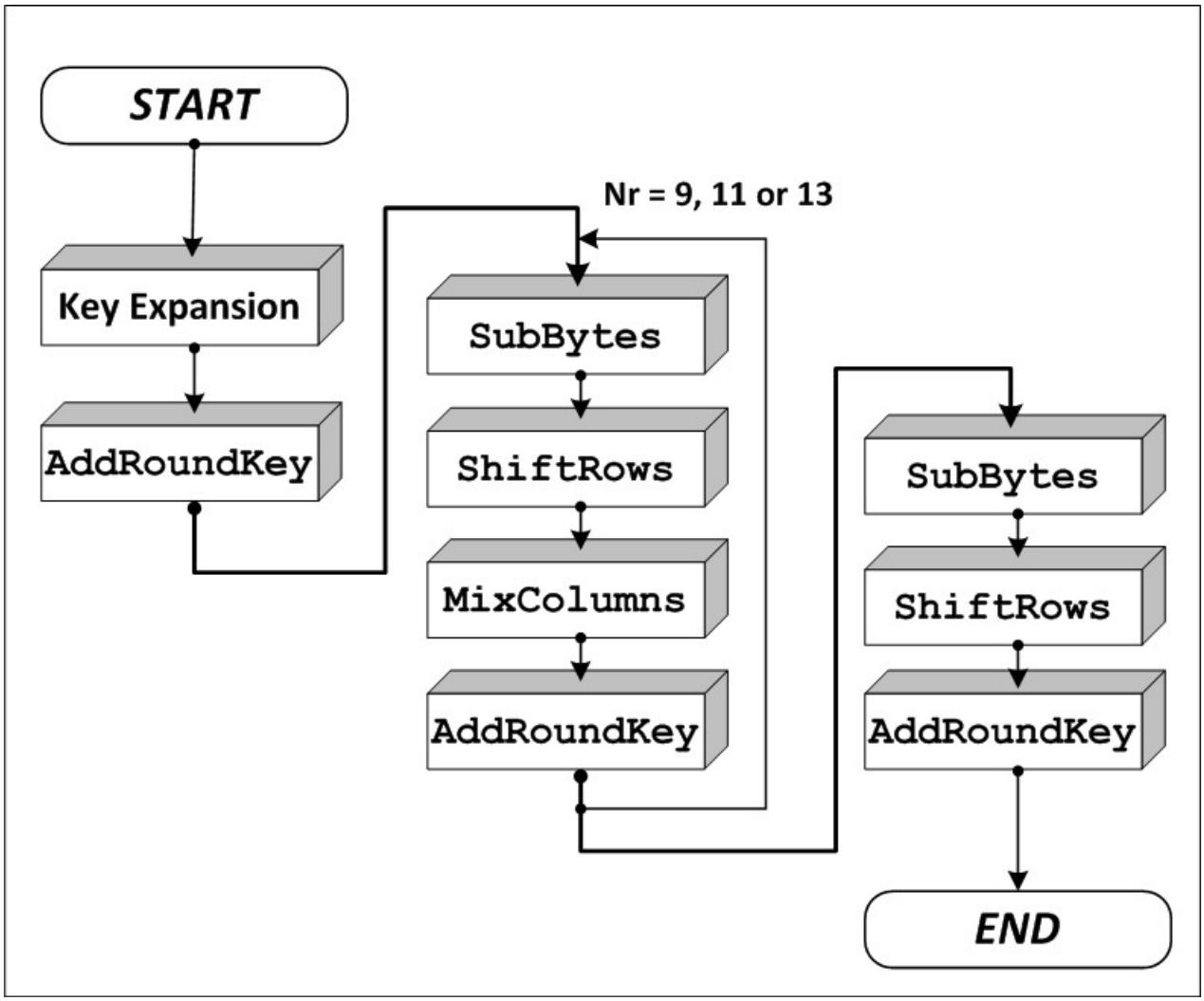

Figure 4.4: The architecture of AES algorithm

The following section defines the stepwise working of the proposed model, which includes the several steps altogether to hide the data securely using the symmetric encryption mechanism as per the algorithmic design.

Algorithm 1: Advanced Encryption Standard Algorithm

1. Acquire the data matrix, denoted (d)

2. Validate the size of data matrix according to the algorithmic requirement, $d_M \leftarrow$ validateInputMatrix(d)

3. Segment the input data matrix according to the algorithmic requirement, $dM^i \leftarrow$ segmentInputMatrix (d_M)

4. Acquire the security key from the user input, denoted (S_k)

5. Expand the key according to the number of rounds, $S_k^i \leftarrow$ expandKeys(S_k)

6. Start the iteration over each block or segment of the input data matrix

7. Add the round key in the initial step, AddSecureRoundKey(S_k^i)

8. Iterate the cyclic block cipher procedure 9 times on the input block after step 7

   a. Apply the sub bytes functions to replace the sub bytes, SubBytes(d_m^i)

   b. Apply the shift rows functions to create the scrambled matrix on rows, ShiftRows(d_m^i)

   c. Apply the mix columns, functions to create the scrambled matrix on rows, MixColumns(d_m^i)

   d. Add the round key to the scrambled matrix, AddSecureRoundKey(S_k^i)

9. Run the final round of encryption

   a. Apply the sub bytes functions to replace the sub bytes, SubBytes(d_m^i)

   b. Apply the shift rows functions to create the scrambled matrix on rows, ShiftRows(d_m^i)

   c. Add the round key to the scrambled matrix, AddSecureRoundKey(S_k^i)

10. Combine the encrypted data segments to recreate the encrypted matrix, $dE_M \leftarrow$ combine Segments(d_m^i)

11. Remove the validation data, which was added in columns or rows of zeros, dE $\leftarrow$ remove Validation Data(dE_M)

12. Return the encrypted data matrix

Moreover, the decryption of the AES algorithm is more complicated and consumes more time than the encryption. So after reading some books, papers and websites, two feasible solutions are found: decomposing the changes of columns to reduce the numbers of times and constructing some forms. Based on decreasing of the storage space, these two decryption optimal algorithms process on the basis of the columns changing that makes the programming smaller than the original one and saves much more time.

4.5.6 Main Algorithm

The main authentication algorithm is based upon the server and client (sender and receiver respectively) for the realization of the proposed security algorithm over the given scenario. The following algorithm describes all of the steps of the proposed model in detail, which describes the complete operations in the structured model design

Algorithm 2: Proposed Paired Key Management (PKM) Model

MAIN ALGORITHM DESIGN:

1. Start the cluster nodes
2. Input the communication radius, energy consumption constant values to transmit and receive values, number of nodes and area parameters
3. Obtain value of N, N ← number of nodes
4. Initialize the sparse matrix with N x N size
5. Run the localization over communication radius
    a. Iterate for all of the nodes in the cluster, I
        i. Iterate for all of the nodes in the cluster, J
            1. Compute the distance between the current two nodes, node I and note J
            2. Distance = $\sqrt{((x1 - x2)^2) + ((y1 - y2)^2)}$
            3. If the distance is less than communication radius
                a. Plot the link between the two nodes
                b. Update the sparse matrix on the (I,J) index with value 1
            4. Else
                a. Do not plot a link
                b. Update the sparse matrix on the (I,J) index value Inf (infinite)
6. Find the route towards the required destinations
    a. Load the number of source nodes
    b. Load the number of destination nodes
    c. Map all of the connection and build a connection array containing source and destination for each end to end connection, connection array ← All source & destination possibilities
    d. Iterate for each row in the connection array, I
        i. Obtain the source node from current row (I,1), where 1 is the column number
        ii. Obtain the destination node from current node (I,2), where 2 is the column number
        iii. Pass the destination, source node and sparse matrix to the routing algorithm

iv. Obtain the path array containing the list of nodes in the particular sequence ranging from source to destination

v. Construct the path between the source and destination

7. IoT node sense the data as per its sensing module

8. IoT node collects the data and starts the forwarding procedure

a. The next hop node is queried for the availability

b. Next hop node replies with the acknowledgement if available

c. Ask for the pre-shared key (PSK) from the receiver node

d. Receiver node replies with pre-shared key (PSK)

e. If PSK verified

i. Post-authentication procedure beings

f. Otherwise

i. Communication Link Refused

ii. Stop the data transmission

g. Random row selection is applied over the sender node's key table, rowId

h. Sender node generates the row id

i. Required coefficients are selected from the target row in the key table

j. Compute the value of X constant by computing the mean of the first column

k. Apply the cubic equation over the to create the query key

l. Encrypt the query key with AES encryption

m. Forward the query key to the receiver node (next hop node)

9. Next hop node following the following procedure to reply with the answer key

a. Next-hop node receives the query key

b. Decrypt the query key with AES encryption

c. Perform the iteration over all of the rows in the key table, I

i. Acquires the current row, I

ii. Acquire the values of first four columns as four coefficients (A, B, C and D) from the current row

iii. Compute the value of X constant by computing the mean of the first column

iv. Apply the cubic function over the coefficient, localKey

v. Match the localKey with the query key

vi. If matches

1. Acquire the coefficients from the columns (5 to 8) in the variables a, b, c, d and e respectively

2. Compute the value of y by applying the mean over the last column of key table
3. Apply the quartic equation over the coefficients and constant y, answerKey
4. Encrypt the answer key with AES encryption
5. Return the answer key to the server node (sender node)

vii. Else

1. Go to 9(b)(i) until its not end of table

10. Decrypt the answer key with AES encryption
11. Server node performs the key matching operation

a. Acquires the row Id previously generated for generation of query key

b. Required coefficients are selected from the target row in the key table (5th to 8th column)

c. Compute the value of Y constant by computing the mean of the last column

d. Apply the quartic equation over the to create the local answer key

e. Match the local answer key with the answer key sent from the receiver node

f. If both keys matches

i. Authentication is successful

ii. Communication starts

g. Otherwise

i. Authentication is failed

ii. Communication ends

12. Begin the data communication between the given nodes
13. Encrypt data over the sender's node
14. Forward the data to next-hop node
15. Decrypt the data over receiver's node
16. Compute the performance parameters
17. Return the simulation

4.5.7 Workflow of Proposed Model

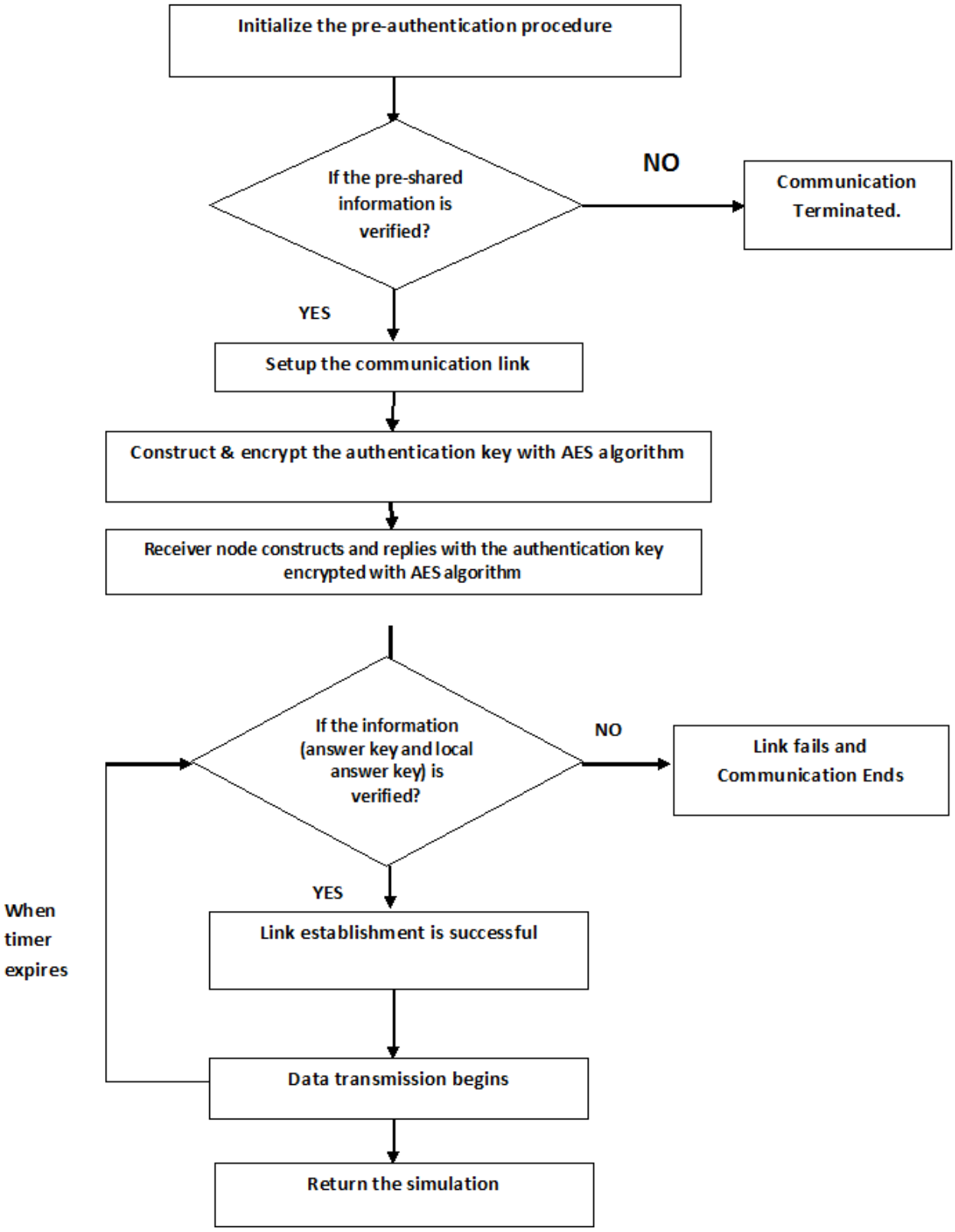

Figure 4.5: Detailed procedure of proposed IoT based authentication model

Chapter 5

EXPERIMENTAL RESULTS

The proposed model has been designed as the highly efficient model of security for the internet of things (IoT) paradigm, and in the distributed manner to enforce the security between the IoT nodes without depending upon the centralized servers. The centralized authentication models are slowed down to the variety of data calls between the IoT nodes and authentication server, which also increases the energy consumption. The proposed model IoT model combines the authentication and encryption model, which eventually decreases the risk of attacks over the IoT networks. The performance is analyzed in the form of projected resources and entropy based analysis. The projected resources describe the use of computational power over the IoT nodes, which are measured to study the need of computation power as well as the energy consumption. The energy consumption can be also studied from the projected resources. The relationship between the projected resources and energy consumption is understood as direct relationship, in which the increase in projected resources is directly proportional to the energy consumption and vice-versa. The value of entropy gives the uniqueness of the keys in the key table. The high uniqueness of the keys describes the higher level of security among the IoT networks.

5.1 Assumptions and Variables Factors

Some of the pre-considerations are conceded in this project, which defines the limitations of the scenario used in the proposed model. The communication channels, delay estimation, idle state of BTS or nodes etc. are discussed in this section. The following point describes the assumptions taken for the proposed model:

• No local or processing delay in considered in this scenario

• No End-to-End delay addition due to the physical media is added to the final results

• Wireless channel allocation is not programmed and it automatically describes the automatic selection of the wireless channels

- Number of nodes is manually adjustable
- Transmission range is manually adjustable
- BTSes or cluster head nodes are not programmed to stay in idle state
- All IoT nodes are considered available in all data rounds
- No duty cycling is accounted in this scenario

5.2 Result Analysis (50 Nodes)

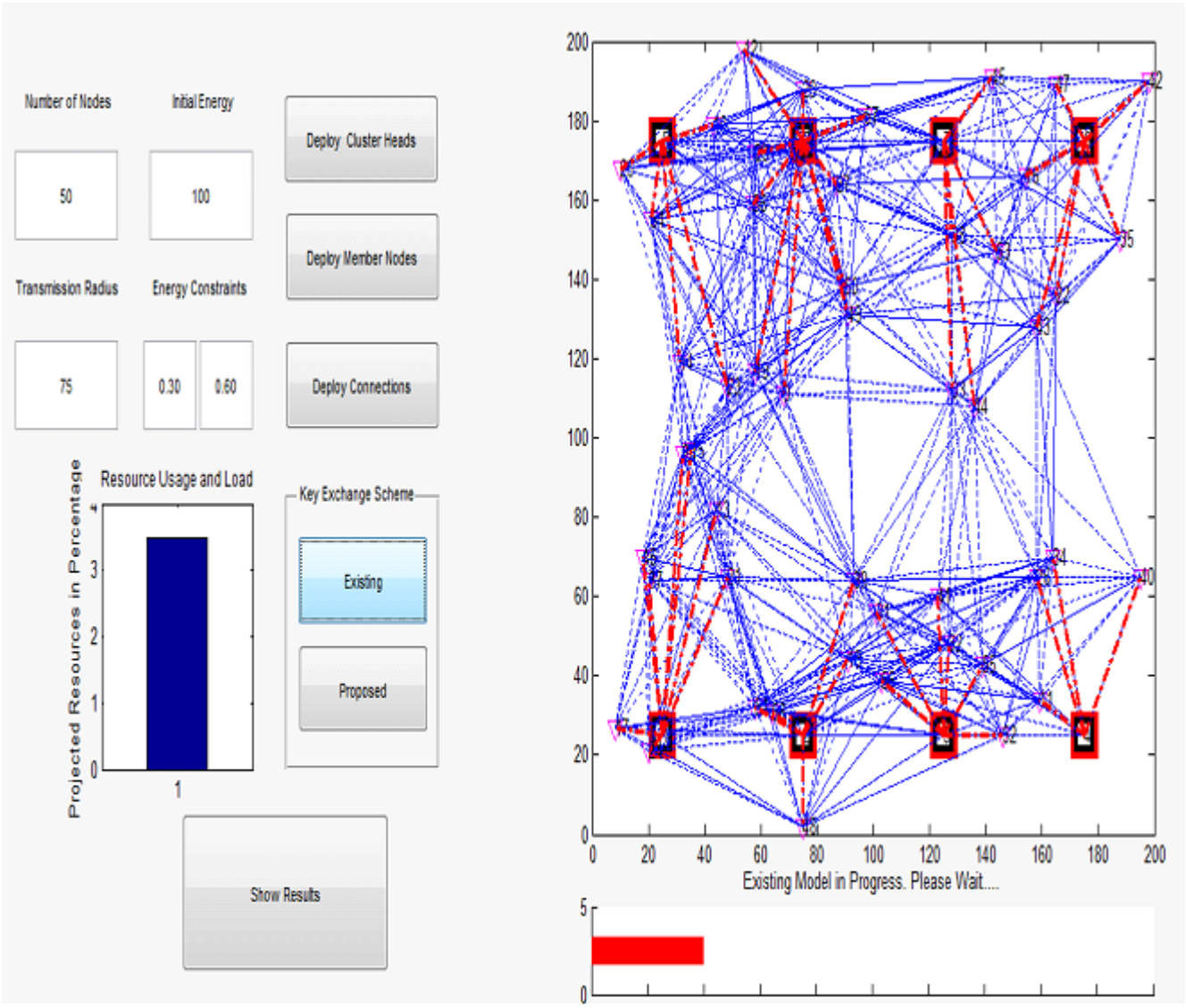

Figure 5.1: Working of IoT model on 50 nodes scenario

The results of the proposed scenario are obtained under the various experiments with different number of nodes, variable transmission range and constant energy transmission and receive values.

In this scenario, 50 nodes are deployed randomly (using permutations) in the area of 200 x 200

Table 5.1: Comparative values obtained from both models for comparison study of projected resources

No. of Iterations	CLC-IBC	CLC-PKM
1	3.72	1.82
2	2.61	1.91
3	1.95	1.11
4	2.92	1.92
5	3.61	1.62
6	1.83	1.09
7	2.93	1.26
8	3.33	1.55
9	2.17	1.95
10	3.17	1.75

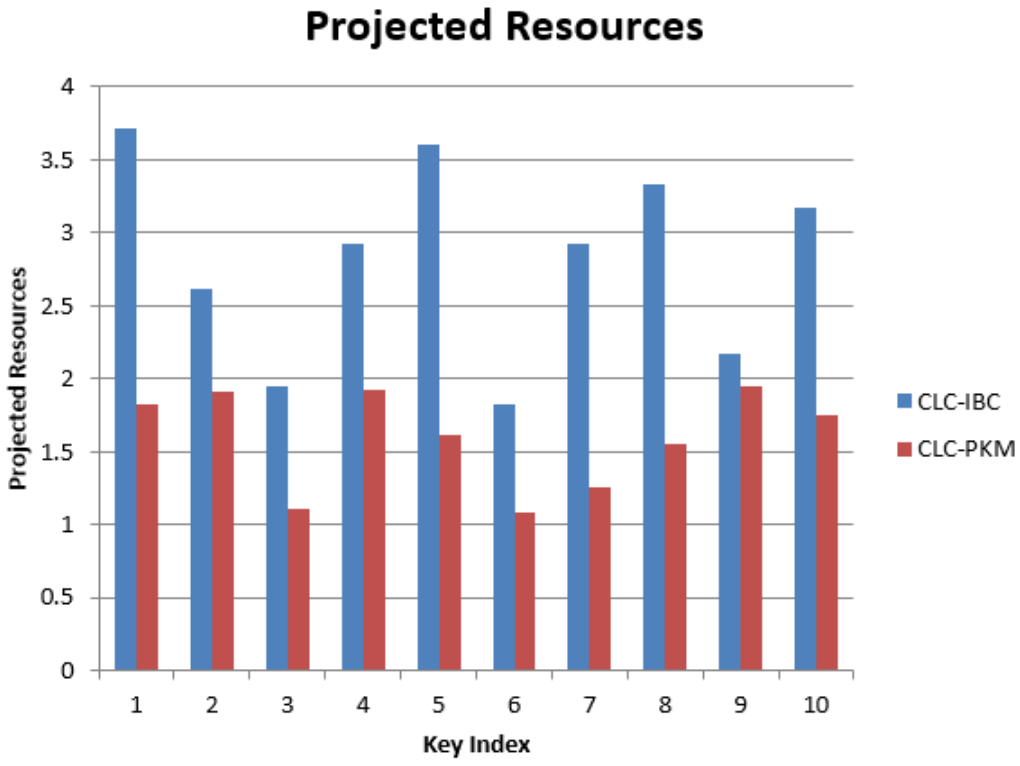

Figure 5.2: Analysis based upon the projected scenario with 50 nodes

square meter of flat ground area. The energy of 0.30 and 0.60 milli-joules is used for the purpose of energy consumption estimation in the given scenario, which is tested for the 10 rounds of data sequence.

The data is transmitted in 10 transmission events and the authentication is applied in all of

Table 5.2: Comparative values obtained from both models for comparison study for entropy

No. of Iterations	CLC-IBC	CLC-PKM
1	1.73	2.72
2	2.15	2.6
3	2.26	2.71
4	1.74	2.13
5	2.045	2.45
6	2.042	2.95
7	2.18	2.98
8	2.02	2.47
9	2.021	2.05
10	1.89	2.17

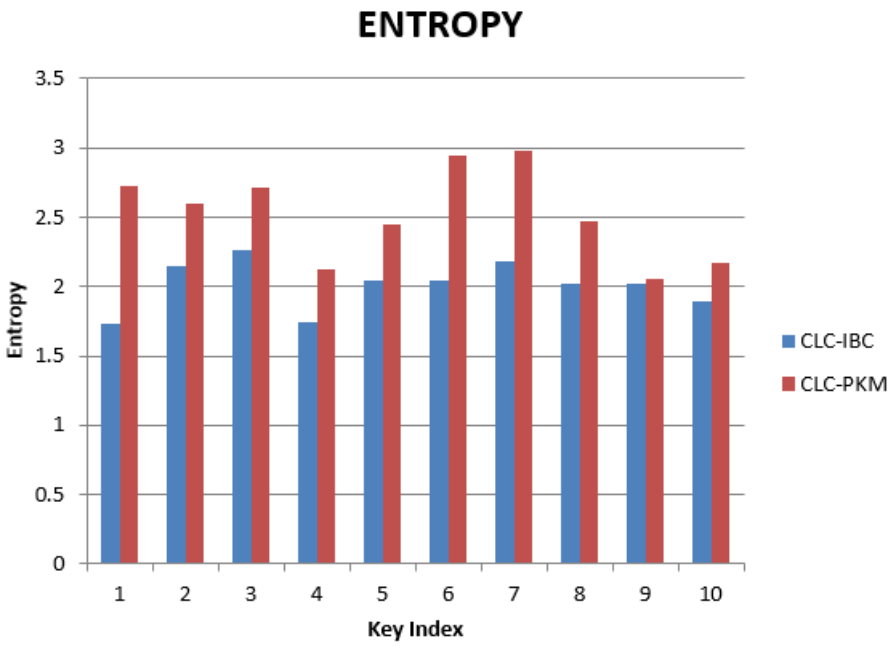

Figure 5.3: Analysis based upon entropy on scenario (IoT) with 50 nodes

the events to describe the effects of authentication on the data events during the authentication rounds. The proposed model has been analyzed for the projected resources over the given scenario of 50 nodes assigned with the transmission range of 75 meters. The proposed model consistently remains lower than the existing model on all of the data events in the following figure (Figure 5.2) for the projected resources. The proposed model has been recorded with the value of projected

resources lesser than 2 percent on all of the authentication events in the proposed model, whereas it seems varying between the 1.8 and 4 percent on all events in the existing model. This phenomenon clearly elaborates he robustness of the proposed model in efficiently handling the authentication model with minimum possible resource usage. The maximum value of entropy remains between the 1.6 and 2.3 for the CLC-IBC model against the CLC-PKS model (proposed model). The proposed model remains between the range of 2 and 3 for the entropy value, which surely gives the higher value than the existing model and justifies the higher order of security of the proposed model.

5.3 Result Analysis (100 Nodes)

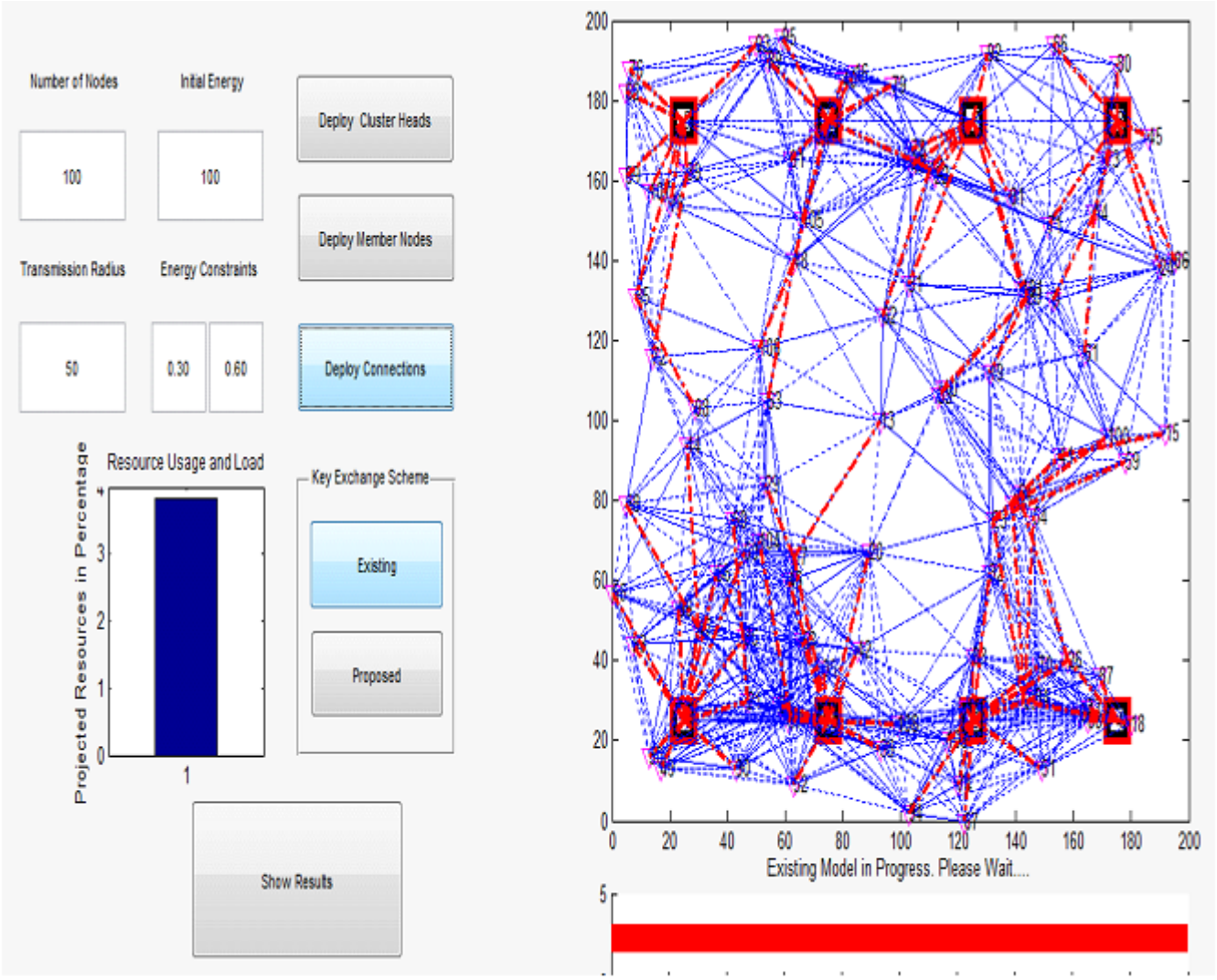

Figure 5.4: Working of IoT model on 100 nodes scenario

Table 5.3: Comparative values obtained from both models for comparison study of projected resources

No. of Iterations	CLC-IBC	CLC-PKM
1	9.42	9.08
2	15.84	9.53
3	10.93	5.64
4	13.32	9.56
5	15.43	8.16
6	7.87	5.49
7	10.58	6.39
8	11.81	7.72
9	19.73	9.81
10	17.25	8.85

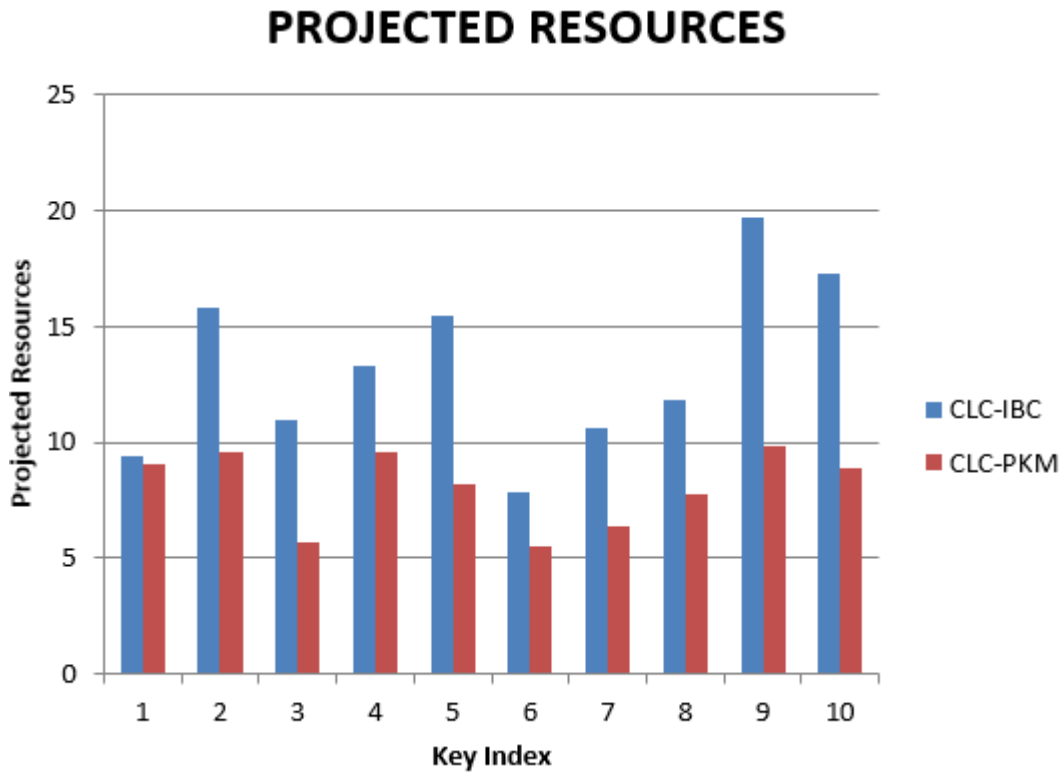

Figure 5.5: Analysis of IoT model on 100 nodes scenario

The results of the proposed scenario are obtained under the various experiments with different number of nodes, variable transmission range and constant energy transmission and receive values. In this scenario, 100 nodes are deployed randomly (using permutations) in the area of 200 x 200 square meter of flat ground area.

The energy of 0.30 and 0.60 milli-joules is used for the purpose of energy consumption estimation

Table 5.4: Comparative values obtained from both models for comparison study of entropy

No. of Iterations	CLC-IBC	CLC-PKM
1	2.02	2.16
2	2.26	3.165
3	1.765	2.64
4	1.61	2.47
5	2.21	2.8
6	2.44	3.39
7	2.17	2.35
8	2.15	3.03
9	2.17	2.92
10	2.53	3.25

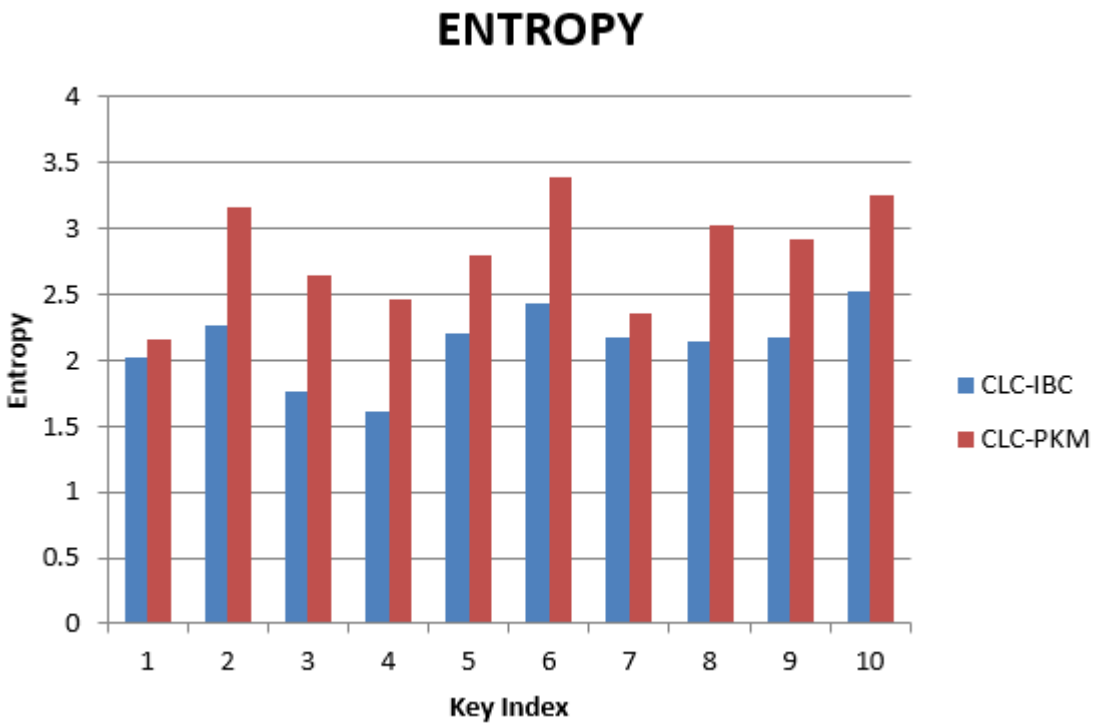

Figure 5.6: Analysis based upon entropy on scenario (IoT) with 100 nodes

in the given scenario, which is tested for the 10 rounds of data sequence. The data is transmitted in 10 transmission events and the authentication is applied in all of the events to describe the effects of authentication on the data events during the authentication rounds. The proposed model has been analyzed for the projected resources over the given scenario of 100 nodes assigned with the

transmission range of 50 meters. The proposed model consistently remains lower than the existing model on all of the data events in the following figure (Figure 5.5) for the projected resources. The projected resources for authentication are recorded between 5 and 10 percent for the proposed model, whereas in the existing model the project resources range lies between 7 and 20 percent. The proposed model consumed half resources in comparison with the existing model on an average in the 10 authentication/data events in the scenario with 100 nodes. The proposed model consumes the higher number of resources than the scenario with 50 nodes, because it needs to host more number of authentication events per node than 50 nodes scenario. The entropy of the proposed model has been recorded higher than 2.1 and below 3.4 on all of the data events in the given scenario. The proposed model has been found consistently higher than the existing model on all of the data events, which is clearly visible from the given scenario (Figure 5.6). The existing model is recorded between 1.6 and 2.5, which is considerably lower than the proposed model on all of the events.

5.4 Result Analysis (150 Nodes)

The results of the proposed scenario are obtained under the various experiments with different number of nodes, variable transmission range and constant energy transmission and receive values. In this scenario, 150 nodes are deployed randomly (using permutations) in the area of 200 x 200 square meter of flat ground area.

The energy of 0.30 and 0.60 milli-joules is used for the purpose of energy consumption estimation in the given scenario, which is tested for the 10 rounds of data sequence. The data is transmitted in 10 transmission events and the authentication is applied in all of the events to describe the effects of authentication on the data events during the authentication rounds. The proposed model has been analyzed for the projected resources over the given scenario of 150 nodes assigned with the transmission range of 25 meters. The proposed model consistently remains lower than the existing model on all of the data events in the following figure (Figure 5.8) for the projected resources. The proposed model scenario is based upon 150 nodes, which are deployed randomly using the pseudo random number generation of the node coordinates. The projected resources for authentication are recorded between 5 and 10 percent for the proposed model, whereas in the existing model the project resources range lies between 7 and 20 percent.

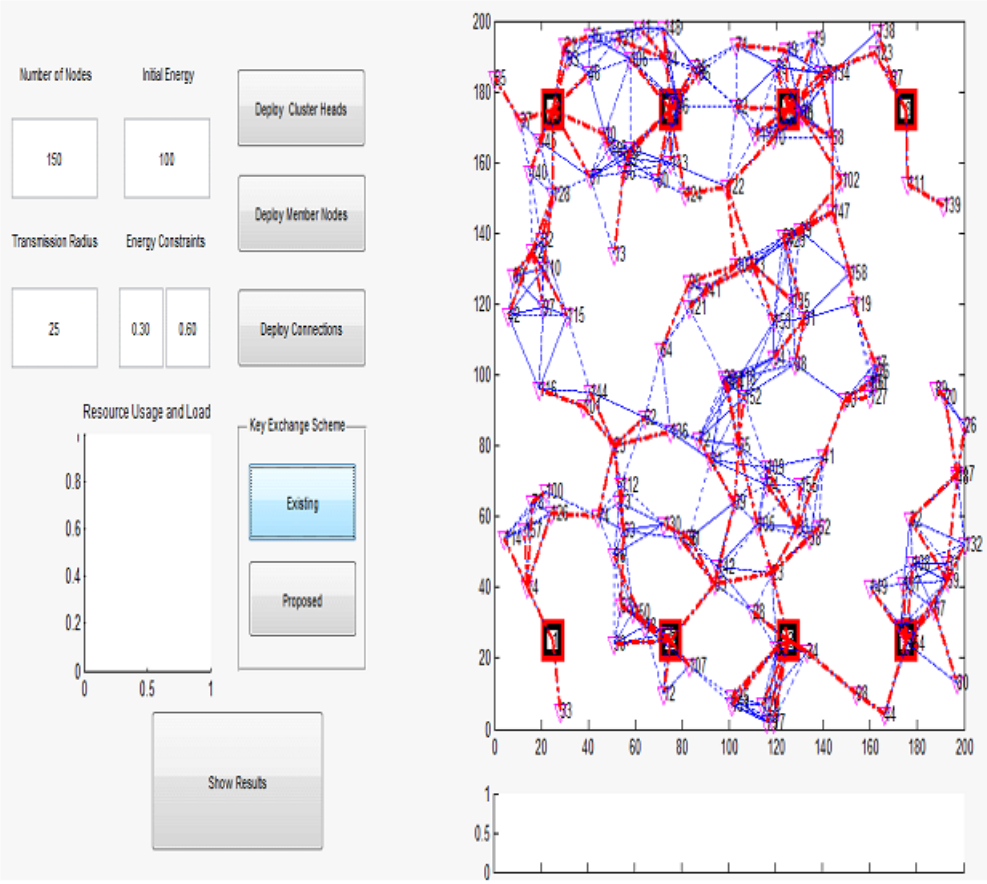

Figure 5.7: Working of IoT model on 150 nodes scenario

The proposed model consumed half resources in comparison with the existing model on an average in the 10 authentication/data events in the scenario with 150 nodes. The proposed model consumes the higher number of resources than the scenarios with 50 and 100 nodes, because it needs to host more number of authentication events per node than 50 and 100 nodes scenarios.

Table 5.5: Comparative values obtained from both models for comparison study of projected resources

No. of Iterations	CLC-IBC	CLC-PKM
1	27.88	18.16
2	38.67	19.15
3	38.45	11.24
4	31.54	19.13
5	28.39	16.33
6	16.94	10.96
7	15.02	12.75
8	26.44	15.44
9	32.59	19.63
10	27.45	16.93

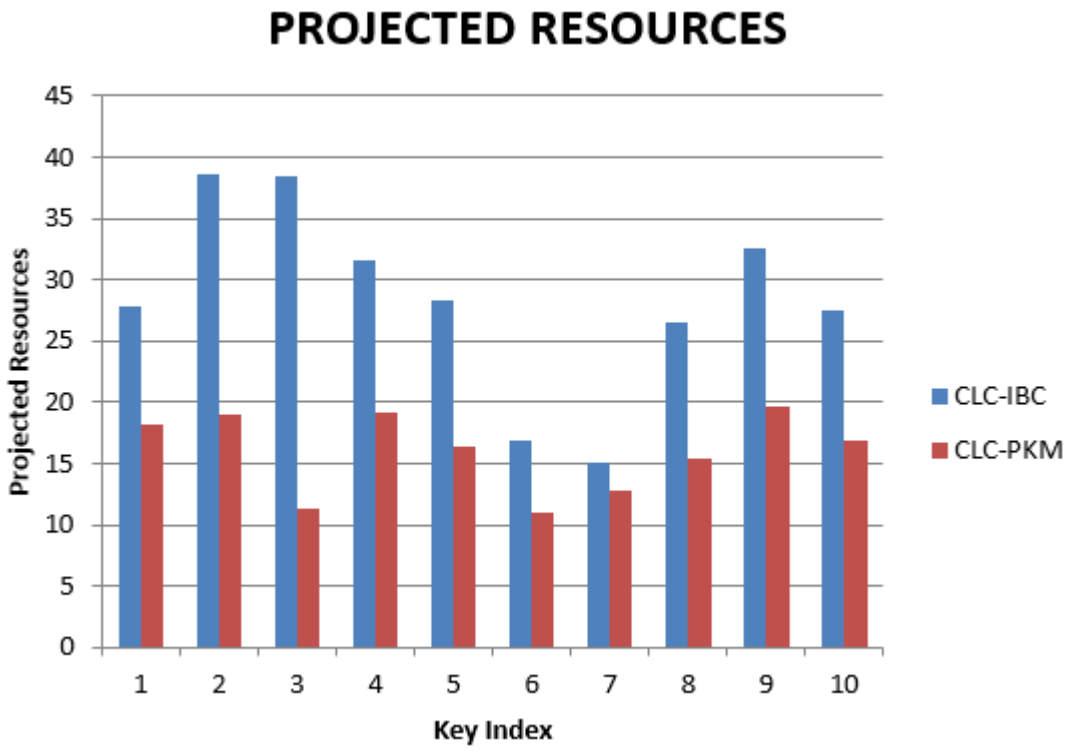

Figure 5.8: Analysis based upon the projected scenario with 150 nodes

Table 5.6: Comparative values obtained from both models for comparison study of entropy

No. of Iterations	CLC-IBC	CLC-PKM
1	1.68	2.01
2	2.33	3.10
3	2.33	2.40
4	2.40	2.83
5	2.08	2.46
6	2.14	3.12
7	2.39	3.30
8	1.85	2.27
9	1.80	2.77
10	2.34	2.85

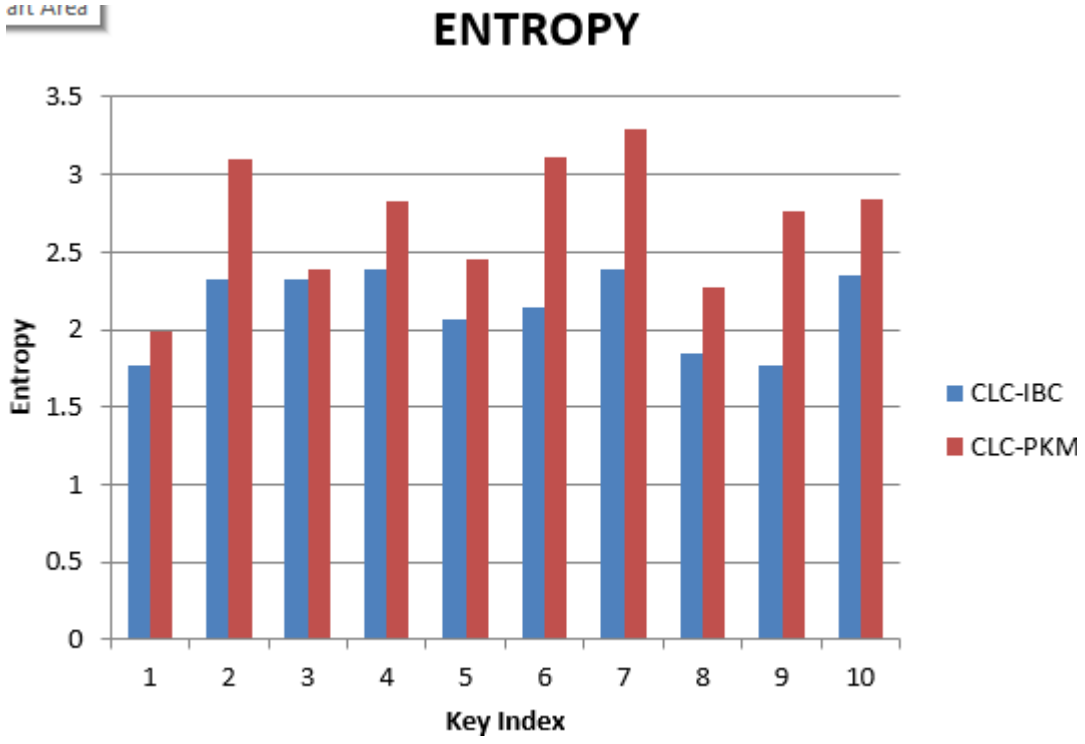

Figure 5.9: Analysis based upon entropy on scenario (IoT) with 150 nodes

The entropy of the proposed model has been recorded higher than 2 and below 3.5 on all of the data events in the given scenario. The proposed model has been found consistently higher than the existing model on all of the data events, which is clearly visible from the given scenario (Figure 5.9). The existing model is recorded between 1.7 and 2.4, which is considerably lower than the proposed model on all of the events.

5.5 Comparative Analysis

5.5.1 Energy Consumption

The proposed model has been recorded with energy consumption in different scenarios with different number of nodes. The energy consumption trend is rising with rise in the number of nodes according to the following 5.7. Afterwards the average value of the energy consumption for all of the scenarios has been drawn in order to compare the proposed model's performance with the existing models.

Table 5.7: Energy consumption of scenarios with different number of nodes

No. of Nodes	Energy (mJ)
50	17.18
100	21.49
150	27.31
200	32.72
250	36.43
Average	27.026

The proposed model has been found efficient in comparison with the existing models. The proposed model has been recorded with the value of 27.026 milli-joules of energy consumption, whereas the existing models , are recorded with 46.63 (CLC-IBC), 100.83 (MXH) and 69.99 (YHZXZ) schemes, which clearly shows the robustness of the proposed model in handling the data traffic with minimum energy consumption due to lower complexity level of the proposed security scheme 5.8.

Table 5.8: Energy consumption comparison with existing schemes

Scheme	Energy Consumption(mJ)
YHZXZ	69.99
MXH	100.83
CLC-IBC	46.63
Proposed	27.026

The following 5.10 describes the above 5.8 graphically, which again justifies the similar trend. The proposed model has been found efficient in comparison with all of the existing models as per shown in the following 5.10.

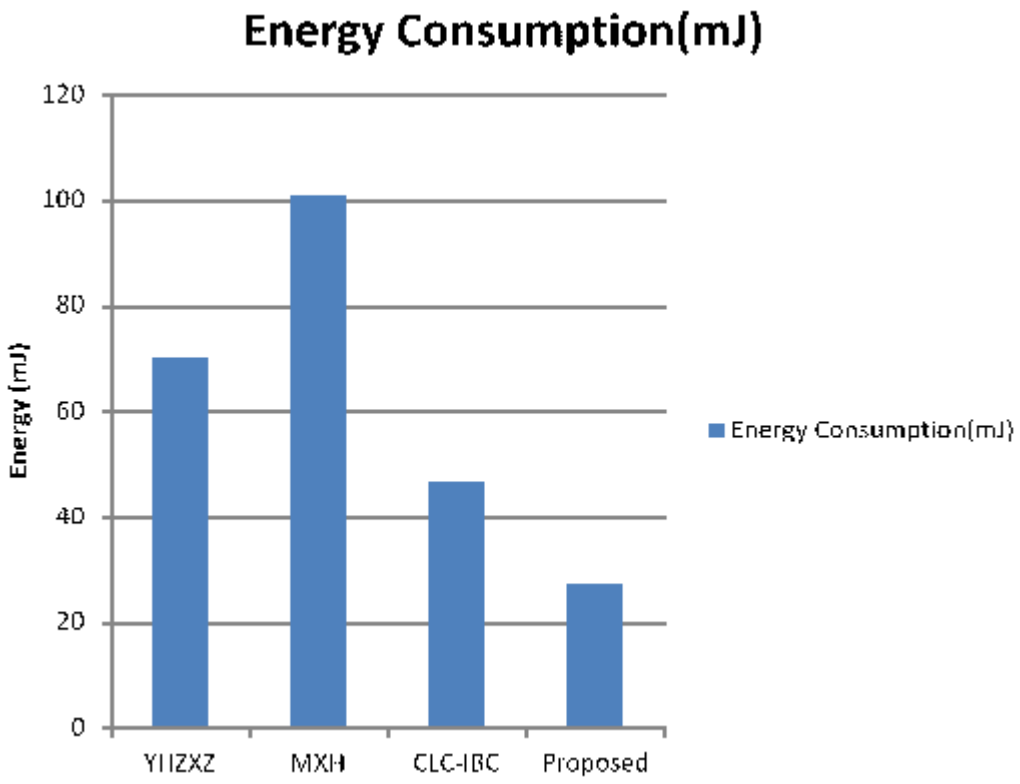

Figure 5.10: Energy consumption comparison with existing schemes

Computational Time The proposed model has been recorded with computational time in different scenarios with different number of nodes and varying transmission radius according to the number of nodes. The computational time trend is similar to the energy consumption and rising with rise in the number of nodes according to the following table (Table 5.9). Afterwards the average value of the computational time for all of the scenarios has been drawn in order to compare the proposed model's performance with the existing models.

Table 5.9: Computational Time of scenarios with different number of nodes

No. of Nodes	Computational Time (seconds)
50	0.04
100	0.09
150	0.16
200	0.29
250	0.53
average	0.222

The proposed model has been recorded with the computational time of 0.22 seconds (Average of all scenarios), which is the lower value against all other readings. The CLC-IBC, MXH and YHZXZ

schemes took 1.9 seconds, 4.05 second and 2.43 seconds respectively, which shows the robustness of the proposed model 5.10.

Table 5.10: Computational time comparison with existing schemes

Scheme	Time(sec)
YHZXZ	2.43
MXH	4.05
CLC-IBC	1.9
Proposed	0.22

The following figure (Figure 5.11) describes the above table graphically for the results of computational time, which again justifies the similar trend as per shown in the table 5.10. The proposed model has been found efficient in comparison with all of the existing models as per shown in the following figure (Figure 5.11) in the terms of computational time, which shows the rapidness of proposed model in handling the data traffic over the IoT networks.

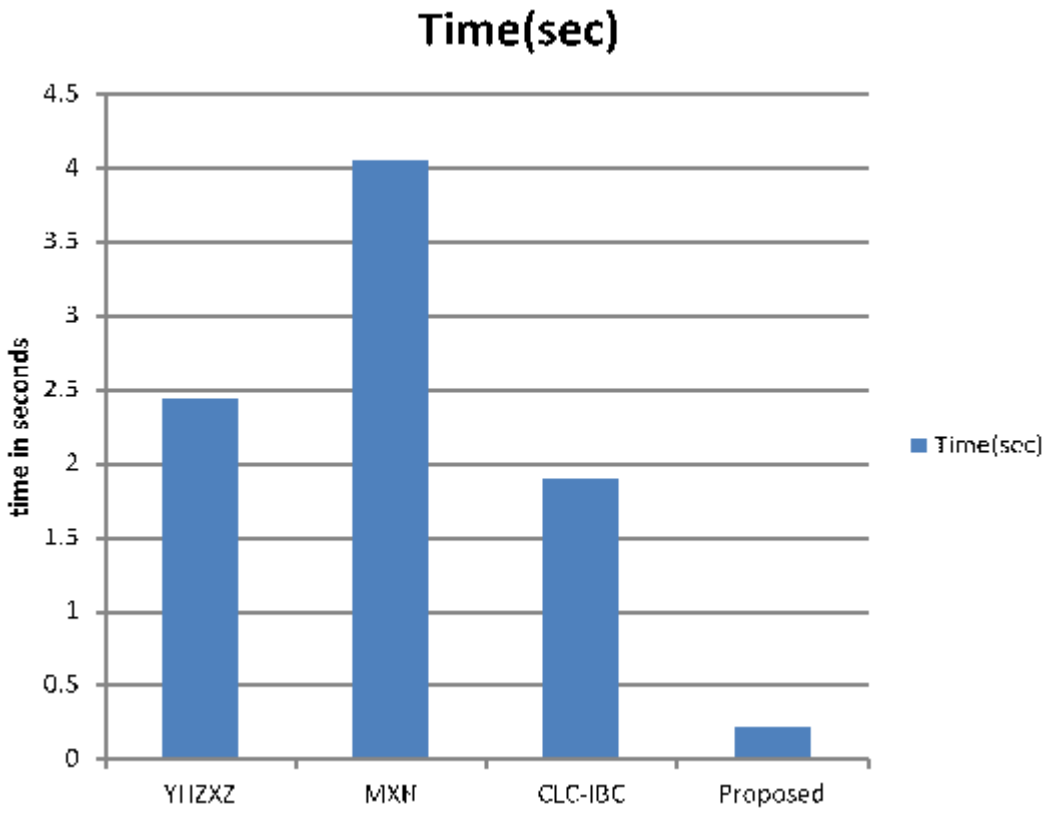

Figure 5.11: Computational time comparison with existing schemes

Chapter 6

CONCLUSION

6.1 Conclusion

The proposed model is designed to incorporate the security over the internet of things (IoT) oriented networks consisted over the wireless mediums. The IoT networks are versatile networks, and have been used in the variety of applications. The limited resources of the IoT nodes push the developers towards the need to light and efficient applications. The requirement of security becomes the most important and vital requirement for the IoT networks. The IoT in healthcare, military applications with sensitive data, and other security sensitive applications require the efficient and light security mechanism, which consumes the lowest possible resources and high entropy values. In this thesis, the proposed model has been designed on the basis of paired key mechanism (PKM) for authentication along with advanced encryption standard (AES) cryptography for the enforcement of the security protocol over the internet of things (IoT). The multi-column complex key formation plays the vital role in the proposed model design. The set of algebraic functions are used for the formation of the complex keys over the multiple columns in the key table consisted of N rows and 8 columns. The paired key mechanism (PKM) based authentication uses the two sets of coefficients to produce the query key (columns 1 to 4, total 4 columns) and answer key (4 to 8, total 5 columns) from the key table using the cubic and quartic equation respectively. The experimental results show the average projected value of proposed model at 2.82, 13.218 and 28.337 against the 1.598, 2.523 and 15.962 of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The experimental results show the average projected value of existing model at 2.82, 13.218 and 28.337 percent against the proposed model's 1.598, 2.523 and 15.962 percent of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The comparison shows the average entropy of proposed model at 2.52, 2.82 and 2.71 percent against the existing model's 2.0, 2.13 and 2.13 percent of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The results clearly shows the improved performance of proposed model than the existing model.

6.2 Future Work

The multi-column authentication model can be further extended with more efficient equations for the creation of the query and answer keys over the key table produced using the pseudo random number generator (PRNG). The proposed model can be further improved using the optimization algorithms such as genetic algorithm (GA), particle swarm optimization (PSO) and bee swarm optimization (BSO). The use of travel salesman problem (TSP) based algorithm for aligning up the key values obtained from the columns to reduce the rigidness of the column based dependency for the generation of the query and answer keys, which can increase the higher order of security.

References

[1] Zareei, Mahdi, AKM Muzahidul Islam, Sabariah Baharun, and Shozo Komaki. *"Energy-efficient and mobility-aware MAC protocol for wireless sensor networks."* In 2013 19th Asia-Pacific Conference on Communications (APCC), pp. 110-114. IEEE, 2013.

[2] Akinyele, Joseph A., Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary NJ Peterson, and Aviel D. Rubin. *"Securing electronic medical records using attribute-based encryption on mobile devices."* InProceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, pp. 75-86. ACM, 2011.

[3] Almashaqbeh, Ghada, Thaier Hayajneh, and Athanasios V. Vasilakos. *"A cloud-based interference-aware remote health monitoring system for non-hospitalized patients."* In 2014 IEEE Global Communications Conference, pp. 2436-2441. IEEE, 2014.

[4] Alshehri, Suhair, Stanislaw P. Radziszowski, and Rajendra K. Raj. *"Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption."* In Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on, pp. 143-146. IEEE, 2012.

[5] Arzeno, Natalia M., Chi-Sang Poon, and Zhi-De Deng. *"Quantitative analysis of QRS detection algorithms based on the first derivative of the ECG."* InEngineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE, pp. 1788-1791. IEEE, 2006.

[6] Benitez, D., P. A. Gaydecki, A. Zaidi, and A. P. Fitzpatrick. *"The use of the Hilbert transform in ECG signal analysis."* Computers in biology and medicine 31, no. 5 (2001): 399-406.

[7] Blom, Rolf. *"An optimal class of symmetric key generation systems."* InWorkshop on the Theory and Application of of Cryptographic Techniques, pp. 335-338. Springer Berlin Heidelberg, 1984.

[8] Du, Wenliang, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili. *"A pairwise key predistribution scheme for wireless sensor networks."* ACM Transactions on Information and System Security (TISSEC) 8, no. 2 (2005): 228-258.

[9] Fan, Lu, W. Buchanan, C. Thummler, Owen Lo, A. Khedim, Omair Uthmani, Alistair Lawson, and Derek Bell. "DACAR platform for eHealth services cloud. *"DACAR platform for eHealth services cloud."* In Cloud Computing (CLOUD), 2011 IEEE International Conference on, pp. 219-226. IEEE, 2011.

[10] Fitch, Daniel F., and Haiping Xu. *"A Petri Net Model for Secure and Fault-Tolerant Cloud-Based Information Storage."* In SEKE, pp. 333-339. 2012.

[11] Lee, Craig A., Samuel D. Gasster, Antonio Plaza, Chein-I. Chang, and Bormin Huang. *"Recent developments in high performance computing for remote sensing: A review."* IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 4, no. 3 (2011): 508-527.

[12] Sebastian, Sherin, Neethu Rachel Jacob, Yedu Manmadhan, V. R. Anand, and M. J. Jayashree. *"Remote patient monitoring system."* International Journal of Distributed and Parallel Systems 3, no. 5 (2012): 99.

[13] Kim, Changmoo, Mookyoung Chung, Yeongon Cho, Mario Konijnenburg, Soojung Ryu, and Jeongwook Kim. *"ULP-SRP: Ultra low power Samsung Reconfigurable Processor for biomedical applications."* In Field-Programmable Technology (FPT), 2012 International Conference on, pp. 329-334. IEEE, 2012.

[14] Li, Ming, Shucheng Yu, Kui Ren, and Wenjing Lou. *"Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings."* In International Conference on Security and Privacy in Communication Systems, pp. 89-106. Springer Berlin Heidelberg, 2010.

[15] Hossain, M. Shamim, and Ghulam Muhammad. *"Cloud-based collaborative media service framework for healthcare."* International Journal of Distributed Sensor Networks 2014 (2014).

[16] Miller, Frederic P., Agnes F. Vandome, and John McBrewster. *"Advanced Encryption Standard."* (2009).

[17] Nakano, Masanao, Toshihiro Konishi, Shintaro Izumi, Hiroshi Kawaguchi, and Masahiko Yoshimoto. *"Instantaneous Heart Rate detection using short-time autocorrelation for wearable healthcare systems."* In 2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 6703-6706. IEEE, 2012.

[18] Su, Yangang, Wenzhi Pan, Xue Gong, Jie Cui, Xianhong Shu, and Junbo Ge. *"Relationships between paced QRS duration and left cardiac structures and function."* Acta cardiologica 64, no. 2 (2009): 231-238.

[19] Pandey, Suraj, William Voorsluys, Sheng Niu, Ahsan Khandoker, and Rajkumar Buyya. *"An autonomic cloud environment for hosting ECG data analysis services."* Future Generation Computer Systems 28, no. 1 (2012): 147-154.

[20] Rolim, Carlos Oberdan, Fernando Luiz Koch, Marcos Dias de Assunção, and Carlos Becker Westphall. *"Towards a Grid of Sensors for Telemedicine."* InCBMS, pp. 485-490. 2006.

[21] Rosenthal, Arnon, Peter Mork, Maya Hao Li, Jean Stanford, David Koester, and Patti Reynolds. *"Cloud computing: a new business paradigm for biomedical information sharing."* Journal of biomedical informatics 43, no. 2 (2010): 342-353.

[22] Smid, Miles E. *"A key notarization system for computer networks."* No. 54. US Dept. of Commerce, National Bureau of Standards: for sale by the Supt. of Docs., US Govt. Print. Off., 1979.

[23] Verma, Om Prakash, Ritu Agarwal, Dhiraj Dafouti, and Shobha Tyagi. *"Peformance analysis of data encryption algorithms."* In Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol. 5, pp. 399-403. IEEE, 2011.

[24] Wan, J, Zou, C, Ullah, S, Lai, C F, Zhou, M, & Wang *"Cloud-enabled wireless body area networks for pervasive healthcare"* IEEE Network, 27(5), 56-61

[25] Wang, H, Peng, D, Wang, W, Sharif, H, Chen, H H, & Khoynezhad *"Resource-aware secure ECG healthcare monitoring through body sensor networks Wireless Communications"* IEEE, 17(1), 12-19

[26] Amiri-Zarandi, Mohammad, Maryam Fadaee, and Naser Hashemi. *"Solving recursive equations in analytical modeling of distributed systems."* InInformation and Knowledge Technology (IKT), 2015 7th Conference on, pp. 1-5. IEEE, 2015.

[27] Zhou, Yun, Yuguang Fang, and Yanchao Zhang. *"Securing wireless sensor networks: a survey."* IEEE Communications Surveys & Tutorials 10, no. 3 (2008): 6-28.

[28] Zhou, Chenfeng Vincent, Christopher Leckie, and Shanika Karunasekera. *"A survey of coordinated attacks and collaborative intrusion detection."* Computers & Security 29, no. 1 (2010): 124-140.

[29] Zhou, Jun, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, and Athanasios V. Vasilakos. *"Securing m-healthcare social networks: Challenges, countermeasures and future directions."* IEEE Wireless Communications 20, no. 4 (2013): 12-21.

[30] Zhou, Jun, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao. *"PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System."*IEEE Transactions on Parallel and Distributed Systems 26, no. 6 (2015): 1693-1703.