

# A NOVEL FRAMEWORK FOR SECURING IOT-BASED APPLICATIONS USING BLOCKCHAIN

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Applications

By

Rohit

Registration Number: 12105464

Supervised By

**Dr. Sakshi Dua**

School of Computer Applications  
(Associate Professor)  
Lovely Professional University

Co-Supervised By

**Dr. Preeti Shoran**

Department of Sciences  
(Associate Professor)  
Christ University  
Uttar Pradesh, India.



LOVELY PROFESSIONAL UNIVERSITY, PUNJAB

2025



## DECLARATION

I, hereby declared that the presented work in the thesis entitled, “**A Novel Framework for Securing IoT-Based Applications using Blockchain**” in fulfillment of degree of Doctor of Philosophy (Ph.D.) is the outcome of research work carried out by me under the supervision of Dr. Sakshi Dua, working as Associate Professor in Computer Application, in the School of Computer Applications of Lovely Professional University, Punjab, India. In keeping with the general practice of reporting scientific observations, due acknowledgements have been made whenever the work described here has been based on the findings of another investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.

(Signature of Scholar)

Rohit

Registration No.:12105464

School of Computer Applications,

Lovely Professional University, Punjab, India.



## CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled, “**A Novel Framework for Securing IoT-Based Applications using Blockchain**” submitted in fulfillment of the requirement for the reward of degree of Doctor of Philosophy (Ph.D.) in the School of Computer Applications of Lovely Professional University, Punjab, India, is a research work carried out by **Rohit, Registration No. 12105464**, is Bonafide record of his original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

**(Signature of Supervisor)**

Dr. Sakshi Dua

Associate Professor

School of Computer Application,

Lovely Professional University, Punjab, India



## ACKNOWLEDGEMENT

This thesis marks the conclusion of a journey that has been both difficult and rewarding. I am genuinely thankful to everyone whose support, guidance, and encouragement have meant a great deal to me. First and foremost, I want to sincerely thank Lord Shiva, the Most Gracious and Merciful, for providing me with the strength, wisdom, and perseverance to complete this work.

I want to sincerely thank my Supervisor, **Dr. Sakshi Dua**, whose unwavering support, wisdom, and expertise have been the foundation of this entire research journey. From the very beginning, Dr. Dua, you have been more than just a guide; you have been a source of strength, encouragement, and emotional reassurance. Your thoughtful feedback, patience, and consistent motivation helped me through moments of uncertainty and self-doubt. I am truly grateful to have a supervisor who believed not only in the potential of my work but also in me as a person. Your compassion and dedication have made a significant impact on my academic and personal growth, and I will always cherish your role in this process. This journey wouldn't have been possible without your emotional and intellectual support, and for that, I am forever thankful.

I also want to sincerely thank my Co-Supervisor, **Dr. Preety Shoran**, from the Department of Sciences at CHRIST(Deemed to be University), Ghaziabad, Uttar Pradesh, India. Your ongoing support, kind mentorship, and valuable insights have meant a lot to me. Your encouragement provided strength during tough times and greatly enhanced this thesis.

I sincerely thank **Dr. Sophiya Sheikh** for their invaluable advice and support throughout my research. My appreciation also goes to **Dr. Rishi Chopra**, HOD of the School of Computer Applications at Lovely Professional University, Punjab. Their inspiring leadership has fostered a positive and encouraging environment for research and learning, which played a crucial role in the successful completion of this thesis. I am genuinely grateful for their steadfast support and the opportunities they've given me. Lastly, I want to warmly thank all the faculty members of the School of Computer Applications at Lovely Professional University, Punjab. To my RAC members, your constructive critiques and invaluable suggestions have significantly enriched this research. Your diverse perspectives and expertise have been instrumental in refining my ideas and pushing the boundaries of my work.

I am also deeply thankful to my colleagues and friends in Lovely Professional

University. Your camaraderie, collaborative spirit, and intellectual exchange have made this journey enjoyable, memorable, and intellectually stimulating. Special thanks to Dr. Ajay Nain, Pawan Bhaker, Dr. Pinki, Dr. Kapil Yadav, Dr. Sheikh Umar Mushtaq, Dr. Avtar Singh, Dr. Sandeep Sheokand, Atul and Mohit Yadav. This research would not have been possible without their emotional support and invaluable help assistance.

A heartfelt thank you to my family, whose constant love and faith in me have truly been my foundation. To my wonderful parents, whose words and actions instilled in me the strength of perseverance and the importance of hard work, your patience, love, and unwavering support have truly been my anchor throughout this journey. Your unwavering belief in me, especially during times when I doubted myself, gave me the courage to keep going. I am deeply grateful for you being my rock every step of the way. To my amazing siblings, your constant encouragement and understanding mean the world to me. I am forever thankful for your sacrifices and endless support, which made this achievement possible. Thank you all from the bottom of my heart!

Lastly, I dedicate this thesis to my beloved family **Late Ch. Satyawan Malik** (Father), **Smt. Kamlesh Devi** (Mother), **Devwanti** and **Dr. Sudesh** (Sisters), **Shakti, Neeraj and Jonny** (Brothers), beloved son **Dakshit Malik** and wife **Sonam**, whose inspiration continues to guide me. Your legacy of passion and dedication consistently reminds me of the values I aim to uphold. This journey has been a beautiful mosaic filled with countless moments of learning, perseverance, and growth. To everyone who has been part of this journey, thank you so much for your trust, support, and encouragement. Your presence has truly made this experience more meaningful and memorable.

*This thesis truly belongs to all of us, embodying our shared efforts and collective spirit.*

# Abstract

The advancement of Internet of Things (IoT) technologies has transformed industries by enabling constant connectivity, automation, and data application. IoT devices are used in healthcare, smart homes, transportation, and industrial systems, which continuously produce enormous data. This technological progress has also introduced new challenges such as better resource utilisation, balanced data security and privacy, and improved system efficiency. As IoT ecosystems diversify, managing various engineering devices, communication, and workloads requires additional solutions to maintain trust and reliability.

Traditional cloud computing architectures offer extensive storage and processing power vital for IoT services. However, these centralised systems are often vulnerable to latency issues, longer transmission times, and excessive reliance on peripheral servers. Such delays in handling time-sensitive and critical data pose serious challenges and can affect the functioning of essential applications like autonomous systems and healthcare monitoring, where minimal delay is crucial. Additionally, reliance on central control systems raises trust issues, as any failure or malicious attack within the network could compromise the entire system.

To address these issues, blockchain technology has emerged as a potential solution for securing applications based on IoT technology. Its decentralised structure, combined with its immutable ledger, provides transparency without the possibility of alteration, as well as trustless data exchanges among IoT devices. Moreover, blockchain technology offers robust identity verification, secure payment transactions, and mediated agreements without a central authority over all participants, enabling fully distributed systems. Integrating these features ensures blockchain technology enhances IoT system security, reduces vulnerabilities, and optimises resource use. The system maintains efficiency alongside reliability across various IoT applications.

The thesis starts with an Introduction Chapter, i.e. Chapter 1 that explains the utilized technologies, motivation, scope and objectives of the study. A detailed literature review is done in Chapter 2, which examines current Blockchain frameworks for securing IoT applications, while also identifying gaps in current studies. To Improve resource optimisation and securing data with blockchain technology, Chapter 3 introduces a combination of blockchain with advanced optimisation techniques to enhance resource use in IoT networks. This integration facilitates an allocation mechanism that not only enhances data integrity but also

detects malicious nodes. To lower energy consumption and delays, the Hybrid Artificial Bee Colony-Whale Optimization Algorithm (ABC-WOA) is used to enhance these processes. The simulation results, showing improvements in energy efficiency, detection probability, false alarm rate, and throughput, support the role of blockchain in optimizing resources within IoT. Chapter 4 introduces a blockchain based node authentication mechanism for securing EHRs. This study proposes a novel blockchain-based node authentication algorithm for IoT healthcare, integrating Hyperledger Fabric, Homomorphic Encryption, and Recurrent Neural Networks(RNN). Employing a dual-layer security approach, the methodology utilizes a challenge response mechanism and dynamic key exchange to ensure tamper-proof data transmission. Encrypted processing preserves confidentiality, while machine learning enhances anomaly detection accuracy to 99.01%, achieving a security rate of 99%. Comprehensive evaluations demonstrate significant improvements in efficiency, scalability, and robustness, addressing latency and computational overhead challenges. Chapter 5 introduces A learning mechanism for an intelligent healthcare communication system that uses blockchain for secure network interactions and includes a data evaluation layer based on cloud technology. This layer actively separates and ranks transactions into three main categories: Good, Moderate, and Malware. This paper introduces several significant contributions, such as the development of a secure blockchain framework for user authentication and a protected digital ledger for communication. Additionally, it incorporates a cloud-driven data analysis layer combined with a neural network to improve training accuracy and category classification. The developed algorithm surpassed the existing works in terms of Quality of Service (QoS) Parameters with low latency, Bit Error Rate (BER), higher Signal to Interference Plus Noise Ratio (SINR), Packet Delivery Ratio (PDR), True Detection Rate (TDR), False Detection Rate (FDR), and Throughput. Also, a thorough comparison of consensus mechanisms like Practical Byzantine Fault Tolerance (pBFT), Proof of Work (PoW), Raft, and Paxos is done to ensure which consensus helps optimize the proposed system in terms of security and fault tolerance with low latency and energy-efficient operations. Also, it establishes a secure and efficient communication network for smart healthcare, aimed at enhancing the overall quality of life for individuals. The thesis is concluded in Chapter 6 with key findings, contributions and directions for future work. The Proposed work advances the development of a blockchain based framework for securing IoT applications which is secure, scalable and efficient in today's environments.

# Contents

|                                                              |          |
|--------------------------------------------------------------|----------|
| Abstract . . . . .                                           | iii      |
| List of Figures . . . . .                                    | ix       |
| List of Tables . . . . .                                     | xiii     |
| <b>1 Introduction</b>                                        | <b>1</b> |
| 1.1 IoT . . . . .                                            | 2        |
| 1.1.1 Layers in IoT System . . . . .                         | 3        |
| 1.1.2 Components of IoT devices . . . . .                    | 4        |
| 1.1.3 Advantages of IoT Systems . . . . .                    | 5        |
| 1.1.4 Data Handling in IoT Devices . . . . .                 | 6        |
| 1.2 Concerns in IoT Devices . . . . .                        | 7        |
| 1.2.1 Data Security . . . . .                                | 8        |
| 1.2.2 Scalability . . . . .                                  | 9        |
| 1.2.3 Data Processing and Handling . . . . .                 | 9        |
| 1.2.4 Importance of Cloud Computing in IoT Systems . . . . . | 10       |
| 1.2.5 Attacks and Security Issues in IoTs . . . . .          | 11       |
| 1.3 Machine Learning . . . . .                               | 13       |
| 1.3.1 RNN . . . . .                                          | 15       |
| 1.3.2 Deep Neural Network (DNN) . . . . .                    | 17       |
| 1.4 Blockchain Technology . . . . .                          | 18       |
| 1.4.1 Blockchain Components . . . . .                        | 19       |

|          |                                                                                  |           |
|----------|----------------------------------------------------------------------------------|-----------|
| 1.4.2    | Characteristics of Blockchain . . . . .                                          | 21        |
| 1.4.3    | Types of Blockchain . . . . .                                                    | 22        |
| 1.4.4    | Blockchain Technology With Multi-Layered Architecture .                          | 25        |
| 1.4.5    | Consensus Mechanism in Blockchain Technology . . . . .                           | 26        |
| 1.4.6    | Attacks in Blockchain . . . . .                                                  | 29        |
| 1.5      | Cryptography . . . . .                                                           | 29        |
| 1.5.1    | Modern Cryptography . . . . .                                                    | 30        |
| 1.5.2    | Digital Signature . . . . .                                                      | 31        |
| 1.5.3    | RSA . . . . .                                                                    | 31        |
| 1.5.4    | SHA-256 . . . . .                                                                | 31        |
| 1.5.5    | Homomorphic Encryption . . . . .                                                 | 32        |
| 1.6      | Authentication . . . . .                                                         | 32        |
| 1.6.1    | Challenge-Response Mechanism . . . . .                                           | 33        |
| 1.6.2    | Polynomial Curve Fitting . . . . .                                               | 33        |
| 1.7      | Blockchain in IoT Architecture . . . . .                                         | 34        |
| 1.7.1    | Utilization of Integration of IoT and Blockchain in various<br>sectors . . . . . | 36        |
| 1.8      | Challenges of Using Blockchain for Securing IoT Devices . . . . .                | 39        |
| 1.9      | Research Objectives . . . . .                                                    | 41        |
| 1.10     | Scope and Motivation . . . . .                                                   | 41        |
| 1.11     | Organization of the Thesis . . . . .                                             | 42        |
| 1.12     | Summary of Context . . . . .                                                     | 43        |
| <b>2</b> | <b>Review of Literature</b>                                                      | <b>45</b> |
| 2.1      | Research Methodology and Plan of Study . . . . .                                 | 46        |
| 2.1.1    | Nature of Searching . . . . .                                                    | 47        |
| 2.1.2    | Sources of Data . . . . .                                                        | 47        |
| 2.1.3    | Duration of Study . . . . .                                                      | 48        |

|          |                                                                                                                   |           |
|----------|-------------------------------------------------------------------------------------------------------------------|-----------|
| 2.1.4    | Study Selection Criteria . . . . .                                                                                | 48        |
| 2.1.5    | Review Judgement . . . . .                                                                                        | 49        |
| 2.2      | Literature Review . . . . .                                                                                       | 50        |
| 2.3      | Node Authentication/Authorization<br>in Blockchain . . . . .                                                      | 60        |
| 2.4      | Machine Learning based Security Environment for IoTs using Blockchain                                             | 65        |
| 2.5      | Real-World Deployment Challenges in Blockchain-Enabled IoT Sys-<br>tems . . . . .                                 | 69        |
| 2.6      | Summary of Context . . . . .                                                                                      | 71        |
| <b>3</b> | <b>Enhancing Security and Resource Optimization in IoT-Edge-Cloud<br/>using Blockchain</b>                        | <b>73</b> |
| 3.1      | Proposed Model . . . . .                                                                                          | 73        |
| 3.1.1    | Local Execution . . . . .                                                                                         | 74        |
| 3.1.2    | Remote Execution . . . . .                                                                                        | 74        |
| 3.1.3    | Transmission Time & Energy Consumption . . . . .                                                                  | 74        |
| 3.1.4    | Latency Model with Blockchain Systems . . . . .                                                                   | 75        |
| 3.1.5    | Hybrid Optimization Algorithm . . . . .                                                                           | 77        |
| 3.1.6    | Computational Complexity . . . . .                                                                                | 78        |
| 3.2      | Result . . . . .                                                                                                  | 78        |
| 3.2.1    | Computation Time . . . . .                                                                                        | 81        |
| 3.2.2    | Average Energy Consumption . . . . .                                                                              | 82        |
| 3.3      | Summary of Context . . . . .                                                                                      | 82        |
| <b>4</b> | <b>Blockchain-based Node Authentication Algorithm for Securing<br/>Electronic Health Record Data Transmission</b> | <b>84</b> |
| 4.1      | The System Model . . . . .                                                                                        | 85        |
| 4.1.1    | System Architecture . . . . .                                                                                     | 86        |
| 4.1.2    | Adversarial Model . . . . .                                                                                       | 93        |

|          |                                                                                                           |            |
|----------|-----------------------------------------------------------------------------------------------------------|------------|
| 4.1.3    | Proposed Methodology . . . . .                                                                            | 93         |
| 4.1.4    | Proposed Algorithm . . . . .                                                                              | 94         |
| 4.1.5    | Evaluation Metrics . . . . .                                                                              | 96         |
| 4.2      | Experimental Study . . . . .                                                                              | 98         |
| 4.2.1    | Experimental Setup . . . . .                                                                              | 98         |
| 4.2.2    | Results and Discussion . . . . .                                                                          | 99         |
| 4.3      | Summary of Context . . . . .                                                                              | 105        |
| <b>5</b> | <b>Blockchain-Integrated Deep Learning Framework for Securing Smart Healthcare Communication Networks</b> | <b>106</b> |
| 5.1      | System Model . . . . .                                                                                    | 108        |
| 5.1.1    | System Architecture . . . . .                                                                             | 108        |
| 5.1.2    | Adversarial Model . . . . .                                                                               | 112        |
| 5.1.3    | Proposed Methodology . . . . .                                                                            | 113        |
| 5.1.4    | Proposed Algorithms . . . . .                                                                             | 113        |
| 5.1.5    | Performance Metrics . . . . .                                                                             | 117        |
| 5.2      | Experimental Study . . . . .                                                                              | 119        |
| 5.2.1    | Experimental Setup . . . . .                                                                              | 119        |
| 5.2.2    | Results and Analysis . . . . .                                                                            | 120        |
| 5.3      | Summary of Context . . . . .                                                                              | 129        |
| <b>6</b> | <b>Conclusion and Future Scope</b>                                                                        | <b>130</b> |
| 6.1      | Conclusion . . . . .                                                                                      | 131        |
| 6.1.1    | Limitations . . . . .                                                                                     | 134        |
| 6.2      | Future Scope . . . . .                                                                                    | 134        |
|          | Bibliography . . . . .                                                                                    | 137        |

# List of Figures

|      |                                                                   |    |
|------|-------------------------------------------------------------------|----|
| 1.1  | The Centralized IoT System . . . . .                              | 3  |
| 1.2  | IoT Layered System Architecture . . . . .                         | 5  |
| 1.3  | Important Aspects of Data Security in IoT Systems . . . . .       | 8  |
| 1.4  | Various Security and Privacy Issues in the IoT Architecture . . . | 11 |
| 1.5  | Supervised Learning . . . . .                                     | 14 |
| 1.6  | Un-Supervised Learning . . . . .                                  | 15 |
| 1.7  | Recurrent Neural Network . . . . .                                | 15 |
| 1.8  | Deep Neural Network . . . . .                                     | 17 |
| 1.9  | Basic Blockchain Working and Structure . . . . .                  | 19 |
| 1.10 | Components of Blockchain . . . . .                                | 20 |
| 1.11 | Characteristics of Blockchain Technology . . . . .                | 21 |
| 1.12 | Types of Blockchain Technology . . . . .                          | 24 |
| 1.13 | Layered Architecture of Blockchain Technology . . . . .           | 26 |
| 1.14 | Integrated Architecture of IoT and Blockchain Technology . . . .  | 35 |
| 2.1  | Percentage of Articles from Publishing Sources . . . . .          | 47 |
| 2.2  | Number of Articles (Year Wise) . . . . .                          | 48 |
| 2.3  | Flow Chart of Inclusion Exclusion Criteria . . . . .              | 50 |
| 3.1  | Probability of Detection Measure . . . . .                        | 79 |
| 3.2  | False Alarm Probability Function . . . . .                        | 79 |
| 3.3  | Average Network Throughput . . . . .                              | 80 |

|     |                                                                                               |     |
|-----|-----------------------------------------------------------------------------------------------|-----|
| 3.4 | Energy Efficiency . . . . .                                                                   | 80  |
| 3.5 | Convergence Plot Showing the Relationship Between Time Delay<br>and Iteration Count . . . . . | 81  |
| 3.6 | Convergence Plot Depicting Total Energy Varies with the Number<br>of Iterations . . . . .     | 82  |
| 4.1 | The Proposed System Model Architecture . . . . .                                              | 86  |
| 4.2 | Hyperledger Blockchain Architecture . . . . .                                                 | 89  |
| 4.3 | Homomorphic Encryption Architecture . . . . .                                                 | 91  |
| 4.4 | The flowchart of the Proposed System Model . . . . .                                          | 97  |
| 4.5 | Performance Metrics of the Proposed Method . . . . .                                          | 100 |
| 4.6 | Performance Metrics of the Proposed Method . . . . .                                          | 103 |
| 4.7 | Comparison of Encryption Time of Proposed Method with Existing<br>Methods . . . . .           | 104 |
| 4.8 | Comparison of Encryption Time of Proposed Method with Existing<br>Methods . . . . .           | 104 |
| 4.9 | A Comparison of the Security of the Suggested Approach and Ex-<br>isting Approaches . . . . . | 104 |
| 5.1 | The Blockchain-based Smart Healthcare System Architecture . . . .                             | 108 |
| 5.2 | Flowchart for the Proposed Model . . . . .                                                    | 114 |
| 5.3 | Throughput Comparison of the Proposed System with Other Re-<br>lated Works . . . . .          | 122 |
| 5.4 | Comparison of BER of Proposed System with Other Related Works                                 | 123 |
| 5.5 | PDR Comparison of the Proposed System with Other Related Works                                | 123 |
| 5.6 | Comparison of SINR of Proposed System with Other Related Works                                | 124 |
| 5.7 | Analysis of the Suggested System's Latency in Relation to Previous<br>Research . . . . .      | 125 |
| 5.8 | Analysis of TDR and FDR with respect to the Increasing Number<br>of Nodes . . . . .           | 125 |

|     |                                                               |     |
|-----|---------------------------------------------------------------|-----|
| 5.9 | Comparison of Various Blockchain Consensus Mechanisms . . . . | 126 |
|-----|---------------------------------------------------------------|-----|



# List of Tables

|     |                                                                                             |     |
|-----|---------------------------------------------------------------------------------------------|-----|
| 1.1 | Comparison of permissionless and permissioned blockchain . . . .                            | 25  |
| 1.2 | Technologies for Blockchain Implementation in Different Sectors .                           | 38  |
| 2.1 | Comparative Analysis of Recent Approaches focusing Blockchain<br>for IoT security . . . . . | 58  |
| 2.2 | Comparison of Different Techniques in Related Studies . . . . .                             | 63  |
| 2.3 | Summary of Studies on Blockchain and IoT Applications . . . . .                             | 68  |
| 4.1 | Adversarial Model Elements . . . . .                                                        | 93  |
| 4.2 | Software, Parameters used in the Simulation . . . . .                                       | 99  |
| 4.3 | Encryption and Decryption Time of the Proposed Method . . . .                               | 101 |
| 4.4 | Feature Comparison Across Related Studies and the Proposed Method                           | 101 |
| 5.1 | Adversarial Model for Proposed System . . . . .                                             | 112 |
| 5.2 | System Specifications and Ordinal Measures of System Model . .                              | 119 |
| 5.3 | Parameters and Hyperparameters of Deep Neural Network used .                                | 120 |
| 5.4 | Comparative Analysis of Proposed Framework with Related Studies                             | 121 |



# Chapter 1

## Introduction

The IoTs has become a significant component of today's technology in recent years. It allows devices to collect, send, receive, and share data with users through the internet [1]. These devices usually contain some form of sensors and can work on their own without the help of a human being. For example, smartphones and smartwatches are now considered everyday tools that help users obtain Information and complete tasks automatically. Some areas where IoT is applied include smart cities, building management systems, wireless sensor networks, smart farming, healthcare, energy consumption, and security. These applications have further enhanced human quality of life alongside operational efficiency. Despite various benefits, IoT also possesses challenges related to data security and user privacy issues. Most IoT systems utilize a centralized architecture where data from different devices is collected and stored in a central server [2]. This model creates a central point of failure for IoT systems that can be a target for security attacks, as it has the potential to store sensitive data. If an attacker manages to breach the server, they can expose sensitive user information or even disrupt the entire network.

Security remains one of the most important things for IoT environments. With billions of devices connected to an IoT network, each device requires a unique identification and secure methods of communication [3]. To avoid security issues in IoT devices related to data and communication, proper data encryption, authentication, and access control techniques are utilized. Malicious nodes or attackers can pose a threat to the entire network [4]. They can also block IoT devices, therefore, to promote data security, confidentiality, and privacy in centralized architectures, blockchain technology is introduced.

Blockchain technology is introduced as a solution to the above-mentioned prob-

lems with high promise. Blockchain Technology is a decentralized and distributed ledger system that can improve the security, transparency, and trust of IoT-sensitive systems [5, 6]. It enables the recording, storing, and sharing of data by IoT devices without relying on a central server. The features of blockchain systems, such as consensus mechanisms, timestamps, and cryptographic hashing, make the data stored on it unalterable. Information added to the blockchain cannot be deleted or changed, which enhances the reliability of the system. Also, the use of Blockchain eradicates the need for a third-party entity, which enhances the speed of data sharing and improved efficiency at application level. [7].

In IoT systems, blockchain technology improves security by updating each transaction instead of using a third party. The distributed nature of blockchain handles the centralized IoT architecture to prevent a single point of failure throughout the network. It accelerates the data exchange, minimises the cost, and supplies the chain more efficiently. The blockchain collects a group of IoT transactions and considers it a block in the ledger [8, 9]. Using the blockchain in IoT devices maximizes trust and ensures the security of IoT devices.

## 1.1 IoT

In the early 2000's, Kevin Ashton coined the term "IoT" during a conference at Procter and Gamble (P&G). The term emerged as internet connectivity grew more popular and essential during that time. Around the same period, Neil Gershenfeld's book "When Things Start to Think" also explored future developments of IoT. Typically, IoT devices facilitate automated data transactions and feature built-in internet-connected sensors that interface with other devices. These devices include wireless sensors, actuators, and computing units.

An IoT ecosystem consists of interconnected smart devices, which are embedded systems linked to the internet. These devices can sense their environment, process information, and transmit data. Typically, the information is sent to a gateway or another device for processing. IoT devices can interact with other connected devices and execute commands based on the data they receive [10]. Most IoT devices are designed to operate with minimal human intervention. The level of interaction, communication, and data exchange a device can perform largely depends on the specific IoT applications it supports.

Through IoT, individuals can digitally manage their daily activities and processes, increasing efficiency in both work and life. In addition to the rise of smart homes,

IoT is essential for further advancing businesses and industries into smart, controlled digital systems. It allows businesses and organizations to monitor and gain insights into the performance of their systems in real-time, including supply chain and logistics operations. Repetitive manual tasks can be completed more quickly and accurately with the assistance of IoT technology, leading to reduced labour costs for companies. Moreover, IoT responsibly enhances resource management by optimizing production and distribution costs, improving service quality, and enabling transparent customer transactions. The impact of IoT is substantial,

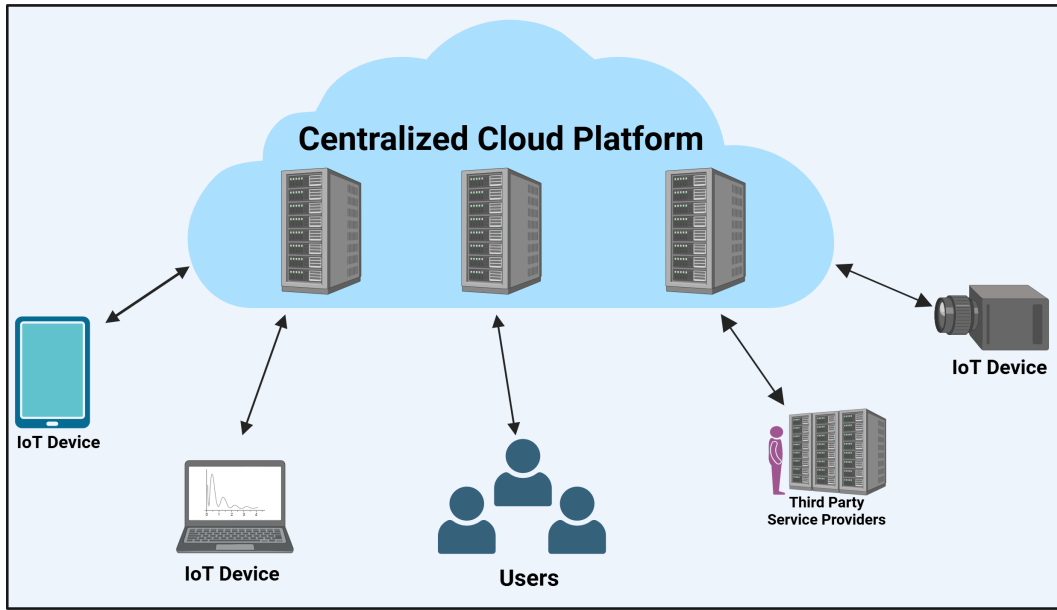


Figure 1.1: The Centralized IoT System

affecting nearly every sector, including finance, healthcare, manufacturing, and retail [11]. IoT generally relies on a centralized architecture, with all devices and objects connected, authenticated, and managed through a central cloud platform. The centralized IoT architecture is shown in Figure 1.1.

### 1.1.1 Layers in IoT System

The IoT architecture consists of three fundamental layers: the Application Layer, the Network Layer, and the Perception Layer [12]. These layers work together to detect, transmit, and process information. Each layer plays a vital role for smooth execution of all operation in the IoT system, reflecting the multi-layered design of the system. The various layers of IoT architecture are explained in detail in Figure 1.2.

#### 1.1.1.1 Perception Layer

This layer, also defined as the sensing layer, constitutes the first level of the IoT architecture. This layer includes wireless sensor networks (WSN), actuators, RFID tags, and other monitoring devices. Its primary function is to detect data and gather information from the environment [12]. The retrieved data is then processed within this layer to generate useful information for the monitoring system.

#### 1.1.1.2 Network Layer

In this layer the IoT devices and objects are connected. It includes a central server that manages communication and processes the information received from the devices. This layer serves as a bridge to the perception layer and the rest of the system. It employs gateways and communication technologies such as broadband, generations of internet, Wi-Fi and broadband for effective data transmission.

#### 1.1.1.3 Application Layer

The application layer handles and processes data obtained from the perception and network layers. It provides digital services for smart cities, smart parking, smart healthcare, and connected vehicles. This layer communicates data using protocols such as CoAP, FTP, HTTP, and SMTP. Additionally, it can enable real-time data analysis to enhance decision-making. By allowing seamless interaction between devices and users, this layer improves overall system efficiency.

### 1.1.2 Components of IoT devices

The elements that constitute an integrated technological system employed in the IoT serve the following functions:

- **Sensors and actuators:** Sensors gather data on temperature, pressure, and movement, while actuators respond to signals by performing actions such as adjusting valves and turning devices off or on.
- **Communication Module:** These devices can connect to the internet or other networks through Wi-Fi, Bluetooth, Zigbee, GSM, or LoRa, thus enabling them to retrieve information.

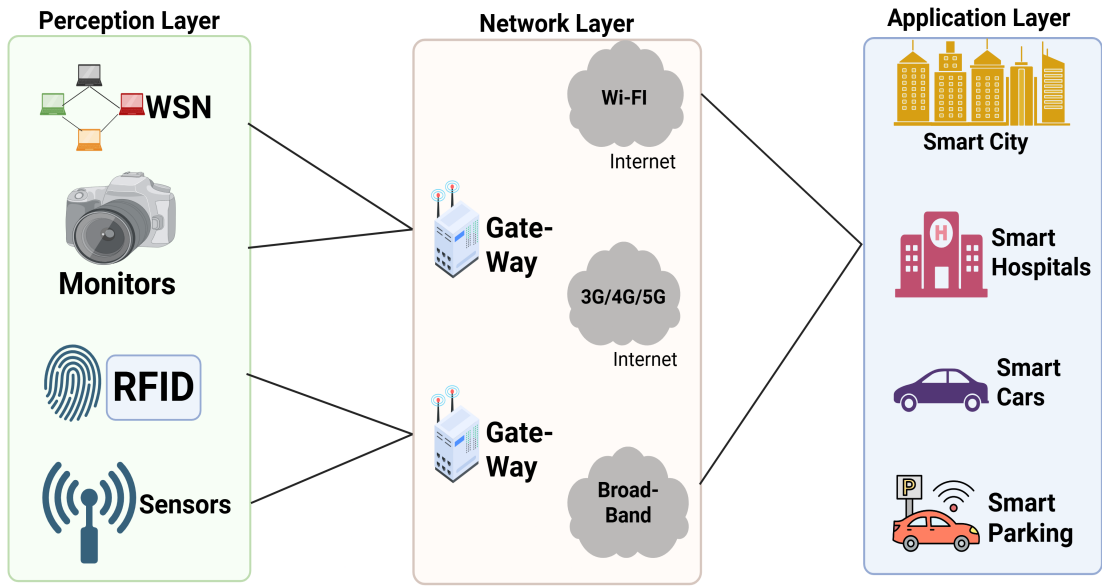


Figure 1.2: IoT Layered System Architecture

- **Microcontroller or Processor:** The processes of automation involve executing predefined tasks, responding to commands, and following instructions.
- **Power Supply:** Reliability in all IoT devices is essential, which may derive from batteries, electricity, or even solar power, depending on the intended function or purpose.
- **Cloud or Local Storage:** Edge devices store data locally, while cloud servers collect and transmit information they receive from IoT devices, undergoing analysis and storage [13].

Together, these components facilitate seamless and efficient machine-to-machine (M2M) communication, making IoT devices essential to the digital transformation of various industries.

### 1.1.3 Advantages of IoT Systems

IoT devices offer versatile benefits, streamline processes, automate tasks, and make effective decisions [14]. These advantages make IoT pivotal in modern technological ecosystems:

- **Convenience:** By enhancing comfort and operational efficiency, IoT devices automate daily tasks and allow for remote control.
- **Energy Efficiency:** Cost and energy savings are achieved by the automatic shut-off of devices that track usage patterns.
- **Enhanced Safety:** Standard safety improves with real-time alerts sent from sensors that help detect hazards such as gas leaks, equipment failures, or unauthorized access.
- **Enhanced Monitoring:** The observation of processes and environments through IoT devices equipped with specialized sensors allows for real-time tracking and the completion of routine tasks without human intervention, thereby supporting predictive maintenance.
- **Time Savings:** By processing data in real time and reducing the human workload, automating operations and instant data processing streamline workflows without delays.
- **Cost Reduction:** By employing intelligent system management, operational expenses are gradually mitigated through the use of predictive analytics combined with optimized resource allocation.
- **Scalability:** Adaptive IoT networks can expand to meet changing demands by adding more devices without requiring extensive infrastructure overhauls.
- **Accessibility:** Systems and data are accessible remotely, making them available through PC's and smartphones 24/7.
- **Data Driven Insights:** Thanks to IoT devices that collect vital information, informed decisions through performance monitoring and analytics are now achievable.

#### 1.1.4 Data Handling in IoT Devices

The effectiveness and reliability of IoT systems are closely linked to how information is managed throughout their lifecycle [15, 16, 17]. User trust and system integrity are upheld when every step, from information generation to its usage, is handled effectively.

- **Data Collection:** With the help of integrated sensors, IoT devices are capable of continuously collecting data such as temperature, pressure, humidity, and motion. This raw data is digitized and sent to the processing unit, where it is further processed.
- **Data Storage:** The collected data is either stored in the cloud or kept locally on the device. The application's requirement for real-time accessibility, backup needs, and data volume typically determine which option to use.
- **Data Processing:** Algorithms are defined to interpret the received raw data, enabling its usability. Occasionally, this information must be filtered, sorted, or analyzed to recognize trends, detect errors, identify urgent events, or initiate specific automatic actions within the system.
- **Data Security:** There are strong encryption techniques as well as secure communication protocols that protect users from unauthorized access and tampering. Only trusted users and devices can access or send sensitive information, and cryptographic measures are implemented to ensure the integrity of these users or devices.
- **Data Privacy:** The IoT impacts numerous areas in our daily lives. Because of the data's sensitive nature that these devices manage, privacy compliance procedures must be strictly followed. Established policies should detail the processes for data collection, access, retention duration, and sharing thresholds.

Proper and secure data management guarantees the seamless functioning of IoT systems, preserves user confidence, and adheres to legal and industry regulations. Accessible and manageable data supports the sustainability of IoT solutions while improving prevention and control systems.

## 1.2 Concerns in IoT Devices

IoT devices offer certain benefits when integrated into real-world use cases, but they also create some technical challenges. These challenges may stem from heterogeneity of devices, restricted system resources, exposure over unsecured networks, and the requirement for immediate feedback from the system. Other persistent concerns include data security, system elasticity, data processing efficiency, and cloud computing systems [18].

### 1.2.1 Data Security

The wide adoption of IoT devices allows easy access to systems, especially using open or pseudonymous networks of the internet. This nature of IoT environments makes them prone to several external attacks. Applying protective measures for the integrity, authenticity, and confidentiality of information is significant for the functioning of any IoT environment. To enhance the reliability of data transmission between smart devices, researchers are focusing on five key components, as depicted in Figure 1.3.

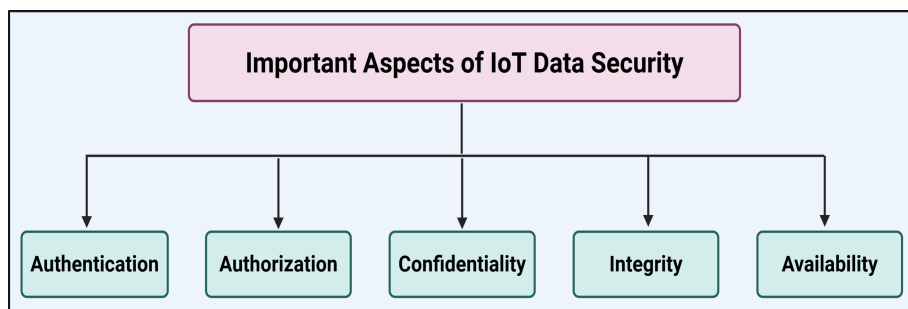


Figure 1.3: Important Aspects of Data Security in IoT Systems

- **Authentication:** Authentication safeguards the network through verifying the user and device's identity. It blocks rogue devices from establishing interactions or manipulating the system functions.
- **Authorization:** After authentication, authorization stipulates which services or resources the user or device may interact with. This mechanism further helps to safeguard restricted zones prone to system breaches.
- **Confidentiality:** This principle ensures that the relevant data exchanged between connected devices cannot be accessed by unauthorized entities. The information is kept safe by applying appropriate encryption mechanisms both during and after the transmission.
- **Integrity:** Data integrity ensures that information transmitted between two parties remains unchanged in the process of transmission. To ensure accuracy, data integrity employs techniques such as hashing which is a way to secure data from alteration or breach.
- **Availability:** Availability focuses on an organization's network services and device function upkeep in relation to their operational readiness for users

within the permissive scope. Furthermore, it encompasses safety from service stoppages, denial-of-service incursions, or network overload.

### 1.2.2 Scalability

Scalability can be defined as the ability of connected devices and data volume to increase without compromising the system's performance and reliability. Poorly engineered systems often fail during high traffic and extended deployments [19].

- **Network Bandwidth:** The increase in the number of connected IoT devices results in a greater total amount of data being transmitted, which can lead to congestion. The system must ensure a minimum bandwidth threshold sufficient to avoid traffic delays or breakdowns in communication.
- **Storage Capacity:** The data from IoT networks tends to be large in volume and, therefore, requires highly efficient methods of storage. IoT networks need scalable storage, such as cloud-based or distributed storage, to manage an uninterrupted flow of data.
- **Processing Power:** The efficiency of real-time data processing heavily relies on the computing resources at hand. IoT systems require strong computing capabilities, and if the resources on the onboard device are inadequate, support from edge or cloud computing becomes necessary.

### 1.2.3 Data Processing and Handling

Timely responses to shifting IoT operational contexts require data from IoT devices to be processed with precision and accuracy. Inaccurate data processing can lead to delays, wasted resources, inefficient processes, and even incorrect outcomes results.

- **Real-time Decision Making:** Instantaneous action and data analysis are essential for real-time healthcare IoT solutions, automated industrial processes, and environmental systems controls. Decreased responsiveness could result in diminished system reliability.
- **Energy Optimization:** Usage pattern analysis and operationalization can allow the system to turn off energy-intensive components that are currently

inactive. This enhances energy efficiency and promotes sustainable operations.

- **Anomaly Detection:** Monitoring device data stream flow in real time creates an opportunity to identify hardware malfunctions, unauthorized intrusions, out-of-bounds sensor activity, or rogue sensors in the early stages, facilitating proactive response management. Prompt corrective measures can be implemented once anomalies are detected.
- **Personalized Services:** Analyzing historical user-device interactions enables the delivery of personalized services tailored to individual user preferences and expectations, while core IoT systems adapt to users' behaviors and habits.

#### 1.2.4 Importance of Cloud Computing in IoT Systems

Cloud computing serves as the critical backbone for IoT systems by providing infrastructure that scales the resources of data storage, processing, and management of devices. Its support is pivotal for enhancing seamless operational efficiency.

- **Remote Access and Control:** Users and operators can interface with IoT devices through cloud systems from any geographic location. This access enhances the usability of automation in IoT devices and facilitates remote system intervention for proactive measures regarding timely system failures [20].
- **Advanced Data Analytics Capabilities:** The collected data is processed in the cloud and analyzed systematically using sophisticated algorithms to extract trends, evaluate performance, and execute models for surveillance and system diagnostics forecasting.
- **Device Maintenance and Update:** Updating firmware and software can be done centrally through cloud platforms, reducing the need for on-site maintenance where devices are checked and enhancing the servicing of device updates in the security technologies sector.
- **Security Services:** Cloud infrastructures have integrated security tools such as access controls to system resources, data encryption for information stored in the cloud, and activity monitoring. These measures help protect the systems from external attacks and misuse from internal manipulations.

### 1.2.5 Attacks and Security Issues in IoTs

An IoT network includes billions of interconnected devices, known as nodes, that exchange crucial information. Each node must have a unique identifier to ensure accurate data transfer. Typically, these devices are connected, allocated, managed, and authenticated by a single cloud platform. As data moves through various points in the network, it encounters several challenges, particularly regarding security and privacy. These challenges are generally categorized into Operational issues and Architectural issues [21].

The security and privacy challenges that IoT systems face are illustrated in Figure 1.4 as existing problems that encompass both operational and architectural categories. Specific operational issues focus on data privacy, threat mitigation, and adherence to legal and regulatory boundaries. Architectural issues involve cloud security, network security, and device security.

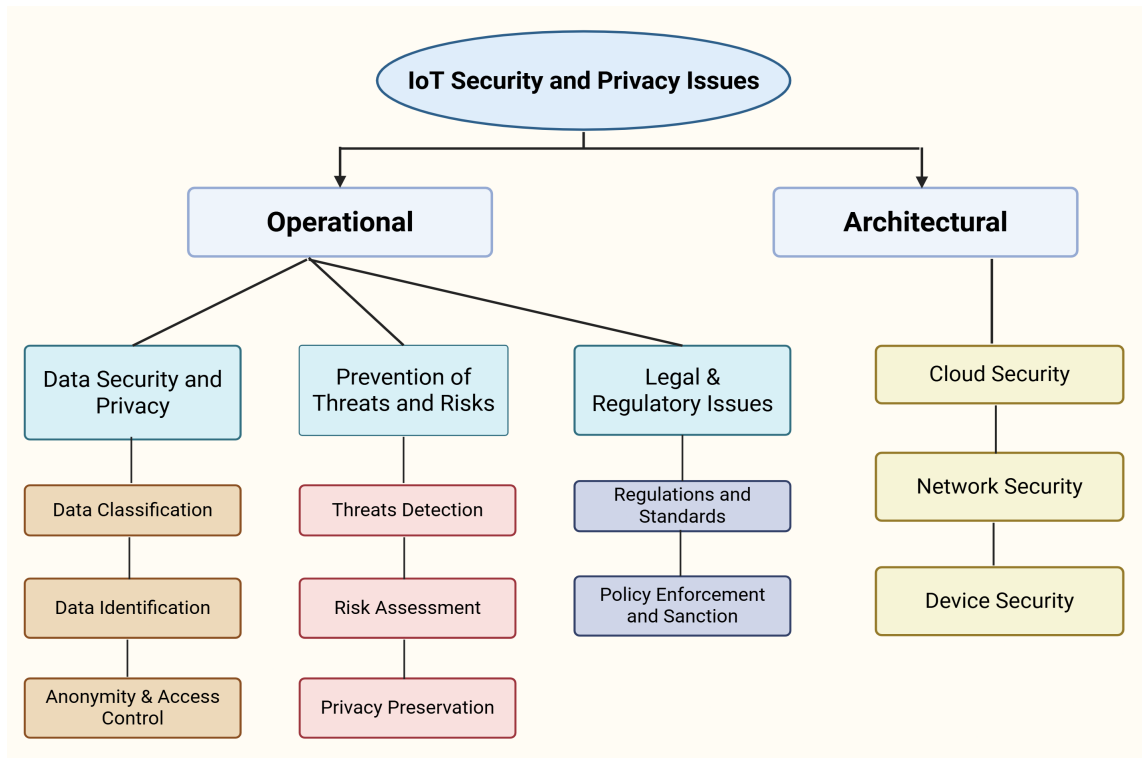


Figure 1.4: Various Security and Privacy Issues in the IoT Architecture

Data privacy becomes critical when dealing with sensitive information such as financial records, confidential data, or authenticated information. Theft of device IDs can lead to breaches of user confidential data and compromise system security. User privacy is also threatened by violations of policies and standards.

Limited control over data, the risk of data theft, and cloud security issues all intersect. Network security faces similar threats from technologies that endanger data integrity. Data security deteriorates when accessed through endpoints like smartphones, tablets, and laptops. Moreover, IoT systems integrated with blockchain technology may be vulnerable to different types of attacks. These attack types are discussed below:

- **Malware Attacks:** Malware attacks pose one of the greatest risks in IoT systems that incorporate blockchain technologies. Such attacks involve gaining unauthorized access to a user's system through malware. They include numerous and various harmful programs such as viruses, ransomwares, spyware, or command-driven parasites that, at the very least, undermine the functionality of the device or compromise its data security.
- **Denial of Service (DoS) Attacks:** These attacks jeopardize the continuous function of an IoT network by sending large volumes of traffic to cause malfunctions. Because the service is disabled, users cannot access the network or retrieve information, leading to lag or interference [22].
- **Phishing Attacks:** Phishing attacks aim to extract sensitive information from users by masquerading as trusted sources. This fraudulent communication seeks to remove the veil of secrecy to capture personally identifiable information, such as social security numbers and financial details.
- **SQL Injection Cyber Attacks:** These types of attacks are typically referred to as SQL injection, whereby an attacker gains unauthorized access by embedding hostile SQL instructions into a database. This method makes it easy to obtain sensitive data stored in databases through skimming, thus simplifying the execution of SQL codes.
- **Password Attacks:** Attempts to access accounts protected by passwords are called password attacks. These attacks are often linked to malware that collects login credentials and leads to the leakage of sensitive information.

To combat and mitigate such threats, the implementation of IoT systems now focuses on integrating with blockchain, which provides a distributed and secure method for protecting the integrity of data and systems.

## 1.3 Machine Learning

Machine learning techniques are being used in optimization fields like healthcare, finance, logistics, and supply chain management. This area of research in computer science typically involves a two-phase process: training and testing. During training, the model is built using known or historical data, enabling it to identify patterns [23, 24]. The testing stage then uses new or unseen data to assess the model's performance and predictive accuracy. This two-step approach is essential for validating the model's effectiveness in real-world applications. The first step focuses on extracting insights from the input data features, whereas the second exposes the model to unknown outcomes, applying the understanding gained previously. These steps are commonly termed learning and prediction. The aim of machine learning is to create models which accurately forecast future events based on historical data [25, 26].

Data clustering can be performed using different approaches, such as supervised, semi-supervised, and unsupervised techniques [27]. It is widely accepted that machine learning algorithms fall into the two categories of 'supervised' and 'unsupervised'. Some also recognize reinforcement learning as an additional category, involving learning patterns through interaction with environments [28]. However, most studies primarily focus on the broadly defined dichotomy for supervised and unsupervised methods. The key distinction that sets the two apart is the presence of labeled data during the training phase: supervised learning uses labeled data inputs, while unsupervised learning does not utilize them [29].

- **Supervised Learning:** In supervised learning, the model is trained using labeled data, also referred to as input data [30]. The aim of this learning technique is to allow the model to understand the relationships between the provided features and the labeled outcomes. A model is then developed to predict new data based on prior training sessions and is shown in 1.5.

Practitioners utilize supervised learning for classification tasks and regression problems. During classification, the model sorts the data into distinct classes. For regression, the model forecasts a continuous variable based on several independent variables. To ensure effective supervised learning, the training dataset should contain clear and well-defined classes that guide the model throughout the learning process.

Supervised learning has recently received attention in the development of intelligent systems [31, 32, 33]. Researchers have employed these techniques

to improve smart environments, and in some instances, they have integrated supervised learning into blockchain frameworks to guarantee secure communication and system reliability [34].

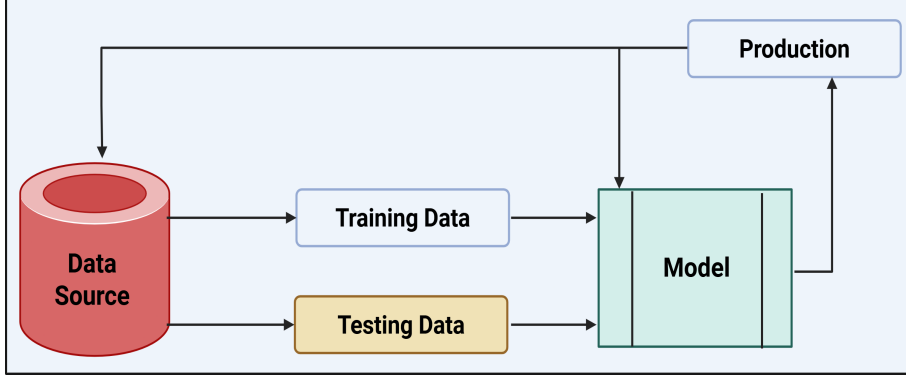


Figure 1.5: Supervised Learning

- Semi-Supervised Learning:** The development of semi-supervised learning techniques has emerged in the context of abundant datasets accompanied by a scarcity of labeled data, which is costly to annotate [35, 36]. In such situations, supervised learning approaches struggle due to their reliance on labeled examples. Although unsupervised learning models do not use labeled datasets, their outputs may be precise but lack reliability. Researchers often focus on one end of the spectrum, either supervised or unsupervised learning; however, other techniques have been developed to tackle classification and prediction challenges. Frequently, researchers employ comparative methods to evaluate the effectiveness of different models. It is common to find SVMs utilized as cross-validation tools. Some studies integrate elements from both supervised and unsupervised paradigms with reinforcement-based models like self-training techniques or modified SVMs [37, 38]. Artificial neural networks and support vector machines remain the most widely used models for generating reliable results in the realm of machine learning, particularly for classification.
- Unsupervised Learning:** In unsupervised learning, the absence of known target outputs means that any errors generated during training cannot be used to adjust the network's behavior [39, 40]. There is no reference data available to evaluate how accurate or effective the outputs are. Instead, the learning process relies entirely on the input values, and the system identifies patterns based solely on this data. As illustrated in Figure 1.6, the model

receives no feedback and therefore uses its internal mechanisms to recognize input-output relationships. This approach establishes a connection between inputs and outputs by discovering patterns independently.

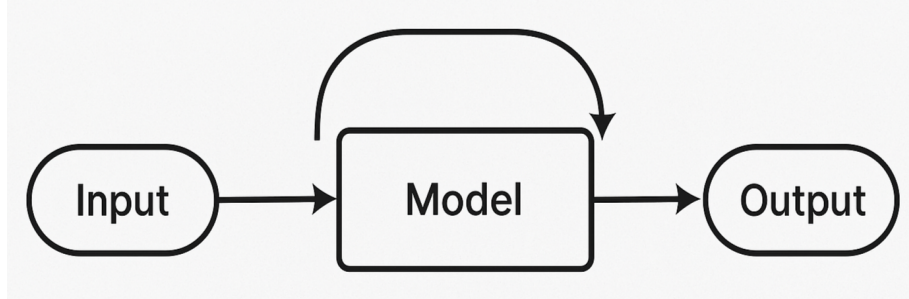


Figure 1.6: Un-Supervised Learning

### 1.3.1 RNN

RNNs are a subtype of neural network architectures designed for sequential data. Unlike classical feedforward networks, RNNs can recall information from prior inputs through an internal memory system, enabling them to capture temporal dependencies [41]. As a result, RNNs are valuable in areas such as natural language processing, speech recognition, and forecasting, where context and order are essential. Figure 1.7 depicts the working of a RNN. In RNNs, the current

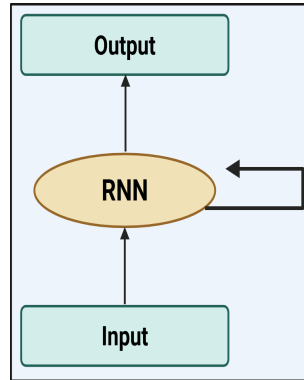


Figure 1.7: Recurrent Neural Network

output is not only dependent on the current input but also on the hidden state from the previous time step. The mathematical formulation is given as:

$$h_t = f(h_{(t-1)}, x_t) \quad (1.3.1)$$

$h_t$ = Current state

$h_{(t-1)}$ = Previous state

$x_t$ = input state

The formula for applying the Activation function( $\tanh$ ):

$$h_t = \tanh(W_h h_{(t-1)} + W_x x_t) \quad (1.3.2)$$

$W_h$ =Weight at the recurrent neuron

$W_x$ =Weight at input neuron

$\tanh$ =hyperbolic tangent function

The formula for calculating the output:

$$Y_t = W_{hy} h_t \quad (1.3.3)$$

$Y_t$ = output

$W_{hy}$ =weight at the output layer

#### 1.3.1.1 Merits of RNN

- RNNs are capable of handling both time-series data and other datasets with ordered dependencies.
- They can remember concepts that help retrieve patterns from context.
- Suitable for text generation, language modeling, and sequence-level classification.

#### 1.3.1.2 Limitations of RNN

- RNNs face challenges with long sequences because of the vanishing or exploding gradient problem.
- The processing order introduces a possibility of extending the period needed for training.
- Models like this often forget information, so they require enhancements such as LSTM or GRU to improve functionality.

### 1.3.2 Deep Neural Network (DNN)

A DNN is a form of artificial neural network which includes several hidden layers positioned between the input and output layers. It is capable of capturing and representing complex, non-linear patterns within large datasets [42, 43]. DNNs consist of interlinked nodes (neurons) that process information at each layer and output the processed information to the subsequent layer. A pictorial representation of a DNN is shown in Figure 1.8. Each neuron in a DNN applies a linear

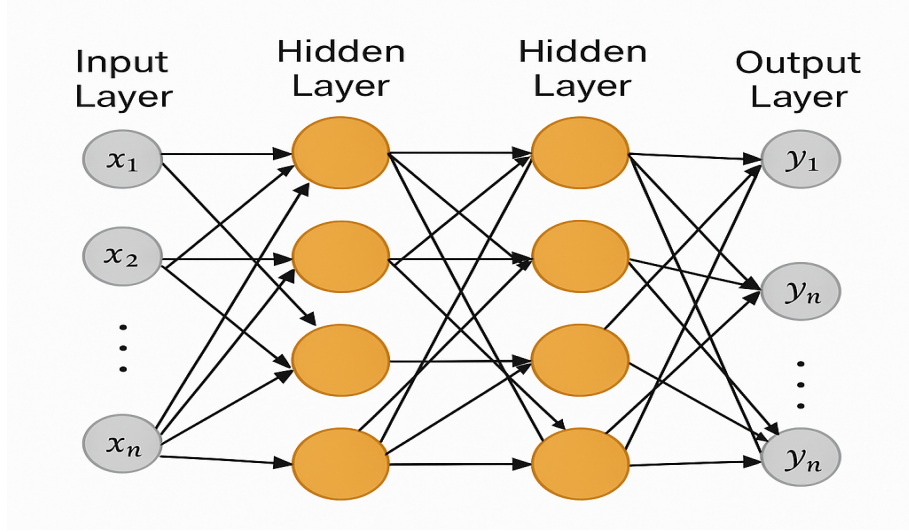


Figure 1.8: Deep Neural Network

transformation followed by a non-linear activation function. The basic operation can be expressed as:

$$a^l = f(W^l a^{l-1} + b^l) \quad (1.3.4)$$

where:

$a^l$  is the activation function in layer  $l$ ,

$W^l$  and  $b^l$  are the weights and biases at layer  $l$ ,

$f$  is a non-linear activation function such as ReLU, sigmoid, or tanh.

DNNs use backpropagation for learning, where the error is propagated backwards from the output layer to adjust the weights in each layer.

#### 1.3.2.1 Merits of DNN

- DNNs can learn and represent intricate features with a high degree of abstraction.

- They are good at performing tasks such as image identification, speech processing, and predictive analytics.
- They can approximate any function or pattern with sufficient data and layers.

### 1.3.2.2 Limitations of DNN

- To train effectively, DNNs require a substantial amount of labeled data along with significant computational resources.
- They are often labeled as 'black-box' models, which makes interpreting the results nearly impossible.
- Without applying appropriate regularization techniques, models are susceptible to overfitting.

## 1.4 Blockchain Technology

The term “blockchain” gained popularity when Satoshi Nakamoto’s work titled “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008 got published [44]. In this paper, he explores the double spending problem inherent in digital currencies without a centralized system. Although blockchain wasn’t the primary invention in the essay, it is the foundational technology that enabled the creation of Bitcoin. In recent years, blockchain has evolved into a standalone technology, attracting attention from various fields.

Initially, blockchain was designed as a decentralized public record of transactions aimed at facilitating Bitcoin transfers. It ensured that transactions were maintained in transparent and secure records without the need for a trust-issuing authority, thereby enabling trustless systems. This approach streamlined processes and removed the necessity for external verification.

In modern times, states, industries, and various organizations are implementing blockchain technology as it provides solutions to the challenges posed by outdated systems. It offers numerous advantages, including enhanced security, immutability, traceability, and transparency [45, 46].

A blockchain serves as a system for recording transactions, auditing, and maintenance, stored on a distributed ledger shared among all participants. It contains blocks of securely linked transactions along with their records. When the network

is created, each participant node receives the entire set of previous blocks, and adding a newly formed block to the set ensures that its information cannot be altered [47].

Figure 1.9 illustrates the structure and operation of blockchain technology. Blockchains can be described as a sequence of records, with each record encapsulated within a block. Each block in a blockchain includes an index and timestamp, as well as a hash, previous block's hash, and additional data. The genesis block represents the first block in the chain, which does not refer to any preceding block since it signifies the starting point of the chain.

An individual block can be seen as a standalone spreadsheet, while the entire sequence of linked blocks constitutes the blockchain. To keep track of activities and resource utilization of the network nodes, index values are captured and monitored on the cloud server. In blockchain systems, timestamps create unique hash values for each block, thus ensuring security and data traceability within those blocks [48, 49]. The addition of each new block in the chain requires the last added block's hash to be incorporated, securely linking the blocks together. The principles of hashing help resolve complex computations while generating additional hash values, which protect the blockchain system and maintain its security.

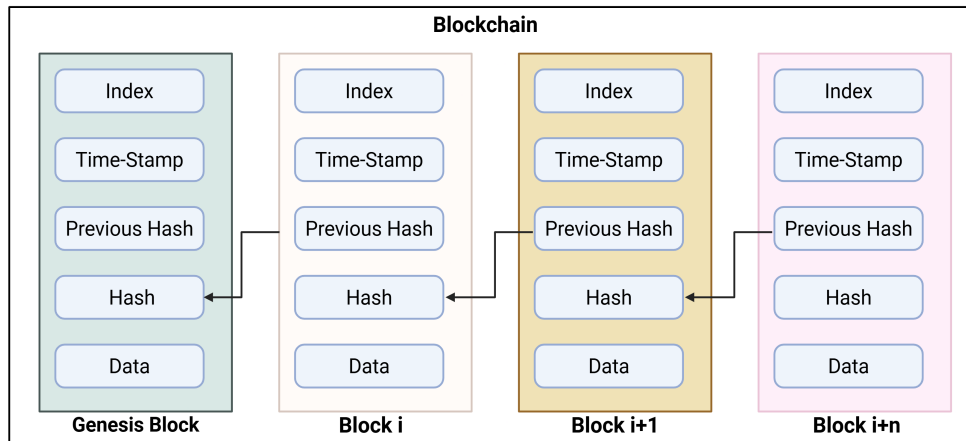


Figure 1.9: Basic Blockchain Working and Structure

### 1.4.1 Blockchain Components

Many applications extensively utilize Blockchain technology to address security issues and challenges. Figure 1.10 illustrates the components involved in blockchain

technology [50].

**Block:** In the blockchain framework, a block acts like an individual spreadsheet

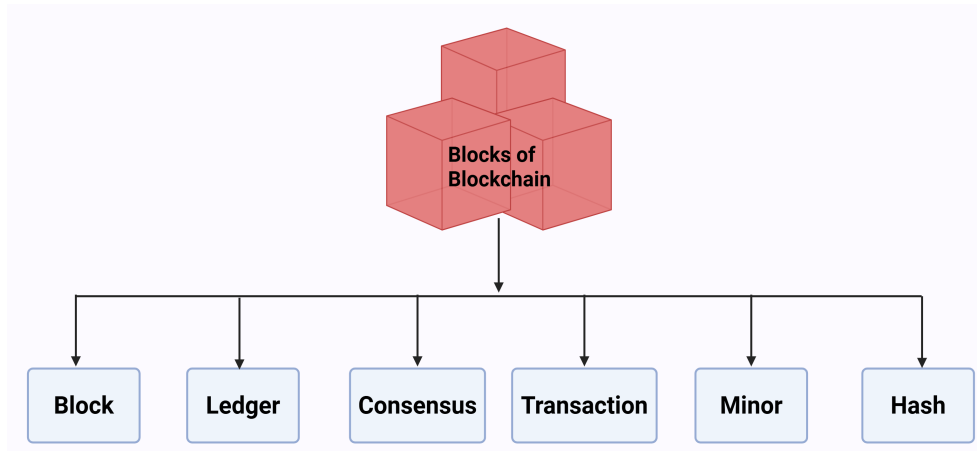


Figure 1.10: Components of Blockchain

that contains transaction data. Multiple blocks are linked together to create a blockchain. Each block is recognised by a unique hash value, connecting it to the next block in the chain while preserving the security and integrity of the data.

**Ledger:** The blockchain comprises various ledgers that contain all transaction information within the network. Unlike conventional databases, which aim to organize information in rows and columns, the blockchain ledger captures details about every transaction arranged within its respective block. Due to the system's decentralized architecture, every individual node maintains a copy of this ledger, establishing a transparent and indisputable record-keeping system.

**Consensus Mechanisms:** Within a blockchain, a consensus mechanism is used to enhance trust and security across the network. This mechanism is responsible for incorporating transactions that are endorsed and reach agreement to be added to the blockchain. It enables designated participants to verify transactions in a trustworthy manner, which strengthens security in a system that relies on central control systems.

**Transaction:** A transaction is known as a series of operations performed in a blockchain network. Each block contains transactions. When a user performs a transaction, a new block is added to cater for that transaction. The block is sent to all users within the network and every user checks the structure and compliance details of the transaction. After all nodes have confirmed the transaction, the nodes that participated in the transaction will be compensated using consensus mechanism. Following approval a block is formed and incorporated into the

existing chain. The new record is distributed to all participants. In this way the transaction is done in a decentralized way and the security is guaranteed.

**Miner:** In blockchain technology, a miner is a computer or system that solves complex equations to create new blocks. After network nodes generate transactions, miners compile them into blocks. Successfully solving these equations enables the addition of the block to the blockchain, thereby sustaining the ongoing chain of transaction processes.

**Hash Function:** In blockchain, the hash function is designed to verify the integrity of data within each block. Consistent with its internal processes, it assigns a unique identifier (hash) to each block based on its contents. This mechanism for generating hashes ensures data integrity, as it is virtually impossible to produce the same hash from two different data sets. Furthermore, assigning a unique hash to every block prevents duplication and collisions in the network.

### 1.4.2 Characteristics of Blockchain

Blockchain technology is frequently utilized across various fields due to its robust and dependable features [51, 52]. Figure 1.11 illustrates the factors that make blockchain suitable for numerous modern applications

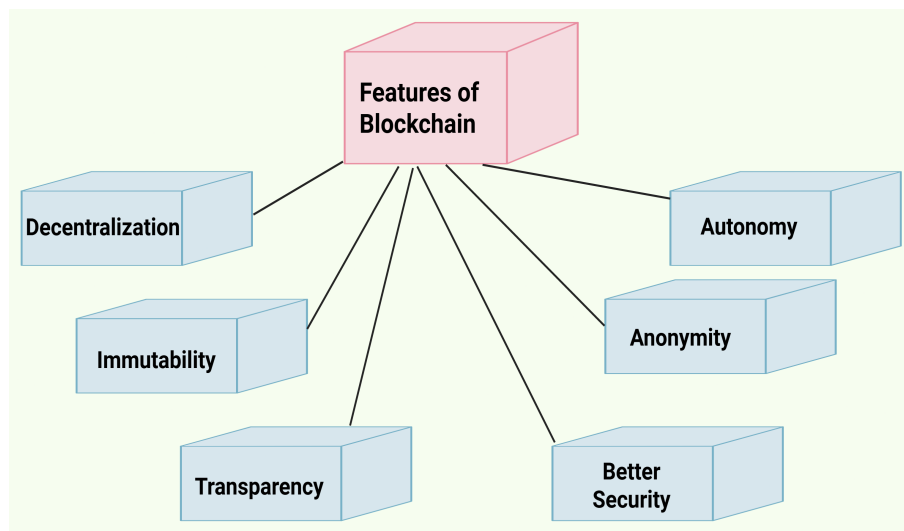


Figure 1.11: Characteristics of Blockchain Technology

- **Decentralization:** A blockchain consists of a peer-to-peer network or distributed system, allowing different nodes to communicate directly with one

another without an intermediary central server. This decentralized structure protects the system from the risks of a single point of failure and helps reduce potential delays within the network.

- **Transparency:** All nodes within a blockchain network have equal access to all transaction details. Unlike centralized systems, where data is often monopolistically controlled by a single entity, blockchain operates without relying on a third party for intermediary services, as no single entity governs the system.
- **Immutability:** Blockchain preserves data integrity through an immutable ledger or distributed ledger technology (DLT). Once a block is added to the chain, it cannot be altered or deleted. Each block is linked to the previous one using a hash, ensuring that the entire transaction history remains concrete and protected from tampering.
- **Enhanced Security:** One of the primary advantages of blockchain is its enhanced security. The consensus mechanisms employed allow the addition of new links to the chain only for completed transactions. This process bolsters user trust in the network while exposing the blockchain to numerous threats.
- **Anonymity:** A user's personal information is protected on the blockchain because users are assigned unique digital identities instead of their real names. While still allowing secure access to the network, this feature ensures privacy and safeguards sensitive information. In applications where confidentiality is critical, such as secure voting systems and financial transactions, this feature is particularly advantageous.
- **Autonomy:** Decisions derived from smart contracts or predefined rules can be made autonomously by the nodes or devices within a blockchain network. This degree of autonomy enables tasks to be executed automatically without requiring constant human intervention, thereby enhancing the reliability and efficiency of the system.

### 1.4.3 Types of Blockchain

This technology was introduced to the world as the concept of open blockchain for the first time. Although the developer's goals remain unclear, the emergence of

decentralized directing technology has impacted communities by enabling them to operate independently of any specific authority. Distributed technologies not only provide solutions to many problems associated with blockchain technology but also address the drawbacks of centralized approaches [53]. Consequently, several issues arise in the first-generation blockchain, particularly its inefficiency and lack of scalability. While a public blockchain is designed to serve everyone's needs, it may not be the optimal choice for all businesses. As technology progressed, various blockchain strategies were developed, such as public, private, consortium, and hybrid blockchains. Figure 1.12 lists the four main types of blockchain networks. These different forms of blockchain have been the primary driving forces behind the advancement of blockchain technology [54].

- **Public Blockchain:** The first form of blockchain technology is the public blockchain. This type of chain allows anyone to join the network via the internet. Both transactions and the processes of verifying and validating blocks can be performed by any user. Every participant can view and access each completed transaction, ensuring the ledger is fully transparent.
- **Private Blockchain:** In a private blockchain, only participants with special permission and access can view, validate, or record transactions. To some extent, the transaction process remains public, but control over who can add or verify transactions is restricted. Primarily used within companies, this variant of blockchain is best suited for entities that require privacy and strict access limitations.
- **Consortium Blockchain:** A consortium blockchain is a partially decentralised system managed collectively by a group of organisations or institutions. Unlike public blockchains, only a few selected nodes are allowed to validate transactions. It is widely adopted in banking, supply chain management, and various other industries, as multiple trusted participants require a secure way to interact.
- **Hybrid Blockchain:** This is the combination of both public and private blockchains. The blockchain is accessible to all participants, while others remain private and are accessible only to select users. This model strikes a balance between transparency and control, making it ideal for use cases that require both data privacy and public access simultaneously.

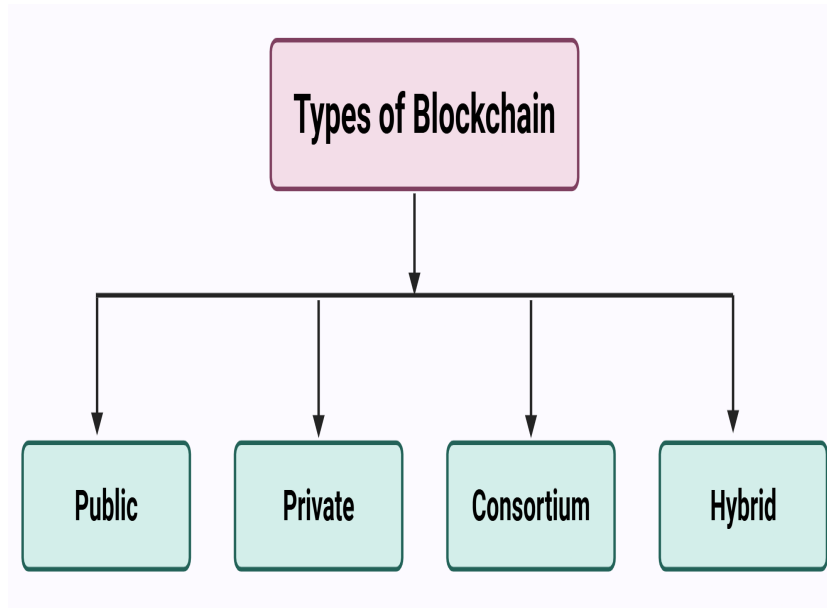


Figure 1.12: Types of Blockchain Technology

A higher level of classification can be made for the types of blockchains based on their access control or permission levels. Public blockchains, often referred to as permissionless blockchains, operate in a trustless environment. In contrast, private (permissioned) blockchains are closed internal systems. Public blockchains are completely open networks where all users can join and participate in the consensus processes used to validate transactions and data. Permissionless blockchains are entirely decentralised and maintained by anonymous users. Key aspects of permissionless blockchains include unrestricted access to information, open-source development, user confidentiality, a lack of control by a central authority, and the presence of incentives in the form of tokens or digital assets. On the other hand, permissioned chains or private blockchains are quite different. Permissioned blockchains operate as closed networks, which means they restrict access to predefined and select members or consortia who are allowed to take part in the consensus. Private permissioned blockchains are partially decentralized systems, as access is limited strictly to known and authenticated participants. They are maintained by recognized and authorized individuals. Permissioned blockchains have clearly defined transparent policies that cater to the needs of the participating organizations. Such systems are created by private information bodies within the group and lack anonymity. Often, a central authority manages the network and trusts users to whom they grant access. Table 1.1 illustrates the distinguishing features between a permissionless blockchain and a permissioned

blockchain.

Table 1.1: Comparison of permissionless and permissioned blockchain

|                      | <b>Permissionless</b>                                                            | <b>Permissioned</b>                                                                                |
|----------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Overview</b>      | Available to all participants, full decentralized                                | Designated participation, partially decentralized                                                  |
| <b>Attributes</b>    | Fully Transparent, Open Source, No Central Authority, Anonymous, Incentive-based | Level-based Transparency, Private, Non-Anonymous, Privacy Protected, Authority, Optional Incentive |
| <b>Advantages</b>    | Decentralized, Transparent, censorship-resistant, resilient security             | Partially Decentralized, Privacy Protected, Customizable, Scalable                                 |
| <b>Disadvantages</b> | Non-energy efficient, Slow scalability and no data privacy                       | Limited network and energy consumption, Scalable, authority-based Access                           |
| <b>Applications</b>  | P2P, B2C                                                                         | B2B, C2C                                                                                           |

#### 1.4.4 Blockchain Technology With Multi-Layered Architecture

Blockchain technology enables tamper-proof digital ledgers that enhance the secure creation and distribution of information. Each new data entry in the ledger is referred to as “blocks”. Block creation undergoes validation on all nodes across network within blockchain. Validation is performed by at least one of the initial five nodes, after which the information is finalised as a block. Every block comprises the new data along with the hash of the preceding block. The blocks are connected using the hash values, forming a chain that provides permanent storage for the data [55]. The blockchain network updates the ledgers, which includes the blocks created during that duration. Blockchain technology is usually structured into three main logical layers: Application Layer, the Blockchain Layer, and the Data Layer [56] as depicted in Figure 1.13.

- **Application Layer:** This layer acts as an interface between the user and the blockchain system. This layer encompasses protocol overlays, APIs, and user-facing platforms. It is ideally suited for creating and operating decentralised applications (dApps).
- **Blockchain Layer:** The blockchain layer ensures the security of information within the data layer. It undertakes critical activities such as fraud

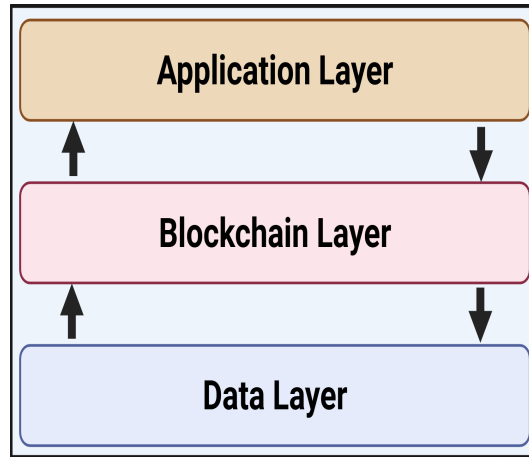


Figure 1.13: Layered Architecture of Blockchain Technology

detection, monitoring data provenance, and managing P2P transactions. These processes guarantee that the application layer receives data that can be trusted, authenticated, confirmed, easily validated, and available in multiple copies. Therefore, this layer is pivotal in establishing trust and reliability within the blockchain system.

- **Data Layer:** The data layer maintains blockchain records, securely storing them and linking blocks through cryptographic hashes to ensure immutability and transparency across the entire network.

#### 1.4.5 Consensus Mechanism in Blockchain Technology

Blockchain is a distributed ledger system that facilitates the exchange of transaction value while ensuring privacy and security in a decentralised environment. Each blockchain network has consensus mechanisms that are integral components of the system. Due to blockchain's security, stability, immutability, and decentralisation, it is relied upon by many digital currencies. Its ability to enable trustless, peer-to-peer transactions has attracted scholarly interest, particularly in the domain of smart home data protection [57].

In decentralised blockchain networks, consensus mechanisms ensure system integrity and security. User trust is established through these methods by enabling all nodes in the network to reach a unified agreement regarding the state of the distributed ledger. Even if participants are total strangers and have no prior trust established, these methods promote collaboration and reinforce trust. The consensus process guarantees that each new block added is validated and accepted by all

nodes, confirming agreement on a singular truth. In a blockchain network, every node must be aligned and reach an agreement on the authenticity of transactions before they are integrated into the ledger. No blockchain system can function efficiently without consensus mechanisms. These mechanisms help ensure that all participants remain updated with the common version of the blockchain and that transaction validations occur in a timely manner; thus improving confidence and trust in the system [58].

#### 1.4.5.1 Distributed Consensus Mechanism Characteristics

Distributed Consensus is described as a technique employed in the context of distributed systems to achieve agreement among multiple nodes within a network. It ensures that all participating nodes reach a common understanding of the situation, and even in the presence of some node failures or differing messages, consensus can still be attained [59, 60, 61]. The key features of a distributed consensus mechanism include the following:

- **Decentralisation:** In a distributed consensus system, operations are carried out using fully decentralised technology, meaning there is no singular focal point with an existential monopolistic privilege, as all nodes possess the same rights and responsibilities.
- **Fault Tolerance:** The mechanism must continue to function in scenarios where some nodes are experiencing network failures, transmitting information poorly, or are completely unresponsive. It will persist in its operation despite the presence of such nodes.
- **Agreement:** Concentrating on conflict resolution enables the successful attainment of the central objective of distributed consensus, whereby all nodes reach the same agreement. Each node presents diverse information, and it is crucial to resolve any disputes that may emerge.
- **Scalability:** Achieving agreement within a single unit of time consistently assures efficient performance, even as the network expands, making it an essential quality of a reliable consensus mechanism that operates in conjunction with a growing number of nodes.
- **Security:** Each mechanism in place ensures that the consensus process is trustworthy and proves to be unforgeable. A harmful or malicious actor will

not be able to disrupt the process flow by granting access to sensitive data or dismantling system components.

#### 1.4.5.2 Models in Consensus Mechanism

Different forms of distributed consensus mechanisms exist, namely Byzantine Fault Tolerance (BFT), pBFT, and the PoW algorithm, commonly used in cryptocurrencies like Bitcoin. The emergence of diverse blockchain protocols has given rise to several consensus models tailored to meet particular needs and challenges in distributed systems [62, 63, 64, 65]:

- **PoW:** PoW is used in blockchain networks as a consensus method where a specific group of individuals, known as miners, validate transactions and add new blocks by solving complex mathematical problems. This process is highly resource-intensive, which helps to enforce security since attackers would need to expend considerable resources to manipulate the system.
- **PBFT:** It is a voting-based consensus algorithm designed for decentralised systems with high consistency requirements and low complexity. Its main steps include: request, pre-preparation, preparation, commitment, and reply. Upon receiving a request from a client, the message is disseminated to a series of nodes. Each node processes the message, and even if one fails, the others will continue until consensus is reached. When sufficient nodes agree, an  $n + 1$  response is issued, where  $n$  represents the faulty nodes. PBFT achieves a reliable and stable consistently shared state across the network, proving useful in scenarios where systems prioritise consistency.
- **Paxos:** Paxos is a highly fault-tolerant algorithm designed to achieve consensus in distributed systems, even when some nodes may fail or when messages are delayed. It ensures consistency by enabling a set of nodes to agree on a proposed value after undergoing processes of proposal delivery and acceptance responses. Paxos guarantees that any decision made is immutable. The algorithm achieves robust agreement in a distributed system with faulty nodes or delayed messages and serves as a consensus mechanism. Consistency is maintained by forming groups of nodes that must reach consensus on a given value through majority voting during value proposition and acceptance. The accepted value remains immutable forever once it is established. In real implementations, Paxos sacrifices speed due to the need

for extensive communication, which results in high latency and decreased effectiveness in large systems.

- **Raft:** Raft is an algorithm designed to create fault tolerance in a distributed system that replicates logs in an orderly fashion. It functions by selecting a primary node that interacts with clients, while follower nodes continue to replicate log entries in a fully ordered manner. In contrast to Paxos, Raft streamlines the process of reaching consensus, enabling easier implementation and conceptual understanding. An important downside, however, is that the consensus mechanism relies heavily on a single leader; when the primary node crashes, the downtime during the primary election limits availability.

### 1.4.6 Attacks in Blockchain

Blockchain attacks are malicious activities that exploit vulnerabilities in blockchain systems to disrupt operations, gain unauthorized access, or manipulate data or transactions. Despite its decentralized and secure design, blockchain is still susceptible to certain types of attacks. Below are some common types:

**51% Attack:** An individual miner or a coalition of miners controlling more than 50% of the computational power in a blockchain network can execute this type of attack. This enables them to manipulate the blockchain by reversing transactions, which facilitates double spending, or by halting the validation of new transactions. Such actions undermine the trust and integrity associated with the blockchain system.

**Sybil Attack:** In Sybil attacks, network participants can easily be misled by attackers who create multiple fictitious personas as nodes of the network, allowing them to gain disproportionate control over these nodes. These bogus nodes weaken the voting and consensus mechanisms and obstruct honest transactions, thus promoting centralization and undermining the standards of blockchain systems.

## 1.5 Cryptography

Cryptography is a method for protecting information and preventing its leakage. This practice traces back to the earliest written words and was initially utilized by military leaders, spies, and intelligence personnel. Today, cryptography plays

a crucial role in ensuring data integrity, recognizing individuals, and enabling the use of digital signatures. It serves as a significant safeguard for data and processes in our modern era of advanced computing [66].

### 1.5.1 Modern Cryptography

Cryptography as a formal discipline began to gain traction only after the mid-1970s. Today, modern cryptology encompasses multiple fields, drawing equally from mathematics, computer science, and advances in Quantum Physics (Hoffstein et al., 2014). A key principle behind most contemporary cryptographic methods is the challenge of solving complex mathematical problems, based on the premise that current computing capabilities are insufficient for easily tackling these issues. However, it is impossible to guarantee complete security, as brute force attacks, which involve systematically testing every possible option, present a constant threat.

Some encryption systems remain secure as long as attackers lack sufficient computational power to solve the underlying mathematical challenges in a timely manner. Efforts by IBM in the early 1970s laid the groundwork for modern cryptographic systems, culminating in the 1977 introduction of the Data Encryption Standard (DES) as a U.S. Federal Information Processing Standard for safeguarding unclassified information. Despite its age, DES continues to be a preferred option for securing electronic transaction data in financial institutions today. It is a symmetric-key or secret-key cryptosystem, meaning that the same key is utilized for both encrypting the plaintext and decrypting the ciphertext.

In the contexts of blockchain and IoT, cryptography serves as a combined approach to safeguard data and communications from unauthorized use or tampering. For instance, blockchain technology employs cryptographic techniques to ensure that data records are secure and cannot be altered. Similarly, IoT devices depend on cryptography to protect the information shared between connected devices. Cryptographic algorithms and building blocks, known as primitives, are designed to maintain the intended security properties even when attempts are made to compromise the system. In most applications, the primary security goals include confidentiality, integrity, authentication, and protection against unauthorized access or misuse [67, 68].

### 1.5.2 Digital Signature

A digital signature is an example of a mathematical scheme that ascertains the authenticity, integrity, and non-repudiation of a document or message [69]. It employs asymmetric cryptography, where a user signs the data with a private key, and others verify it using the corresponding public key. If the signature is verified, it certifies that:

- The message is authentic.
- The message is certified to have not been changed or modified after it was signed.
- The sender cannot contest that they signed off on the document.

In blockchain, digital signatures ensure that the transaction data or the creation of a block is performed by an authorized signer. Verification will fail if there is any form of alteration to the message or the signature, which ensures that no one can modify this process.

### 1.5.3 RSA

The RSA (Rivest–Shamir–Adleman) algorithm is known as an asymmetric encryption technique that depends on a public-private key pair. Operations related to the public key include encryption or verification, while operations concerning the private key involve decryption and signing [70].

### 1.5.4 SHA-256

SHA-256 guarantees a unique hash of a specific length for any given input. It is classified as a one-way function because the reconstruction of the original input from the hash obtained is impossible.

- Primarily used to compute the current hash of a block.
- This serves to maintain the integrity of a given message.
- It assures that the identity of each block is irrevocably tied to its contents.

In blockchain, it supports immutability if any small change in block data occurs, it will lead to a completely different hash.

### 1.5.5 Homomorphic Encryption

It is a specific type of encryption that allows operations to be performed on ciphertext without requiring plaintext at any point in the process [71]. All operations performed, when finally decrypted, yield results that would have been obtained if the operations had been conducted on the original plaintext. This property makes homomorphic encryption one of the most powerful cryptographic methods designed to enable secure processing of data in distributed or untrusted environments.

Since homomorphic encryption allows the entire process to be carried out without revealing the encrypted data, sensitive information remains permanently concealed from unauthorized access. This technique provides protection even during active computation, eliminating the risk of exposure during processing stages. There are two categories:

- Partially Homomorphic Encryption (PHE) allows only one function to be performed, for example, either addition or multiplication.
- Fully Homomorphic Encryption (FHE) permits any computations on ciphertexts without restriction. Homomorphic encryption allows for the computation of sensitive information without revealing the data itself, proving useful for privacy-preserving computation in domains such as healthcare, voting, and financial transactions. This technique enables smart contracts and blockchain nodes to compute on encrypted data without ever disclosing sensitive information, ensuring confidentiality is maintained at every stage.

## 1.6 Authentication

Authentication is a crucial process for maintaining information security, verifying the identity of a user, device, or system prior to granting access to resources or services. It ensures that the entity requesting access is genuinely what it claims to be. Authentication methods are tools designed to facilitate digital access control and to prevent violations of security protocols. Additionally, they play a significant role in safeguarding against data breaches, impersonation, and other malicious activities across the computer network. Authentication of IoT devices can be done using challenge-response mechanisms and curve fitting algorithms [72].

### 1.6.1 Challenge-Response Mechanism

A challenge-response mechanism is a cryptographic method used for authentication, confirming identity without exposing sensitive information over a network. This method involves two parties: one (the verifier) issues a random challenge (nonce or unpredictable string), and the other (the prover) must respond with a valid cryptographic answer based on a secret key. Authentication is granted if the prover's response is successful. For the authentication of IoT devices, the challenge-response mechanism offers an efficient method to authenticate connected devices by providing security and resource efficiency, thus serving as a lightweight solution. When attempting to connect or communicate, device challengers (gateways, blockchain nodes, etc.) present discrete cryptographic challenges. Devices sign these challenges by either using their private key or executing specific predefined cryptographic actions. The verifier checks the response through the device's public key, which is almost always kept in a secure ledger (e.g., blockchains). Key benefits of this method include:

- The absence of secret key transmission prevents exposure during communication.
- Resistance to replay attacks exists, as each challenge is unique and expires after use.
- Compatibility with asymmetric encryption enables identity verification in decentralized networks without a central authority.

### 1.6.2 Polynomial Curve Fitting

Polynomial Curve Fitting is a mathematical modelling technique used to establish an analytical relationship between sensed data points and underlying system behavior [73]. It involves fitting a polynomial function to a set of IoT data points (e.g., temperature, voltage, or signal strength) so that the resulting function captures patterns, trends, and deviations.

$$y = a_0 + a_1x^2 + a_2x^3 \cdots a_nx^n$$

In such systems, polynomial fitting has the following important uses:

- **Sensor Calibration:** Correcting the error curve in the IoT devices readings requires modeling the correction functions.

- **Data Prediction:** Deriving new values for time-series data from IoT devices.
- **Threshold-based Authentication:** In some lightweight cryptographic protocols, polynomial functions are used for secret sharing and authentication. For identity verification, each device maintains a point on a confidential polynomial, allowing only authorized devices to reconstruct the polynomial.

## 1.7 Blockchain in IoT Architecture

Blockchain has emerged as a powerful solution to solve the problems concerning the security of IoT systems. Blockchain can be implemented in IoT in various ways, including by applying its consensus protocols and block mining methods [74]. An Illustration of integrated structure for blockchain and IoT is shown in Figure 1.14.

- **Perception Layer:** This layer includes IoT devices and components such as sensors, storage devices, actuators, and communication modules. Its function is to monitor the environment by gathering current information for further analysis.
- **Network Layer:** Communication for IoT devices and data transmission are handled by the network layer. It utilizes broadband and Wi-Fi technologies. In addition to ensuring smooth data transmission, this layer manages the data flow and routing of the entire network. It also assists in processing big data while maintaining the dependability of the entire system
- **Blockchain Layer:** The conventional architecture of IoT systems is now complemented by this layer. It integrates components such as distributed ledgers, peer-to-peer communication protocols, smart contracts, consensus mechanisms, blockchain identity management, and more. With the aid of a distributed ledger, each device in the network can access synchronized and uncorrupted copies of the data. Smart contracts enable the automation of decisions based on preset conditions, and big data analytics enhance the storage and processing of large information streams.
- **Application Layer:** As a vital component of the architecture framework, the application layer provides services over a network and processes the

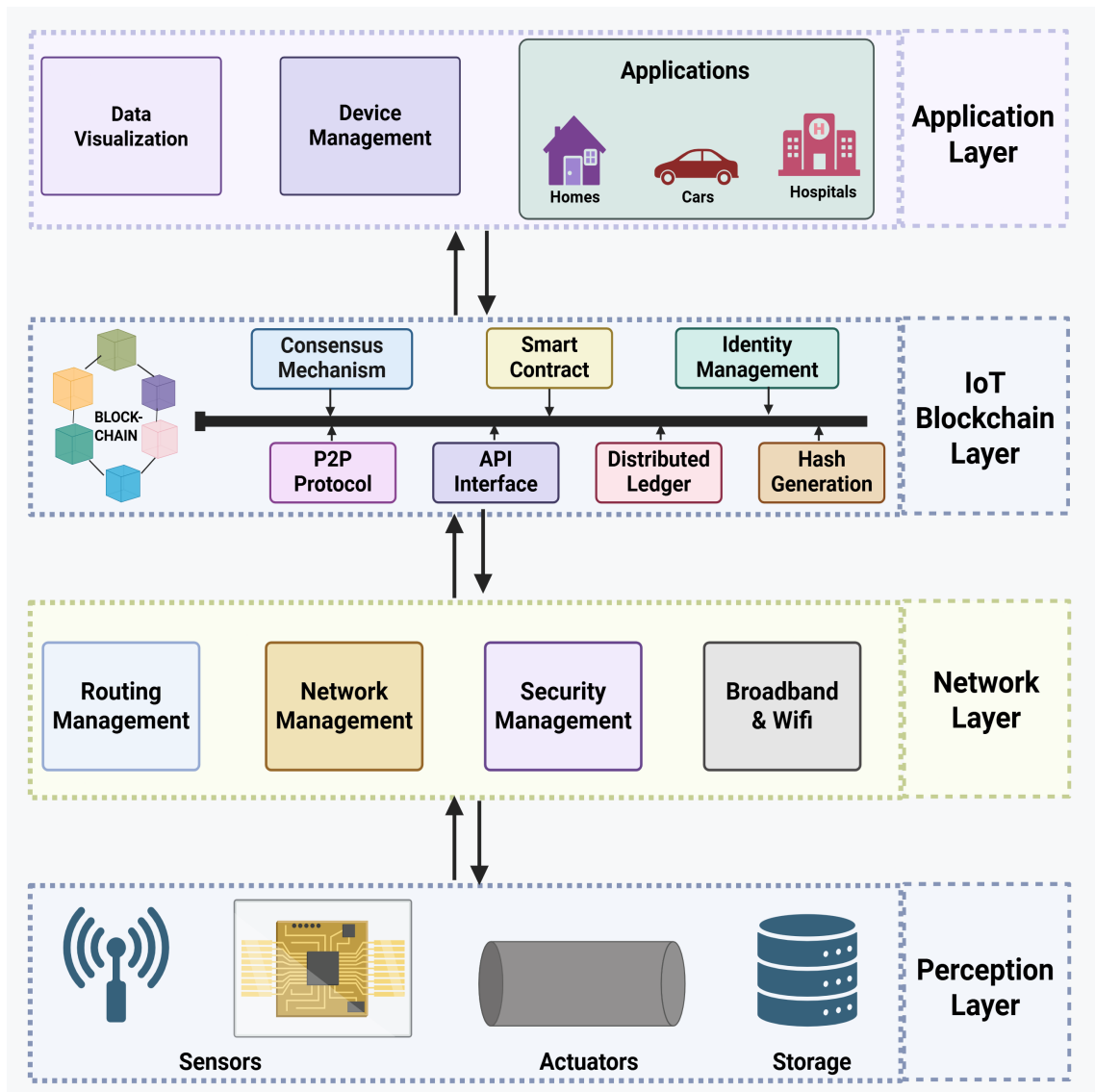


Figure 1.14: Integrated Architecture of IoT and Blockchain Technology

data received from the lower layers. Additionally, it supports various types of IoT implications as healthcare, intelligent transportation systems, and smart cities. This layer ensures that the captured data is processed and refined into timely and actionable insights, allowing users to make informed decisions, thereby helping to derive value from the data.

To implement a reliable blockchain-based IoT system, engineers must collect and evaluate data related to various hardware and software parameters [75]. Selecting an appropriate blockchain platform and consensus mechanism is essential for effective deployment. The choice depends on factors such as the number of

devices in the network, transaction frequency, and the rate of block generation. A lightweight blockchain platform with a low-resource consensus mechanism is generally preferred. This facilitates the use of private blockchains that demand less computational power. Development environments for smart contracts vary across platforms, which may influence implementation. System throughput and software architecture dictate the necessary hardware specifications. Accurate identification of these requirements is essential before deploying the prototype with real IoT devices. Each platform offers specific benefits and limitations when applied to existing systems. Adapting to a new platform may result in integration issues with current infrastructure. Blockchain integration can enhance data privacy and security in IoT systems [76]. This approach also involves transforming traditional infrastructures into a blockchain-based framework. Due to integration challenges, users may need to operate both existing and blockchain-based systems simultaneously. Although certain technical problems remain unresolved, the integration of blockchain into IoT devices continues to be a subject of technical study due to its effect on security and system performance.

### **1.7.1 Utilization of Integration of IoT and Blockchain in various sectors**

This study explores the various operational areas across sectors that might gain from adopting blockchain technology. It examines the potential applications of blockchain both currently and in the future. Implementing blockchain technology presents notable benefits, such as enhanced information security for storage, sharing, and networking. This could lead to increased efficiency, streamlined operations, and improved security measures due to distributed ledger technology [77, 78]. Additionally, this technology can improve process management, record evaluation, and information service administration. Moreover, integrating blockchain in these sectors offers benefits to administrators and data managers by protecting their intellectual property rights [79].

Blockchain technology has emerged as a groundbreaking innovation with the potential to transform various sectors by enhancing security, transparency, and efficiency. By providing a decentralized and tamper-resistant platform for recording and verifying transactions, blockchain offers a new paradigm for digital trust. However, successful implementation of blockchain requires utilizing different technologies tailored to the specific needs of each sector. This section explores the diverse technologies commonly employed in blockchain implementation across sec-

tors, highlighting their benefits and use cases. The various sectors that can be benefitted from the integration are:

- **Supply Chain Management:** The implementation of blockchain technology has the potential to augment transparency, traceability, and accountability within supply chains. IoTs have the capability to monitor and capture up-to-the-minute data pertaining to products, shipments, and transportation conditions. The utilization of blockchain technology [80] guarantees the veracity of the data, thereby mitigating fraudulent activities and upholding the integrity of goods.
- **Healthcare:** IoT devices, such as wearable devices and medical equipment, have the capability to produce substantial quantities of highly sensitive patient data [81, 82]. The utilization of blockchain technology can effectively guarantee the secure storage and sharing of data, while simultaneously upholding patient privacy [83]. This enables the achievement of interoperability and the maintenance of accurate health records.
- **Smart Cities:** IoT devices are essential for the advancement and implementation of intelligent urban infrastructure. Blockchain has the potential to provide a secure and decentralized method for managing data generated by sensors and devices in urban environments [84]. This pertains to the administration of energy consumption, traffic flow, waste management, and other associated factors.
- **Automotive Industry:** IoT devices installed in vehicles [85] have the capability to gather valuable data pertaining to driving behavior, vehicle performance, and maintenance requirements. The utilization of blockchain technology facilitates the secure storage and sharing of data, thereby enabling various applications such as usage-based insurance, secure vehicle history records, and communication among autonomous vehicles.
- **Waste Management:** IoT devices have the capability to monitor waste [86] levels in bins and subsequently optimize collection routes. The utilization of blockchain technology has the potential to facilitate the establishment of a transparent and immutable ledger for waste disposal and recycling activities, thereby fostering the adoption of sustainable practices.
- **Agriculture:** IoT devices have the capability to monitor various aspects related to agriculture [87], such as crop conditions, soil quality, and livestock

health. The implementation of blockchain technology enables the establishment of a trustworthy and transparent ledger encompassing the complete supply chain, spanning from the origin of food production to its final consumption. This utilization of blockchain ensures the preservation of food safety standards while simultaneously mitigating fraudulent activities.

- **Logistics and Shipping:** IoT devices possess the capacity to observe and document the motion, temperature, and general state of commodities during the entirety of the transportation procedure [88]. The utilization of blockchain technology provides a permanent and unalterable record, thereby augmenting visibility, mitigating conflicts, and safeguarding the authenticity of commodities.

The uses of blockchain and its features with IoT devices extends beyond the above sectors, finding applications in diverse industries such as Insurance sector, environmental monitoring, energy management, manufacturing sector and also in even cross border trades, creating a new era of secure and accountable data management. Table 1.2 explores the diverse technologies commonly employed in blockchain implementation across various sectors, highlighting their benefits and use cases.

Table 1.2: Technologies for Blockchain Implementation in Different Sectors

| Sectors                 | Technologies                                                                      | Benefits                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Financial Services      | Public and Private Block chains, Consensus Algorithms, Smart Contracts            | Improved transaction speed and security, Reduced cost and intermediaries, Enhanced transparency and audit ability.     |
| Supply Chain Management | Internet of Things (IoT), Smart Contracts, Distributed Ledger Technology (DLT).   | End to end traceability and transparency, Efficient inventory management, Fraud prevention and detection.              |
| Healthcare              | Interoperability Solutions, Cryptography, Smart Contracts.                        | Secure and interoperable health data exchange, Enhanced patient privacy and consent management, Streamlined processes. |
| Energy                  | Peer-to-Peer (P2P) Energy Trading Platforms, Distributed Ledger Technology (DLT). | Decentralized energy trading, Efficient grid management, Transparency in renewable energy generation and usage.        |

|                       |                                                                                 |                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Voting                | Cryptography, Smart Contracts, Consensus Algorithms.                            | Immutable and transparent voting records, Increased security and trust in the electoral process, Reduced fraud.           |
| Real-Estate           | Tokenization, Smart Contracts, Distributed Ledger Technology (DLT).             | Fractional ownership and liquidity Secure property transactions, Reduction in fraud and dispute resolution time.          |
| Intellectual Property | Digital Identity Solutions, Smart Contracts, Interoperability Solutions.        | Digital Identity Solutions, Smart Contracts, Interoperability Solutions.                                                  |
| Agriculture           | Internet of Things (IoT), Supply Chain Tracking, Smart Contracts.               | Traceability and transparency in the food supply chain, Quality control and certification, Fair trade and sustainability. |
| Education             | Credentials Verification, Smart Contracts, Distributed Ledger Technology (DLT). | Secure and tamper-proof academic credentials, Simplified verification processes, Fraud prevention.                        |

## 1.8 Challenges of Using Blockchain for Securing IoT Devices

Integrating blockchain into IoT systems enhances security and decentralization but also introduces several technological and operational challenges. These challenges need to be acknowledged to fully realize the potential of a distinctive, efficient, and fully automated IoT ecosystem powered by blockchain technology. The combination of blockchain with IoT has notably tackled many security concerns typically linked to IoT devices. However, this integration also brings forth various obstacles[89, 90].

- **Device Connectivity Issue:** The IoTs enables the connectivity of a vast array of devices to the Internet, with a potential scale of reaching billions. The potential for connectivity issues arises from the utilisation of blockchain technology to establish connections between IoT devices. Connectivity problems with devices may arise due to failures in data servers or routers.
- **Big Data Handling:** In the context of blockchain technology, it can be observed that every individual node possesses a unique decentralized database

that is accountable for maintaining the associated transactions [91]. In the event of new data being received, every node proceeds to update the distributed ledger. Tiago et al. reported that the number of machine-to-machine connections is expected to rise from 780 million to 3.4 billion by 2025 [92]. Expanding storage capacity is a difficulty posed by the combination of blockchain and IoT. The enormous number of devices linked to the router and server network is producing a sizeable amount of data that is difficult to handle [93].

- **Regulatory and Legal Issues:** Blockchain-enabled IoT systems encounter a multitude of regulatory and legal hurdles, encompassing an array of aspects such as data privacy regulations, Intellectual Rights, liability concerns and compliance obligations. The intricate terrain of regulatory frameworks and legal statutes pertaining to blockchain and IoT, which exhibit jurisdictional discrepancies, presents a formidable challenge [94]. Ensuring adherence to pertinent regulations and legislation, mitigating legal obstacles, and establishing suitable legal frameworks for the operation of blockchain-based IoT systems are essential to ensure their secure and lawful functioning [95, 96].
- **Concurrency & Throughput:** Necessitates the attainment of high levels of synchronisation and throughput, whereas blockchain technology operates within constrained parameters [97]. Therefore, taking into account the need for higher throughput to enable quicker transactions is necessary for the integration of blockchain technology with the IoTs. Enhancing throughput can be achieved through parallel processing, while the utilisation of a variable speculative currency control algorithm can enhance smart contracts [98].
- **Performance & Security:** The integration of blockchain with IoT facilitates the processing of data blocks generated by IoT devices. Panarello and colleagues proposed that the augmentation of blockchain block capacity can lead to an improvement in both the security of blockchain and the performance of IoT technology [101].
- **Scalability:** The issue of blockchain scalability arises when the quantity of nodes within the IoT expands, leading to a decline in the efficiency of blockchain operations. The issue at hand pertains to the IoTs, which involves a significant quantity of individual nodes [99]. This issue has the potential to constrain the network's capacity to process substantial data transactions.

The proliferation of internet-connected devices has led to a steady increase in the quantity of nodes over time [100].

- **Processing & Time:** In the context of blockchain, upon the addition of a new block, individual nodes undertake the management of their respective ledger copies, wherein data is stored. The process of altering data transactions on multiple ledgers concurrently is a laborious task [95]. The operating systems of IoT devices vary according to their intended application, and the execution speed and functionality of programmes may differ among devices [96]. Earlier iterations of the algorithm exhibit a longer runtime, while more recent iterations demonstrate a shorter runtime.

## 1.9 Research Objectives

- (i) To perform a comprehensive analysis of existing blockchain-based solutions for IoT applications.
- (ii) Designing a secured novel framework for blockchain-based security in IoT applications.
- (iii) To verify the performance of the proposed framework with respect to the existing state-of-the-art blockchain frameworks.

## 1.10 Scope and Motivation

The rapid proliferation of IoTs in smart homes, cities, and digital healthcare systems has elicited concerns regarding privacy, secure communication, and the reliability of data. Conversely, traditional legacy systems, characterised by their centralised architecture, impose delays, scaling challenges, and points of failure that are unsuitable within environments encompassing billions of diverse devices. Existing methodologies, especially access control and encryption, provide only partial protection and are inadequate for delivering comprehensive end-to-end security and dependable trust management in extensive, distributed IoT networks. Blockchain shows promise for addressing these issues due to its decentralized, transparent, and secure nature. For example, [13] developed a cloud storage system using blockchain and CP-ABE for access control, demonstrating its effectiveness in protecting data. [43] combined blockchain with machine learning to

enhance security in smart home communications. [24] focused on improving mobile edge IoT environments by integrating blockchain with reinforcement learning. [26] discussed using blockchain and AI for secure data management in smart cities and urban development. In healthcare, [91] and [78] proposed blockchain solutions for neural networks as secure searchable encryption and for sharing electronic health records. Additional research, highlighting the potential of blockchain for securing IoT included decentralized authentication for digital healthcare IoT [81], blockchain-enabled health data management infrastructures [82], and advanced cryptographic methods like RECC-MSS [90].

Recent advancements in blockchain have not fully addressed issues related to scalability, energy efficiency, and seamless integration into real-time IoT applications. Therefore, there is a need for a comprehensive blockchain framework that ensures the safe, transparent, and efficient management of IoT systems. This research aims to define and develop such a framework, emphasising the enhancement of IoT security while achieving performance goals such as low latency, balanced resource use, and robust resistance to cyberattacks and large-scale persistent threats.

## 1.11 Organization of the Thesis

The thesis is organized in the following manner:

### **Chapter 1 : Introduction**

This chapter discusses the background, significance, and challenges related to the applications of IoT technology, especially security concerns. It also outlines the research objectives, motivation, scope of the study, and how the research aims to fill the existing gaps.

### **Chapter 2: Review of Literature**

This chapter explores the literature on security within IoTs, blockchain technology, and related optimization techniques. This section reviews the literature on these topics, organises the materials, highlights the contribution of each work, and identifies gaps to be addressed, which motivate the current research.

### **Chapter 3: Enhancing Security and Resource Optimization in IoT-Edge Cloud using Blockchain**

This chapter introduces the initial proposed model, which combines the Artificial Bee Colony (ABC) and Whale Optimization Algorithm (WOA), emphasising resource optimisation and security enhancements through blockchain technology. The system model, proposed methodology, and performance results are carefully

analysed.

#### **Chapter 4: Blockchain-based Node Authentication Algorithm for Securing Electronic Health Record Data Transmission**

This chapter describes a secure communication framework for smart healthcare through a combination of blockchain technology and advanced deep learning techniques. The system design, adversarial framework, algorithm and assessment metrics, and experimental validation are presented and explained.

#### **Chapter 5: Blockchain-Integrated Deep Learning Framework for Securing Smart Healthcare Communication Networks**

This chapter introduces a novel blockchain integrated deep learning framework. It provides detailed methodology, algorithms, and comparative performance analysis against existing techniques, demonstrating improvements in throughput, latency, and data reliability.

#### **Chapter 6: Conclusion and Future Directions**

This chapter concludes the thesis and the future direction in the field of smart .

## **1.12 Summary of Context**

This chapter presents the IoT system, examining its layered structure and the distinct forms of attacks and security concerns prevalent at each layer. Additionally, it covers blockchain technology, its building blocks, attributes, categories, and its integration into a multi-layered framework to enhance the security and trust of IoT systems. It also provides in-depth explanations of consensus mechanisms and certain attacks that can be considered blockchain-specific. Various cryptographic methods, such as digital signatures, RSA, SHA-256, and even homomorphic encryption, are discussed to demonstrate how the confidentiality and integrity of data can be ensured. Challenge-response and polynomial curve fitting are explained in the context of device authentication and their connection to the discussed concepts. The advantages and challenges of integrating blockchain into IoT architecture are also explored. Numerous examples in different domains are provided from the practical perspective of this combination. Finally, research issues are addressed alongside the objectives, scope, and motivation of the study, and the thesis upon which it is structured is described. The last chapter reviews the literature related to IoT and blockchain.

\*\*\*\*\*



# Chapter 2

## Review of Literature

A comprehensive review of current literature will significantly aid in connecting the practical aspects of IoT application security with its future needs. This chapter examines solutions related to blockchain's role in IoT authentication, integrity, access control, and trust management. The review highlights the key shortcomings of existing research. Although progress has been made, challenges persist regarding scalability, overhead management, and the mitigation of complex cyber threats in diverse IoT frameworks.

A lack of research still exists on integrating blockchain technology with IoT to protect resource-constrained devices efficiently. New architectures are needed to enable secure data sharing, lightweight blockchain-based consensus, and decentralized access control tailored to IoT networks. Addressing these issues is essential for developing distributed IoT systems that ensure data confidentiality, integrity, and flexible access control. This chapter aims to tackle these concerns and proposes a mechanism that could improve security for IoT systems enhanced with blockchain technology.

This work explores how blockchain can enhance security in IoT systems, especially in areas like identity validation, data provenance, and intrusion detection, to offer greater assurance. In this review, the authors examine the performance of the methods described under real-world conditions, where the IoT is dynamic, vast, and heterogeneous. The literature is analyzed in terms of secure and lightweight communication, distributed trust systems, privacy-preserving data control and

dissemination, the role of intelligent machine learning in the IoT with embedded blockchain, and in the IoT's high degrees of synthesis.

Disruptive technologies such as blockchain have fundamentally transformed the management of trust and integrity within IoT systems. This shift is primarily attributable to the decentralized and distributed ledger technology, which incorporates validated cryptography, thereby reducing attack surfaces through the elimination of central authorities and the decentralization of system dependencies. Such advancements are vital for IoT applications in healthcare, smart grids, and transportation, where the reliability and security of data are of utmost importance. A variety of techniques have been introduced, including blockchain-enabled decentralized authentication, secure data offloading, distributed access control, and blockade-based intrusion prevention systems.

These methods aim to enable safe and secure collaboration among multi-party IoT systems, providing seamless access to transaction systems with improved resilience against attacks. Advanced systems achieve this through real-time distributed ledger technologies and highly synchronized blockchains. As a result, decentralized IoT record systems can offer increased protection, greater trust, and better performance in highly distributed environments.

## **2.1 Research Methodology and Plan of Study**

This section outlines the methodological framework used to conduct a qualitative analysis of the literature within the review, as well as the sources of the selected state-of-the-art contributions. It also includes the methodology integrated into the proposed research and discusses the contribution to the conducted review. The present study follows the systematic literature review (SLR) approach as outlined by Prisma (2020) and the work of Kitchenham and Charters (2007) [102, 103]. The aim is to thoroughly assess existing research papers and analyze previous scholarly contributions to develop a structured review that can support future research efforts..

### 2.1.1 Nature of Searching

This literature survey of security and trust management in IoT–Blockchain environments was carried out using established research sources. Several search keywords included securing IoT with blockchain, blockchain-enabled IoT security, overview of blockchain-based IoT frameworks, data privacy in IoT–Blockchain systems, decentralized access control, and lightweight authentication in blockchain-integrated IoT management.

### 2.1.2 Sources of Data

A wide range of credible sources was reviewed to gather and analyze the different methods and approaches discussed in this study. Relevant journal and conference papers were identified through well-known databases, including Scopus, WoS, SCI, and SCIE. Each selected work was carefully examined to determine the specific research areas and applications where the proposed techniques have been implemented. The percentage wise selection of papers from publishing sources is given in the Figure 2.1.2.

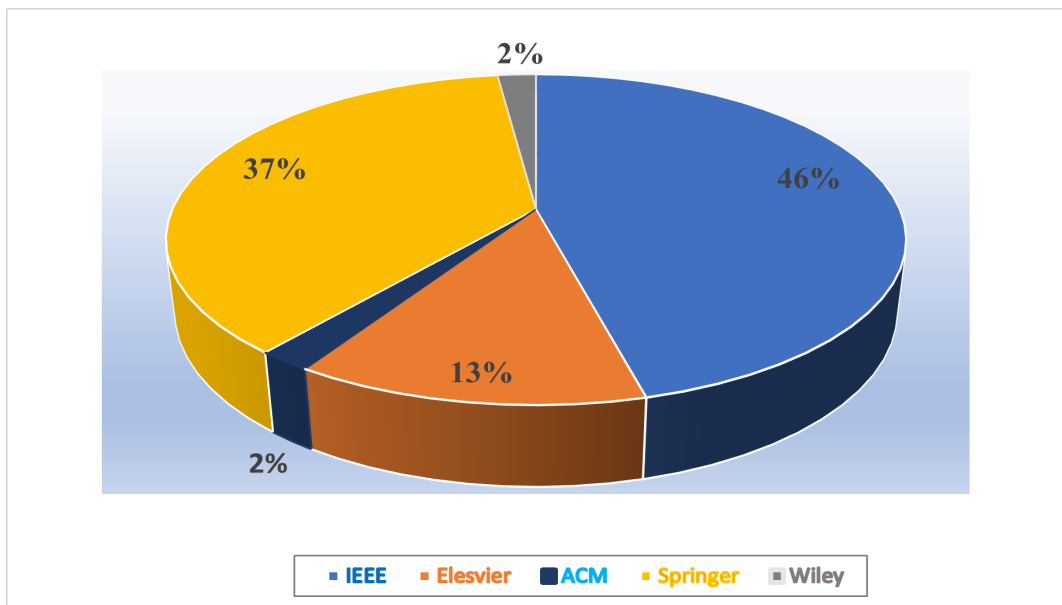


Figure 2.1: Percentage of Articles from Publishing Sources

### 2.1.3 Duration of Study

This literature survey primarily comprises papers from 2013 to 2025, selected from reputable peer-reviewed articles, technical reports, and conference records. The distribution of publications across these years is illustrated in Figure 2.2.

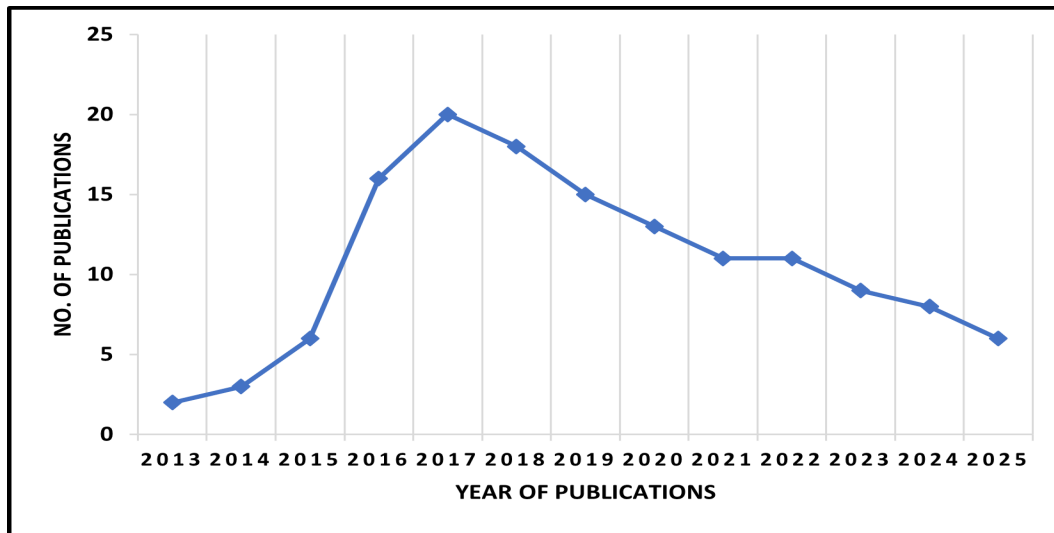


Figure 2.2: Number of Articles (Year Wise)

The graph indicates that the largest number of manuscripts was published during the period from 2016 to 2019. The period from 2012 to 2019 marked a significant boom in publications within the relevant fields.

### 2.1.4 Study Selection Criteria

The selection of articles is entirely based on whether they satisfy the inclusion criteria, whereas the exclusion criteria determine which studies are omitted from the review. Figure 2.3 shows the selection criteria for the literature.

**Inclusion criteria:** The inclusion criteria for the study encompass the following:

- Articles composed in English
- Relevant search strings
- Verifiability through reliable sources

- Scholarly evaluation by field experts.
- Publication dates ranging from 2015 to 2025 for up-to-date information.

**Exclusion criteria:**

- Discussions that lack focus on the pertinent concerns surrounding IoT technology are excluded.
- Materials that do not adequately address the security issues arising from the combination of blockchain technology and IoT are excluded.
- Any article that do not meet the specified search criteria are excluded from consideration.
- Articles that have not undergone peer review by experts in the field are excluded to ensure high-quality and reliable information.
- Publications that were published before the year 2010 are excluded to prioritize more recent and up-to-date sources.

### **2.1.5 Review Judgement**

This section provides a comprehensive overview of the qualitative evaluation methods applied throughout the review process. Well-defined criteria carefully guided the selection of studies to ensure that only relevant and high-quality research was considered. Initially, articles were screened based on their abstracts to determine their potential relevance. Those who passed this preliminary assessment underwent a more detailed evaluation in accordance with established inclusion and exclusion standards. Studies were ultimately included if they satisfied the following conditions, ensuring a systematic and rigorous review of the existing literature.

- Blockchain technology for securing IoT applications.

- Different architectures Blockchain for IoT environments.
- Additionally, the selected articles were critically examined with respect to their methodologies, key findings, limitations, and other relevant aspects.

### Flow chart

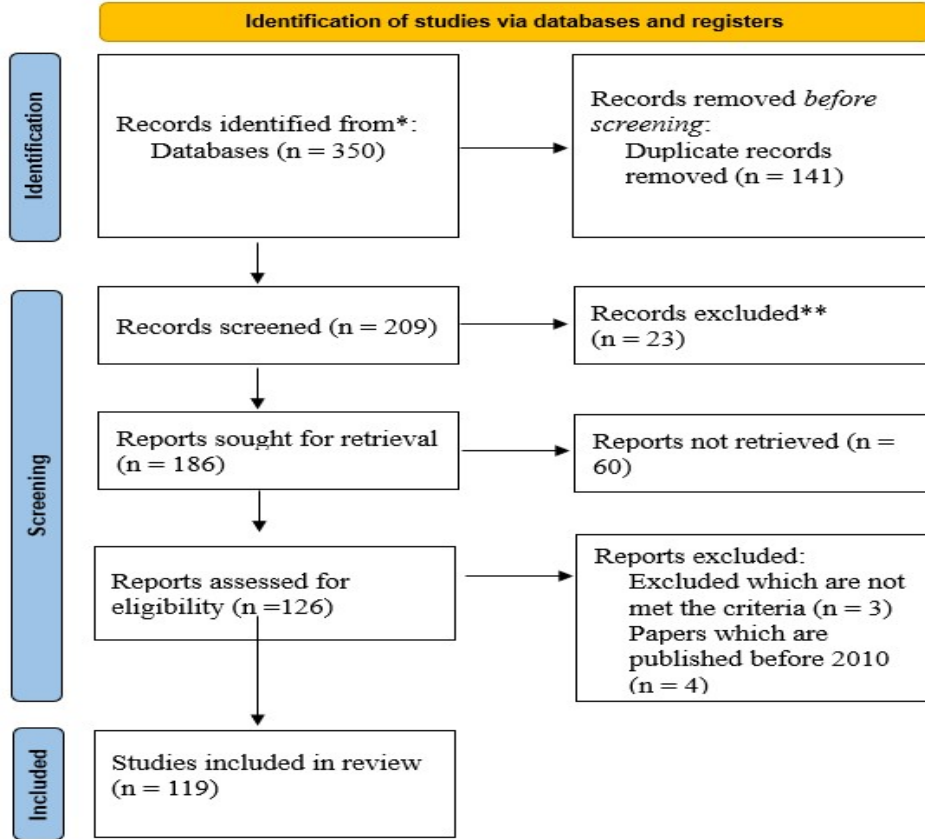


Figure 2.3: Flow Chart of Inclusion Exclusion Criteria

## 2.2 Literature Review

This section provides a detailed overview of the research findings and conclusions concerning the security implications of blockchain in IoT systems. It reviews the methodologies, approaches, and architectures adopted by various researchers to explore the advantages, challenges, and potential applications of blockchain technology in securing IoT devices and networks. The discussion also highlights key insights and advancements aimed at developing efficient and secure blockchain-based IoT frameworks. Moreover, emphasis is placed on the design of architec-

tures, algorithms, and protocols, along with the assessment of essential performance metrics such as scalability, privacy, and trust.

The authors examined how blockchain and AI can be combined to enhance IoT security against DDoS attacks, unauthorised access and data manipulation. The authors propose the BASIS framework, which categorises security solutions into seven dimensions. Blockchain guarantees decentralisation and tamper-proof records, whereas AI enhances anomaly detection and predictive security. The paper highlights the challenges of scalability, privacy, and interoperability in real-world implementations [104].

The research outlines multi-layer IoT security based on SDN, blockchain, and machine learning. It focuses on device, control, network, and application-level security. Blockchain enhances trust and immutability, SDN offers programmability and monitoring, and ML offers anomaly detection. The challenges the study has identified include scalability, energy overhead, and the lack of validation for large-scale deployment [105].

The IoTs are one of the technological advances now growing quickly and rapidly expanding technologies in contemporary society. The academic community is placing a high priority on the matter of safety and confidentiality with regards to IoTs, given its exponential growth in everyday utilisation. The functionality of IoT devices and applications is predominantly dependent on centralized cloud systems, which could potentially pose security risks to the authentication credentials of users [106]. Successful applications of IoT can be found in addressing the requirements of the community, however, it has been unable to effectively address the concerns related to privacy and security [107].

In recent times, scholars have established a correlation between the intention of reducing security threats in the area of cyber security, the IoTs and AI are utilised. In their study, Kuzlu et al. presented novel concepts aimed at developing sophisticated AI algorithms with the objective of mitigating cyber security breaches on IoT devices [108]. Despite IoTs and I convergence, unresolved security challenges persist. Consequently, the emergence of security challenges has necessitated the

application of blockchain technology alongside IoT to shield IoT devices from a range of security risks [109].

The authors of [110] developed, executed, and assessed a healthcare software framework that emphasized a worldwide vaccination approach, taking into account concerns related to healthcare privacy, the reduction of latency, support for scalability, and the utilization of a global identification system. The authors conceptualized, constructed, and prototyped the healthcare software Fog-Care. They utilized it in a fictitious scenario to assess performance metrics including latency, throughput, and send rate. In this scenario, numerous locations implemented a worldwide integrated vaccination campaign. The strategy made use of fog computing, blockchain, and unique identity technologies. The evaluation outcomes indicate that the minimum latency metric develops linearly and requires less than one second to execute. Scalable solutions are feasible with decentralized infrastructures that incorporate blockchain, global unique identification, and fog computing. Vaccination campaign conducted in clinics, hospitals, and research institutions across the globe. Privacy and identity concerns regarding data sharing are addressed.

In [111], Authors suggested to use an ECC digital signature as a hashing method with a public-permitted blockchain. At the IoT fog layer, this security mechanism offers a permanent security solution for medical data. The hash value of the file associated with the sharing link is encrypted during transmission, and a digital certificate is provided that can be accessed only by the authorized requester, even in cases where the files are publicly accessible. The captured data is securely stored within a fog-enabled blockchain ledger, while replicated copies of the blockchain records are maintained across multiple fog nodes and processed in the cloud database. To overcome challenges related to scalability and centralized control, the study employs a decentralized and distributed ledger-based blockchain record management framework. This provided transparency and prevented data manipulation.

In [112], Through the implementation of a decentralized peer-to-peer network, the

authors of this article alter the manner in which IoT data is stored and exchanged by replacing the centralized back-end paradigm with one based on Blockchain. This technology ensures a high level of accessibility for Personal Health Records, permits naming and tracking of connected devices, and safeguards patients' privacy via cryptography, according to the context of this article. The most significant contribution is the FogChain model, which proposes a differential strategy and the addition of an intermediary fog layer near the periphery to increase the capabilities and resources of the Internet of Things in order to circumvent its limitations. In contrast to Cloudlike Blockchain infrastructures, FogChain experiments indicate a possible 62.6% increase in response time.

In [113], The authors discussed healthcare IoT device identification and data authentication issues. Then, the author introduces a fresh approach to processing the PHD more securely. The PHD is filtered by conventional cloud servers in a centralized fashion. A single point of failure is more likely to occur with these centralized systems. Furthermore, hackers, nefarious actors, and outside invaders can all assault healthcare IoT devices. This results in data manipulation. Unreliable and unauthenticated PHD is caused by a high number of heterogeneous IoT devices. To address the aforementioned challenges, the authors proposed a three-tier fog-cloud-based blockchain architecture, supported by a mathematical framework and an advanced ASE algorithm. Additionally, they developed an analytical model for patient health data authentication and IoT device identification, ensuring secure data transmission within healthcare IoT environments. The iFogSim, SimBlock, and Python Editor tools are utilized to solve issue and carry out the suggested work. The suggested technique increases reliability and detection accuracy for malicious nodes. The ASE technique also minimizes packet errors during the transmission of PHD between end users and healthcare IoT systems. In performance evaluation and result analysis, the proposed algorithm demonstrates superior efficiency compared to existing state-of-the-art approaches such as FogBus, BeeKeeper, FemtoCloud, and FBAN.

In [114], authors described a revolutionary architecture for healthcare systems

based on the application of many cutting-edge technologies, including blockchain, IoT, FC, and AI. Here, an architecture that incorporates all of these technologies has been developed to take use of an integration of their capabilities. An illustration of a diabetes use case was used to support the suggested strategy. Diabetes was predicted using four ML algorithms: DT, RF, LR, and SVM. The diabetes dataset from the Frankfurt hospital was subjected to these algorithms, with the RF algorithm producing the best accuracy of 96.4%.

A smart healthcare framework is proposed in [115], demonstrating the feasibility of integrating and achieving interoperability between Blockchain 3.0 and Healthcare 4.0 while considering practical healthcare scenarios. Statistical simulation and optimization techniques are employed to evaluate Healthcare 4.0 processes in terms of data accessibility. The paper presents a comprehensive comparative analysis of contemporary blockchain-based smart healthcare systems. The study also explores optimization algorithms relevant to emerging Healthcare 4.0 trends, enhancing the efficiency and functionality of decentralized blockchain-driven healthcare applications. The proposed system incorporates predesigned smart contracts aimed at expediting payment procedures and fostering trust among stakeholders. To validate the proposed approach, both simulation and implementation were conducted.

In [116], The authors presented a novel method for automating cryptocurrency payments for services rendered by public fog nodes using blockchain technology. The suggested system is decentralized, reliable, automated, with guarantees for quality of service, client satisfaction, and conflict remedies via a reputation system. The suggested remedy controls communication between gadgets and fog nodes using the Ethereum blockchain and native smart contract functionalities. The suggested solution is put into practise, tested, and evaluated to ensure proper functioning and behaviour. Study also offers cost and security analyses and demonstrate the resistance of our solution to significant security intrusions.

In [117], the authors proposed segmenting the fog computing system into Fog Node Clusters (FNCs) to enhance security, where the fog nodes (FNs) within each

cluster share a unified Access Control List (ACL) secured through blockchain technology. Since blockchain generation is computationally intensive and can quickly exhaust the processing resources of FNs, the authors introduced modifications to the blockchain structure within FNCs to reduce storage and CPU requirements. Furthermore, they developed a novel blockchain-based FNC (BFNC) mechanism that enables automatic ACL recovery. In addition, a heuristic approach was proposed to minimize the time required for block hash computation by efficiently utilizing all available devices.

In [118], various sizes of content records were scrambled and decrypted by authors using AES calculations, and the results were compared to other calculations such as “DES, TDES, RC2 and Rijndael”. The analysis presented precise durations for each computation involved in the encryption and decryption processes of content documents of different sizes utilizing AES. The implementation of the execution aspect of the Rijndael cipher and its backward is addressed, despite the fact that Rijndael is suitable for efficient implementation on various processors and dedicated equipment.

The authors examined an innovative methodology in [119] for the integration of blockchain technology with fog and IoT networks, in addition to securing the communication of devices connected to internet. The framework has undergone deployment and testing within the IoT network. Enhancing the efficacy of an IoT framework in a heterogeneous environment is a feasible application of this research. This framework is suitable for ensuring communication security in the event that heterogeneous environments become the norm in the future and transmit massive quantities of data. They evaluated the system under a variety of conditions, including the impact of integrated system memory and processor consumption on overall system performance. It was found that the proposed framework enhances throughput and mitigates the need for direct connections between IoT nodes, thereby contributing to the system’s stability.

In [120], the authors focused on developing a user-centric access control framework that allows data owners to directly define and enforce access control policies.

To ensure reliability, the proposed system emphasizes auditability and trusted logging features enabled through blockchain technology. From a transactional perspective, blockchain transactions are utilized solely for storing access control attributes, while smart contracts are employed to leverage their flexibility and capability to enforce access control rules automatically. The proposed architectures and systems are categorized based on their domain, access control mechanisms, and underlying blockchain platforms. Moreover, the framework is designed to be adaptable, allowing customization according to user-specific requirements.

In [121], the authors designed and implemented a decentralized user authentication system using an Ethereum-based smart contract. The primary objective was to address authentication challenges in decentralized environments and mitigate security issues in fog computing that arise from IoT and cloud infrastructures. The study proposed integrating traditional authentication mechanisms within fog and blockchain environments to establish a distributed authentication framework, effectively resolving issues related to immutability and scalability in fog computing. To facilitate seamless adoption in real-world scenarios, the system incorporated commonly used authentication factors, ensuring compatibility with existing practices. Experimental comparison demonstrated that the given approach achieved improved performance, required less Ethereum (Ether) for execution, and exhibited enhanced scalability while utilizing fewer computational resources.

In [122], the authors proposed a decentralized blockchain-based framework that facilitates smart contracts between traffic data producers and consumers to address trust and latency challenges in data exchange among these stakeholders. The system leverages cooperative edge servers, allowing autonomous vehicles to connect to local edge nodes for data sharing and service utilization in accordance with predefined agreements. To evaluate the effectiveness of the proposed approach, proof-of-concept experiments were conducted using Hyperledger Fabric and virtual vehicle simulations, assessing system throughput under secure unicast and multicast data transmission scenarios.

In [123], Despite ongoing efforts to develop a successful BIoT (Blockchain-IoT)

integration, several challenges limit appropriate implementation as well as the application range of the integrated system to ensure its optimal use. The seven categories of challenges researchers discovered are security, privacy preservation, technological concerns, scalability, computational processing, regulations, and BIoT design. Future Internet of Things problems and research directions were also discussed.

Data authentication and confidentiality are two significant subjects addressed in the work cited as [124]. The proposed system encrypts and decrypts data using a secure mechanism and a 512-bit key to ensure data authentication. By utilizing the Blockchain ledger technology, data confidentiality is maintained while authorized users are granted access to the data. Finally, the encrypted data is stored on the edge device. In order to facilitate extremely rapid data access, medical reports are stored within the edge network utilizing edge computing technology. The data is capable of undergoing rapid decryption and processing when accessed by a verified user. The updated and processed data is stored in both the Blockchain and the cloud server. The proposed methodology guarantees the confidentiality and expeditious retrieval of medical data and reports.

In [125], the authors propose PriFoB, a privacy-aware, fog-enhanced, blockchain-based solution for international accreditation, which incorporates the concept of digital credential verification. Following that, two alternative consensus mechanisms, PoA and SoW, were implemented alongside digital signatures, SHA-256, AES, and RSA encryption schemes. In addition, a novel Distributed Ledger (3DDL) based on a dimensional DAG that features effective deterministic finality has been introduced. PriFoB's security, privacy, latency, throughput, and power consumption were evaluated by the author. Furthermore, they compared and contrasted our cloud-based implementation of PriFoB with analogous blockchain-based solutions designed for differently configured systems. All previously proposed solutions employing the Ethereum and Hyperledger technologies were outperformed by PriFoB. (Besu, Fabric and Indy). Paper also offered a PriFoB implementation that is prepared for deployment and made it accessible through

a public, open-source repository.

In [126], This study analyses the resource contribution paradigm when fog computing introduces blockchain between the fog node and cloud or consumers. The proposed model leverages the blockchain’s reward and penalty mechanism to incentivize active resource contribution from fog nodes. A transparent, open, and immutable service evaluation index is created by packaging the fog node’s resource-contributing behaviour and the task’s degree of completion into blocks and storing them in the blockchain system. The aforementioned process is modeled and analyzed, with the interaction between each fog nodes optimal resource contribution strategy and the corresponding maximum benefit addressed using the differential game method.

In [127], The main aim of this research is to provide a self-sufficient system where users can keep their credentials independently of TTPs. The usage of an autonomous network is essential for this, where individuals might identify themselves using their individuality. Three Blockchains Identity Management with Elliptic Curve Cryptography (3BI-ECC) is the framework that The Author suggest. Their framework is a decentralized system for managing identities where users’ identities are generated independently.

Table 2.1: Comparative Analysis of Recent Approaches focusing Blockchain for IoT security

| Year & Ref.   | Proposed Ap-<br>proach                                                                                         | Key Findings                                          | Pros                                  | Cons                           |
|---------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------|--------------------------------|
| 2026<br>[104] | Proposed BASIS framework integrates blockchain, AI, federated learning, and Layer-2 consensus for IoT security | Improved threat detection and secure trust management | Strong taxonomy, comprehensive review | Scalability and privacy issues |
| 2026<br>[105] | Multi-layer security using SDN, blockchain, machine learning, and federated learning for IoT defense           | Better anomaly detection and decentralized security   | Multi-layer defense approach          | Mostly simulation-based        |

|               |                                                                                    |                                                                                                   |                                                                                                |                                                                                |
|---------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 2022<br>[128] | Implementation of BC using Improved ECC Algorithm in E-learning platforms          | Improved trust in e-learning, Compared efficiency with other algorithms like RSA,DES,AES          | Improved Security, Improved Performance, Decreased Energy Consumption                          | Use of Complex virtual machine.                                                |
| 2021<br>[124] | Light-Weight Cryptographic Algorithm ECC is used.                                  | ECC with Blockchain provides maximum data privacy with lesser key size.                           | Maximize Security, High QoS, Increased Privacy                                                 | Energy efficiency is not considered, Communication cost is also not considered |
| 2021<br>[129] | A novel BC based privacy preserving architecture for IoT health-care applications  | User data stored in IHM and controlled by data owner, The data owner defines data access policies | No TTP required, Reduced BC load, Provides data integrity                                      | Data access time increases with increased load.                                |
| 2021<br>[113] | An algorithm for IoT device identification, verification and authentication        | Better performance when reduces the packet error                                                  | ASE encryption in FC easily outperform the cloud and others, High security, Better performance | Cost factors not considered, Complex implementation                            |
| 2020<br>[130] | BC-based approach for implementing a permission based HER system using chain code. | The system is made to facilitate health-care 4.0 applications, Improved security and privacy.     | Satisfy Different QoS requirement High CPU Utilization Good Response Time                      | Energy-constrains are not taken into consideration                             |

|               |                                                                                      |                                                                                           |                                                                                                              |                                                                                                      |
|---------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| 2020<br>[127] | 3BC based ECC framework for Identity management                                      | ECC used with BC to provide maximum data security and privacy with increasing performance | Identity privacy is considered, Node identification to prevent attack, Provides CA for every unique identity | Multiple IDs can be created by one user if unique identity is provided, Single factor authorization. |
| 2020<br>[115] | Integration of blockchain in Industry 4.0, Optimization algorithm for healthcare 4.0 | Ethereum implementation on network Blockchain                                             | Better Performance                                                                                           | No other parameters are discussed                                                                    |
| 2019<br>[131] | Proposed an e-learning blockchain system for assessment and certification            | Improves overall e-learning environment, Uses combo of both public and private BC         | Improved security, Improved storage, Increased performance of the system                                     | Energy constrains not considered, Other factors not considered                                       |

## 2.3 Node Authentication/Authorization in Blockchain

The security challenges faced by IoT devices, there is an increasing demand for a robust framework to address these issues. Blockchain has potential to enhance security within the IoT ecosystem by using decentralized and immutable nature. IoT systems can achieve greater protection against data tampering, unauthorized access, and other vulnerabilities. To analyse the existing frameworks, a thorough literature review is conducted in this section.

Velmurugan et al., (2024) [78] proposed Blockchain-enabled Hyperledger Fabric Architecture. The proposed solution had three steps: secure upload, download, and authentication. Authentication includes patient registration, login, and verification. The empirical analysis results indicated that the system outperformed

baseline methods. The proposed MKP-ABE outperformed the rest for file sizes between 10 to 25 MB.

Mahmood et al., (2024) [132] created a Cost-effective Authenticated Solution (CAS) for medical applications that are enabled by 6G. The CAS protocol offered the highest level of security enrichment based on the performance comparison. In addition, CAS reduced the cost of calculation by 8% and communication cost by 52% compared with competing similar protocols.

Shahzad et al., (2024) [133] introduced a system that applied the technology of blockchain for the encryption of EHR data and adopted the scheme of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to grant access control at the granularity level. The proposed technique provided EHRs, both secure and easily accessible by integrating a cloud-based healthcare Short Message Service with blockchain technology and smart contracts. The results revealed that the algorithm significantly improved safety and efficiency in the process of health data transfers.

Sonkamble et al., (2023) [134] proposed a mechanism to control access to electronic health record transactions and policies using Smart Contracts And Key Exchange Mechanism called SPAKE. The experimental setup had four nodes of the hyperledger fabric. In the results, it was seen that the proposed framework had better throughput than MedChain.

Mahmood et al., (2022) [135] provided a safe and economical authentication method for the wearable health monitoring device that uses the cloud. To demonstrate the suggested scheme's security robustness against known security risks, an informal security proof was discussed. Then, after comparing the suggested scheme's performance with related protocols, it was found that the method cut communication costs by 40% and calculation costs by 37%.

Shamshad et al., (2022) [136] introduced an authentication framework with powerful anonymity for IoT-enabled multi-server architecture in the Telecare Medical Information System (TMIS) via a physical function which is unclonable. The informal security assessment indicated that the suggested paradigm successfully

mitigates many security vulnerabilities encountered by contemporary TMIS-based protocols.

Fasila, K. A., and Sheena Mathew (2022) [137] offered an innovative and efficient technique for securing IoT applications. The suggested approach employed cellular automata concepts to regularly update this session key. The results proved the scheme's safety against several potential threats, and the Cost of an Advanced Encryption Standard (AES) encryption/decryption with a 128-bit key would be 9 mili joules.

Algarni et al., (2021) [138] studied the security and privacy of the IoT, highlighting issues stemming from its setup and rapid growth. The suggested solution primarily focused on developing BCMs to safeguard IoT access control and enable encrypted local communication between IoT nodes. The technology also opened opportunities for encrypted data exchange between IoT gadgets, fog nodes, and the cloud.

Shamshad et al., (2021) [139] provided an efficient and physically safe key-based methodology for smart wearables in the healthcare ecosystem based on Industrial Cyber-Physical Systems (I-CPS). Based on the security analysis, the proposed protocol offered robust protection against both physical and cyber-attacks. Moreover, its communication and computation overhead was compared with that of other protocols, thus validating its feasibility and practicability for deployment in an I-CPS-based intelligent wearable device with resource-constrained devices within the healthcare ecosystem.

Shamshad et al., (2020) [140] presented blockchain has potential for sharing EHRs while protecting patients' privacy and data. The proposed method ensured patients' privacy and security, which could enhance the efficiency of TMIS diagnosis and treatment. Before constructing any blockchain, its consensus, data structure, and methods were specified for private and consortium blockchains. All the EHRs were encrypted by a public-key and appropriate searchable keywords to obtain better access control, secure search, data security, and privacy protection. The systems security analysis demonstrated that it had achieved all its security

goals by preventing several security threats.

Ferrag et al., (2020) [141] detailed the problems and challenges of finding issues concerning the privacy and security aspects in the green IoT-based farming practices. Researchers divided green IoT-based agriculture threats into different categories, consisting of confidentiality, availability, privacy, authentication, and integrity. They presented the outcome and discussed possible future work problems in security and privacy concerning green IoT-based agriculture applications. Ali et al., (2020) [91] solved the problem of privacy and security in the IoT system. The Ethereum testing platform was used to develop Blockchain’s integration with IoT. To build an IoT smart environment, researchers employed a variety of sensors, all of which were authorized on the Ethereum network using the DecAuth protocol. Experimental results showed that the method achieved an accuracy of 98%.

Nguyen et al., (2019) [142] proposed a implementation of the Ethereum in a real-world scenario of data exchange via a mobile app hosted on the Amazon AWS cloud. The findings validated the concept as a viable method for secure data transfers in mobile clouds, protecting Protected Health Information (PHI) in the process with an overhead of about 100 ms. Table 1 provides a comparative analysis of various studies that have explored different techniques and methodologies for securing IoT applications using blockchain technology. The table highlights the key features, outcomes, pros, and cons of each study.

Table 2.2: Comparison of Different Techniques in Related Studies

| Year<br>Ref. | &<br>Techniques<br>Used | Outcomes                                           | Pros                                            | Cons                                                                         |
|--------------|-------------------------|----------------------------------------------------|-------------------------------------------------|------------------------------------------------------------------------------|
| 2024 [78]    | MKP-<br>ABE             | Demonstrated high<br>security and perfor-<br>mance | High security<br>through phased<br>verification | Limited<br>perfor-<br>mance<br>for files<br>outside the<br>10-25 MB<br>range |

|            |        |                                                                                                 |                                                                                 |                                                           |
|------------|--------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|-----------------------------------------------------------|
| 2024 [132] | AIoMT  | Maximum security with 8% computation and 52% communication cost reduction                       | Cost-effective and computation-efficient                                        | Limited scalability for extremely large datasets          |
| 2024 [133] | CP-ABE | Enhanced security and efficiency for EHR data exchanges                                         | Improved health data security and accessibility                                 | Complexity might increase with scaling                    |
| 2023 [134] | SPAKE  | Outperformed MedChain in throughput in a four-node Hyperledger fabric setup                     | High throughput; effective access control via smart contracts                   | Limited scalability                                       |
| 2022 [137] | AVISPA | Enhanced security against potential threats                                                     | Regularly updated session keys, quick and efficient system                      | Require significant computational resources               |
| 2021 [138] | BCMs   | Lightweight, decentralized, safe access control for IoT systems                                 | Encrypted local communication, opportunities for encrypted data exchange        | Potential scalability issues                              |
| 2021 [139] | I-CPS  | Strong defence against physical and cyber threats, with efficient communication and computation | Secure protocol for limited-resource intelligent wearable devices in healthcare | Specific constraints in hardware adaptability             |
| 2020 [140] | TMIS   | Enhanced EHR sharing while ensuring patient privacy and security                                | Improved diagnosis and treatment efficiency, robust privacy protection          | High implementation costs and blockchain setup complexity |

|            |                               |                                                                                                 |                                                                                                                       |                                                                         |
|------------|-------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 2020 [141] | 4-tier green IoT architecture | Classification of IoT-based agricultural threats, potential future research avenues             | Comprehensive threat classification focuses on privacy, authentication, confidentiality, availability, and integrity. | It requires extensive resources for implementation and maintenance.     |
| 2020 [91]  | Neural Network                | Secure data storage and smart contract testing                                                  | A decentralized nature ensures data safety, smart environment creation                                                | Potential challenges in scaling and integration with diverse sensors    |
| 2019 [142] | Ethereum blockchain           | Secure data transfers in mobile clouds, protection of Personally Identifiable Information (PHI) | Reliable access control, practical uses Ethereum blockchain                                                           | Implementation challenges in real-world medical data exchange scenarios |

## 2.4 Machine Learning based Security Environment for IoTs using Blockchain

Pratima et al., [13] proposed a blockchain-based cloud storage system integrating CP-ABE for secure, decentralized access control with fine-grained user revocation. The framework employs bilinear mapping-based cryptography and ensures data integrity via blockchain. While it enhances privacy and access flexibility, the system incurs high computational overhead, limiting its applicability in real-time, resource-constrained IoT environments. However, it lacks any neural network-based optimization, limiting its adaptability to varying network conditions.

Singh et al., [143] This study focuses on DDoS detection and mitigation issues in Software Defined Networks (SDNs) and conventional methods like packet-limit

techniques. Evaluation was done using a custom dataset of 1.7 million records for Snort (an IDS) and Machine Learning—with eight algorithms using a hybrid SVM-RF model achieving 99.1% accuracy. For mitigation, two methods were implemented capturing both dropping and redirecting illicit traffic, with redirection yielding greater network insights. The hybrid model significantly strengthened detection and mitigation functions, surpassing the single algorithm performance. Farooq et al., [144] proposed a security model for smart home networks that utilizes blockchain technology within a decentralized framework, incorporating integrated machine learning techniques. The authors aimed to combine network security with machine learning to leverage the data generated during communication among smart devices, optimizing computational efficiency while maintaining robust security through a cloud-based platform. The objective of the proposed system was to minimize computation delays while ensuring secure data exchanges within the network.

Menon et. Al., [43] discussed security challenges in IoT-based smart home networks and introduced a new communication architecture where blockchain and machine learning are used combinedly. The designed system allows authenticated users to communicate through the system and manage data transactions across smart, moderate, and avoidable categories using a neural network classification system. Also, a cloud-based evaluation layer and blockchain ledger improved data accuracy and security. The performance metrics reported that the proposed algorithm outperformed existing models in computational efficiency and false authentication rates, providing secure and efficient smart home communication.

A smartphone app for medical facilities was developed by Ichikawa et al., [145] that makes use of blockchain-based systems to provide continuous surveillance. This application performs as platform for helping the interactions between healthcare providers and patients, allowing effective management of needs through regular evaluation and treatment in healthcare systems. The utilization of Blockchain technology enables trusted audits, and tamper-resistant system. The performance evaluation of the application lacks the inclusion of comparison with current

methodologies.

A lightweight and safe blockchain-based framework for medical facilities was introduced by Srivastava et al. [146]. This concept uses cryptographic methods to circumvent the need for a PoW algorithm, and it uses IoT gadgets for surveillance. Using the blockchain system, Meng et al., [147] created a model for healthcare smartphone networks that can detect unwanted nodes. In order to better detect fraudulent activity, the system updates blacklisted information across different nodes in order to collect traffic-related information from possibly suspect nodes. However, the proposed model lacks a thorough analysis of security and privacy concerns. In order to confirm the reliability of medical IoT devices, Akkaoui [148] suggested a way of authentication that uses blockchain-based technology. While guaranteeing the safety of the firmware upgrade procedure for these gadgets, the proposed mechanism tackles the issue of duplication or duplicating units. The design incorporates a consortium blockchain, ensuring the features of confidentiality, privacy, security, and anonymity are effectively upheld. Additionally, it employs symmetric encryption to safeguard medical data and utilizes the zero-knowledge proof protocol for key security; however, it does not provide information regarding throughput.

The authors Ferrag et al., introduced a layered intrusion detection system that integrates three distinct classifiers. These classifiers feed their classification to the third one while two of them operate in parallel. RDTIDS system performed better when accuracy is measured and compared to Random Forest, Jrip, Naive Bayes machine learning algorithms [149].

Malik et al., [150] proposed a framework that uses blockchain technology to secure electronic health records (EHR), combining homomorphic encryption with recurrent neural networks to achieve better anomaly detection. While the mechanism effectively enforces authentication and protects patient privacy, the significant computational load may limit scalability in healthcare settings with limited processing power and memory. Table 1 presents a summary of the key features, limitations and relevance of the existing literature to the proposed work of the

related articles.

Table 2.3: Summary of Studies on Blockchain and IoT Applications

| Year & Ref. | Findings                                                                                                                              | Techniques Used                             | Pros                                                                                                                    | Cons                                                                                            |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 2024 [151]  | AI-driven blockchain integrated with edge computing for IoT networks, improving scalability, reducing latency, and enhancing security | IoT Networks integrating Blockchain and AI  | AI-based resource management, lightweight consensus algorithm, scalability improvements, reduced power consumption      | Limited to PoS algorithm; requires further testing in diverse IoT scenarios                     |
| 2024 [24]   | Optimization of IoT offloading in MEC environments with blockchain and deep reinforcement learning                                    | Mobile Edge Computing (MEC) and Blockchain  | DDQN and TOPSIS-based offloading decisions, improved energy consumption, cost, and latency                              | Complex implementation and dependency on synthetic datasets                                     |
| 2024 [26]   | Integration of AI and blockchain for secure data management in smart cities                                                           | AI-Blockchain Systems for Smart Cities      | Enhanced data security and decision-making, decentralized architecture                                                  | Focused on specific smart city applications; lacks details on integration with legacy systems.  |
| 2023 [152]  | BENIGREEN framework for Green IoT, addressing energy conservation, privacy, and decentralization                                      | Green IoT for Smart Cities                  | Cluster head selection using weight metrics, decentralized blockchain for privacy, certification, and revocation phases | Limited performance evaluation; does not address scalability in large-scale implementations     |
| 2023 [153]  | Secure datastore based on Ethereum smart contracts for confidentiality and cost reduction                                             | Ethereum Blockchain for Secure Data Storage | Tag-value pair-based design, reduced gas consumption, decentralized structure                                           | Limited query flexibility; high data volumes still require external storage solutions like IPFS |

|               |                                                                                               |                                          |                                                                                                 |                                                                                  |
|---------------|-----------------------------------------------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 2022<br>[13]  | Blockchain-based cloud storage with CP-ABE-based access control and immediate user revocation | Cloud Storage Integrated with Blockchain | Decentralized access control, bilinear mapping-based cryptography, fine-grained user revocation | High computational overhead; requires further analysis for real-time scalability |
| 2021<br>[154] | A medical certificate generation and verification system based on Blockchain                  | IoT-Based Healthcare Systems             | Decentralized certificate management, secure data sharing among health-care providers           | Implementation and testing are limited to theoretical designs                    |

## 2.5 Real-World Deployment Challenges in Blockchain-Enabled IoT Systems

Although blockchain integration in IoT systems offers numerous benefits, practical issues limit its implementation in the real world. Scalability and latency are one of the main issues. Traditional blockchain protocols, including Proof of Work and Proof of Stake, are inherently time-consuming and have low transaction throughput. This becomes a significant drawback of IoT applications that require real-time responsiveness such as smart healthcare, industrial automation, and smart transportation systems. The most recent research also focuses on the blockchain trilemma, highlighting how challenging it is to balance scalability, security, and decentralisation, thereby limiting the effectiveness of large-scale IoT implementations[155, 156].

The resource-constrained nature of IoT devices is also another critical issue. The computational capabilities, memory and battery life of most IoT nodes is limited, and it is not practical to execute complex cryptographic functions or maintain a full blockchain ledger. This incompatibility between blockchain requirements and device capabilities requires edge or cloud support, introducing additional design complexity and overhead. In the absence of lightweight blockchain solutions,

direct integration is inefficient and unsustainable [157].

Besides resource constraints, blockchain systems also come with significant computational and energy overhead. Constant transaction checking and running consensus mechanisms consume a lot of energy, and this issue is especially concerning for IoT devices, which are usually powered by batteries. This does not just affect the devices but also escalates the overall cost of running the system, raising questions about its viability in energy-sensitive applications.

Another key issue of real-world deployment is interoperability. The IoT ecosystem is highly heterogeneous, with a variety of devices, communication protocols, and network structures. The evolution of blockchain in these spaces needs to be compatible across multiple platforms, which would be hard to make seamless without standardised frameworks. Consequently, facilitating effective communication and coordination between IoT devices and blockchain networks is challenging [158].

Moreover, privacy and data management are of concern. Blockchain guarantees transparency and immutability but may oppose the privacy needs of sensitive IoT data, e.g., personal or healthcare information. When information is stored on the blockchain, it is difficult to alter or delete, and this creates difficulties in meeting the rules of data protection. The maintenance of privacy without compromising transparency remains a research question [156].

In network terms, real-world IoT implementations are prone to unstable connectivity, limited bandwidth, and changing environmental conditions. With such constraints, blockchain systems, which rely on constant synchronisation among distributed nodes, could perform poorly. According to recent studies, such infrastructure constraints can be a major factor affecting the reliability and performance of blockchain-based IoT systems, particularly at scale [159].

Although blockchain enhances security through its decentralised architecture and cryptographic mechanisms, it is not immune to vulnerabilities. There are problems like attacks when offloading tasks, manipulating consensus, and lack of

fault tolerance in dynamic environments that remain. Ensuring the robust and consistent operation of large-scale IoT systems is another challenging area that needs further research [160].

The adoption of blockchain alongside edge and cloud computing increases system complexity. There must be effective coordination to share computation, storage, and communication tasks among various layers. This integration may result in longer latency and poor resource utilization unless it is orchestrated properly. Recent studies indicate that blockchain-based hybrid architectures that integrate edge and cloud computing should be optimized further to enable real-world deployment scenarios [158, 159].

## 2.6 Summary of Context

This chapter provides a comprehensive overview of existing literature exploring how blockchain technology can be integrated with IoT systems, focusing on aspects like security, trust management, authentication, and access control. The discussion highlights how decentralized and distributed ledger technologies can address challenges faced by centralized IoT systems, particularly regarding scalability, data privacy, and vulnerability to cyber threats. The review emphasizes important contributions related to lightweight authentication, secure data offloading, decentralized trust systems, and privacy-preserving communication. It also highlights how blockchain can be used in healthcare, smart grids, and other critical infrastructures, where reliable and resilient data are essential. A systematic literature review approach, employing specific inclusion and exclusion criteria to ensure the selection of high-quality and relevant studies, is utilized. The findings indicate that although blockchain has improved IoT security, challenges related to computational overhead, interoperability, and large-scale deployment still need to be addressed.

\*\*\*\*\*



## Chapter 3

# Enhancing Security and Resource Optimization in IoT-Edge-Cloud using Blockchain

The increase in use and reliance on interconnected devices and data-driven services have increased the need for more sophisticated and secure computing frameworks. This study introduces the problem of security in IoT applications and resource management. To address these issues, we develop a hybrid framework that integrates the principles of blockchain technology with advanced optimization models, ensuring transparency, immutability, resource efficiency, and effective task execution. This work lays the foundation for reducing latency in IoT system, reducing energy consumption, and enhancing data integration within blockchain-powered IoT systems. The results demonstrate that the hybrid model outperforms existing research, proving its effectiveness in achieving better security and resource allocation.

### 3.1 Proposed Model

In this section, we delve into the models for both local and remote execution of multiple IoT devices, coupled with the integration of edge computing to optimize resource utilization. Additionally, we explore the crucial aspect of latency within blockchain systems and its implications.

### 3.1.1 Local Execution

Consider local computing with computing capability of  $l_i^{UE}$  at User Equipment(UE),  $i$ ,  $q_i$  is the required CPU cycles per bit and  $\alpha_i$  is the ratio of tasks computed locally. Thus, the local computation time of task can be expressed as

$$t_i^{UE} = \alpha_i y_i \frac{q_i}{l_i^{UE}}, \quad (3.1.1)$$

where  $y_i$  is the size of computation tasks. The total requested tasks of  $UE$ 's represented as

$$T = \sum_{i=1}^M y_i. \quad (3.1.2)$$

Here,  $T$  is the total task requests of all the users. The consumed energy at  $e_i^{UE}$  for local computation of tasks can be expressed as:

$$e_i^{UE} = (f_i q_i) \alpha_i y_i \quad (3.1.3)$$

Where  $f_i$  is the power coefficient of energy consumed per CPU cycle for local computation.

### 3.1.2 Remote Execution

It is necessary to send further task requests to the Remote IoT device, which must be overloaded, since the IoT device, has an indefinite capacity to carry out all of the  $UE$ 's tasks. The amount of time required for transmission to IoT device, may be stated as

$$t_j^{CC.trans} = 1 - \alpha_i - \beta_i \frac{y_i}{r_j} \quad (3.1.4)$$

where  $r_j$  is the data rate being sent from  $FBS_j$  to the IoT device, the transmission between FBSs and IoT devices often takes place through wired fronthaul lines. Wired connections are always faster than wireless connections and much more dependable.

### 3.1.3 Transmission Time & Energy Consumption

$UE_i$  will load its tasks to edge computing. We can compute the uplink data rate,  $r_{i,j}$  as in [161] for offloading by considering the background interference and

mutual interference caused by other UEs as

$$r_{i,j} = B \log_2 \left( 1 + \frac{p_i h_{i,j}}{\sigma^2 + I_{i,j}} \right) \quad (3.1.5)$$

$$I_{i,j} = \sum_{k \in m, k \neq i} p_k h_{k,j} \quad (3.1.6)$$

where  $p_i$  represents the data uploading transmit power of  $UE_i$  and  $h_{i,j}$  indicates the uplink channel power gain between  $UE_i$  and the  $FBS_j$ . When it comes to the uplink transmission, we use the assumption that all users are on the same frequency channel with a bandwidth of  $B$ .  $\sigma^2$  indicates the noise power level, and  $I_{i,j}$  is the interference power that comes from other users, where  $p_k$  represents the transmit power of  $UE_k$  and  $h_{k,j}$  is the uplink channel power gain between  $UE_k$  and the  $FBS_j$ . According to formula (4), the transmission time of  $UE_i$  for the purpose of data offloading between  $UE_i$  and  $FBS_j$  is specified as

$$t_{i,j}^{offl} = (1 - \alpha_i) \frac{y_i}{r_{i,j}} \quad (3.1.7)$$

The amount of energy that may be saved by offloading the duty of transferring UE data from  $UE_i$  to  $FBS_j$  is

$$e_{i,j}^{offl} = \frac{p_i(1 - \alpha_i)y_i}{r_{i,j}} \quad (3.1.8)$$

### 3.1.4 Latency Model with Blockchain Systems

Although latency is permitted for data, and its delay is often considerably larger than that of sensitive communication, this does not imply that latency of data transmission and calculation is unbounded. Latency, in particular, is regarded as a key measure for blockchain systems and cannot be overlooked. In general, data transaction processing in blockchain systems occurs in two stages: first, a block is formed, and then all users gain consensus on the generated block. As a result, the latency of data processing in blockchain systems includes the delay of block formation and confirmation, which is denoted as  $T_{block}$

$$T_{block} = T_g + T_d + T_v \quad (3.1.9)$$

where  $T_g$  is the average time needed for blockchain systems to generate a new block,  $T_d$  is the time used by data transmission, and  $T_v$  is the time cost for blockchain system validation.

$$\begin{aligned}
T_d = & \frac{1}{P} \times \left[ \left[ \min \frac{MS_b}{c_{n_m, n'_m}}, T_{lim} \right] \right. \\
& + \min \left[ \max_{n_i \neq n_m, n'_m} \frac{MS_b}{c_{n_m, n_i}}, T_{lim} \right] \\
& + \min \left[ \max_{n_i \neq n_j \neq n_m} \frac{MS_b}{c_{n_i, n_j}}, T_{lim} \right] \\
& + \min \left[ \max_{n_i \neq n_j} \frac{MS_b}{c_{n_i, n_j}}, T_{lim} \right] \\
& \left. + \min \left[ \max_{n_i \neq n_m} \frac{MS_b}{c_{n_m, n_i}}, T_{lim} \right] \right], \tag{3.1.10}
\end{aligned}$$

where  $P$  marks the total size of the block,  $S_b$  the number of bytes in each block,  $T_{lim}$  the average time necessary for the block producer to construct a new block, and  $C_{n_i, n_j}$  the data transmission rate of the connection between each pair of MTCDS. Furthermore, the time cost for  $T_v$  validation may be estimated as

$$T_v = \frac{1}{P} \max_{n_m=1, \dots, N_m} \left( \frac{P\gamma + [P + 4(K + \varsigma + 1)]\delta}{F_{n_m}} \right), \tag{3.1.11}$$

where  $\gamma$  and  $\delta$  are the computational costs for validating signatures and creating message authentication codes,  $K$  is the number of block producers, and  $\varsigma$  is the number of defective replicas.

In this formulation, the goal is to minimize the total time spent on tasks across IoT devices. Constraints ensure that each task is allocated to precisely one edge device, with sufficient processing capacity and available bandwidth to meet latency requirements.

To tackle this optimization challenge, we employ the ABC-WOA hybrid algorithm. ABC efficiently explores the solution space, while WOA enhances global search capabilities and convergence speed. Through simulations, we will assess the effectiveness of this approach, comparing it with other optimization methods. The aim is to showcase how the ABC-WOA approach excels in achieving resource optimization efficiency within IoT devices.

### 3.1.5 Hybrid Optimization Algorithm

Hybridizing optimization algorithms, like combining Artificial Bee Colony (ABC) and Whale Optimization Algorithm (WOA), is vital for achieving superior optimization outcomes. This approach enhances performance by synergizing the strengths of multiple algorithms, balancing exploration and exploitation, and providing robustness across various problem types. By customizing the hybrid approach to specific problems and dynamically adapting to changing landscapes, hybridization accelerates convergence, overcomes algorithm limitations, and maximizes the chances of finding high-quality solutions. It plays a crucial role in addressing complex optimization challenges across diverse fields, ultimately advancing efficiency and effectiveness in problem-solving.

---

**Algorithm 1:** Hybrid ABC-WOA Algorithm

```
1: procedure INITIALIZE ABC AND WOA POPULATIONS RANDOMLY:
2:   -ABC population: N_ABC bees
3:   -WOA population: N_WOA Whales
4:   Repeat for a Maximum of max_iterations or until termination criteria are
      met:
5:     for Each ABC Bee in ABC Population: do
6:       Employed Bees explore solutions locally:
7:       Modify the position of Bee using a local search strategy.
8:       Calculate the fitness of Each Employed Bee.
9:       Onlooker Bees select Employed bees based on Fitness and perform
         global search:
10:        Select Employed bees probabilistically.
11:        Apply global search strategy.
12:        Evaluate fitness of Onlooker bee.
13:     end for
14:     for Each WOA whale in WOA population do
15:       Update Whale Position using WOA equations:
16:
          
$$X\_WOA\_j = A * \sin(B) * | C * X\_rand - X\_WOA\_j | - X\_WOA\_j$$

17:       Evaluate fitness of WOA whale.
18:     end for
19: end procedure
```

---

**Security Enhancement:** The blockchain-based method is utilized to identify the malicious users in the IoT applications. The proposed method is implemented in MATLAB and performance is evaluated by performance metrics such as the probability of detection, false alarm probability, sensing performance gain, total error probability, missed detection probability, number of selected sensing nodes, average network throughput, and energy efficiency. The proposed method is compared by existing methods such as Friend or Foe(FOF) and Tidal Trust Algorithm(TTA).

### 3.1.6 Computational Complexity

The complexity of the proposed Hybrid ABC-WOA algorithm depends on the number of iterations, the population size, and the cost of the fitness function analysis based on the IoT and blockchain model presented in the paper. In both algorithms, ABC and WOA modules update their populations and calculate fitness values, resulting in a complexity of  $O((N_{ABC} + N_{WOA}) \cdot F(n))$  per iteration, where  $F(n)$  is the cost of evaluating task distribution, transmission rate, energy usage, and blockchain latency. The computation of the fitness itself is based on the number of IoT tasks/users ( $M$ ), blockchain transaction size ( $P$ ) and number of blockchain nodes ( $K$ ) and  $F(n) \approx O(M + P + K)$ . The overall time complexity after  $T$  iterations is  $O(T \cdot (N_{ABC} + N_{WOA}) \cdot (M + P + K))$ , which reduces to  $O(T \cdot N \cdot (M + P + K))$  when the sizes of the two populations are equal. Therefore, the proposed method has polynomial time complexity, and because of its quicker convergence pattern, the algorithm has improved practical efficiency compared to standalone ABC and WOA algorithms.

## 3.2 Result

The implemented proposed method undergoes thorough validation, employing a range of performance metrics. These metrics include Probability of Detection, False Alarm Probability, Average Network Throughput, and Energy Efficiency. Figure 3.1, we visualize the Probability of Detection measure. Our newly proposed methodology is subject to a comparative analysis against existing methods, namely FOF and TTA. Remarkably, our proposed methodology has achieved the highest Probability of Detection rate, standing impressively at 0.99. In contrast, the existing methods have yielded considerably lower Probability of Detection

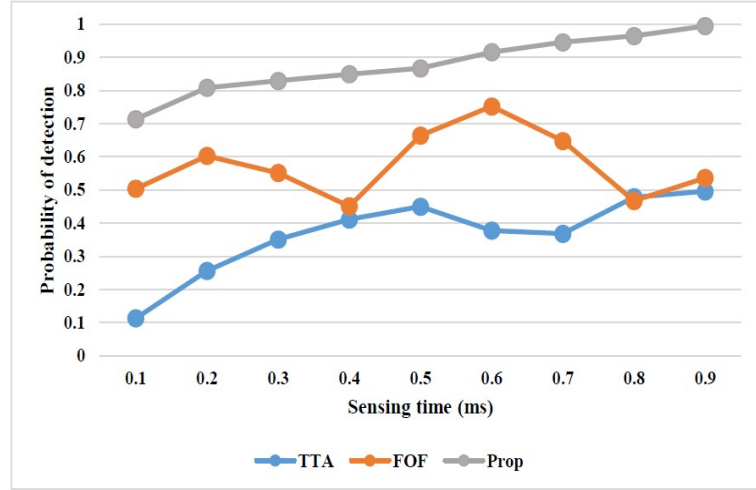


Figure 3.1: Probability of Detection Measure

rates, measuring at 0.53 and 0.49, respectively. Figure 3.2 represents the False

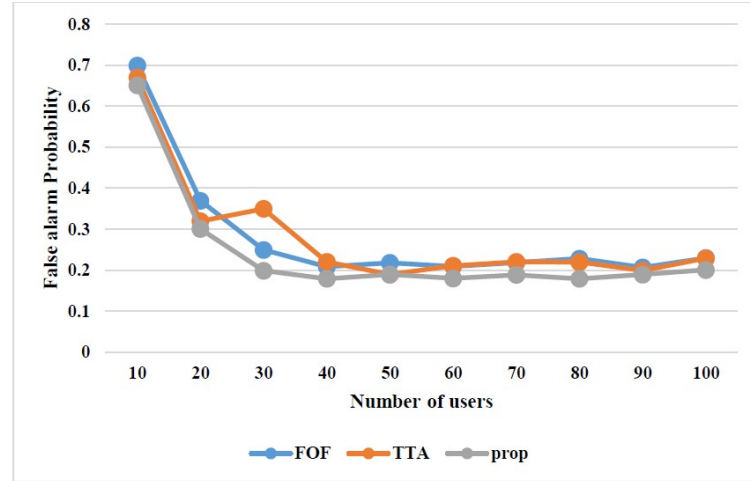


Figure 3.2: False Alarm Probability Function

Alarm Probability function. Our newly introduced methodology has excelled in maintaining a notably low False Alarm Probability rate, achieving an impressive 0.20. In contrast, the existing methods have demonstrated notably higher False Alarm Probability rates, measuring at 0.22 and 0.22, respectively.

Figure 3.3 displays the Average Network Throughput. Our newly proposed methodology stands out by achieving a notably high average network throughput of 2.2. In contrast, the existing methods, FOF and TTA, record lower average network throughputs, specifically 1.8 and 1.9, respectively. This comparative analysis unequivocally demonstrates the superior performance of our proposed method in terms of achieving the highest average network throughput.

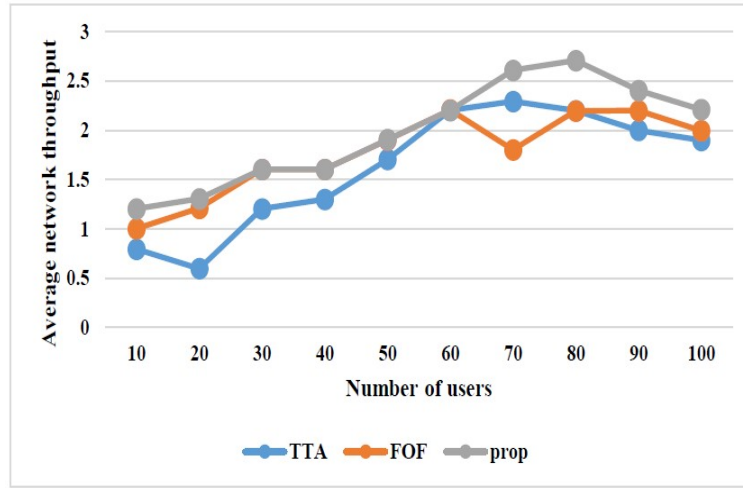


Figure 3.3: Average Network Throughput

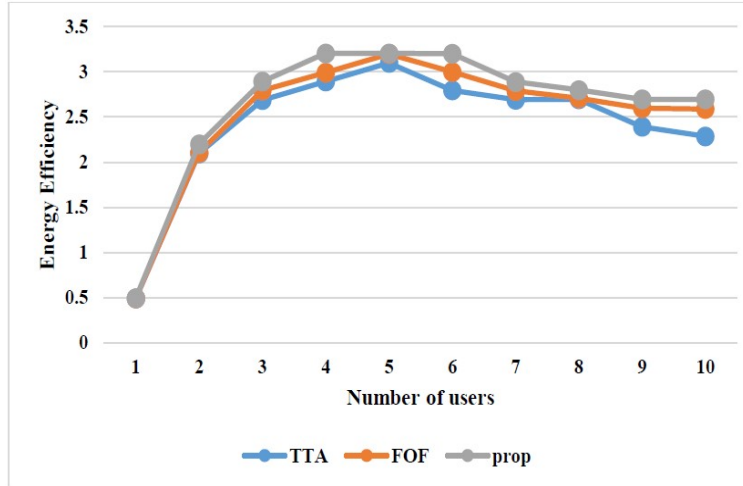


Figure 3.4: Energy Efficiency

Figure 3.4 visually represents the Energy Efficiency. Our newly introduced methodology excels with an impressive energy efficiency score of 2.6. In comparison, the existing methods, namely FOF and TTA, achieve slightly lower energy efficiency scores, measuring at 2.5 and 2.2, respectively. This comparative analysis unambiguously highlights the superior energy efficiency of our proposed method. To assess the performance of in resource optimization in IOT devices, we conducted a comparative evaluation of three optimization algorithms: ABC-WOA, ABC, WOA. Over the course of 10 iterations, we analyzed how each algorithm optimized time delay and energy consumption. This evaluation aimed to identify the most efficient algorithm for achieving resource optimization in IOT devices.

### 3.2.1 Computation Time

The computation time in our proposed ABC-WOA algorithm involves the amalgamation of data transmission time, processing time, and result fetching time from remote IoT devices. To optimize this time, we prioritize delay-bound tasks and allocate them to nearby IoT devices for faster processing. Simultaneously, resource-intensive or lower-priority tasks are offloaded to the centralized data center, which can handle higher computational demands. This approach ensures efficient resource optimization in the wireless sensor network, effectively reducing delays and enhancing overall performance by strategically distributing tasks based on their characteristics and requirements.

Figure 3.5 illustrates the convergence plot depicting the relationship between time

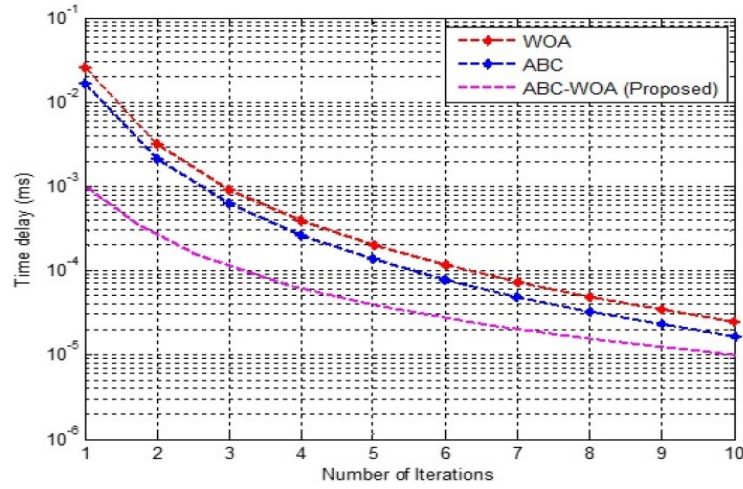


Figure 3.5: Convergence Plot Showing the Relationship Between Time Delay and Iteration Count

delay and the iterations for various methods, including the proposed ABC-WOA, ABC, WOA. The comparison results indicate that the proposed ABC-WOA exhibits a shorter time consumption compared to the other methods. By analysing the convergence plot, it becomes apparent that as the number of iterations increases, the time delay decreases for all the methods. However, the proposed ABC-WOA consistently demonstrates a faster convergence, resulting in reduced time delay in comparison to ABC and WOA. This finding suggests that the proposed ABC-WOA algorithm is more efficient in terms of time consumption when compared to the other methods considered in the study. Its ability to converge quickly allows for a faster optimization process, potentially leading to improved performance and time-saving benefits in practical applications.

### 3.2.2 Average Energy Consumption

Due to their limited processing capabilities, sensing devices have a lower  $E_{ij}^{total}$  than fog devices or centralised cloud servers. It should be noted that the overall energy consumption  $E_{ij}^{total}$  of fog networks is also dependent on  $E_{ij}^D$ ,  $E_{ij}^U$ , and  $E_{ij}^V$ . As a result of increasing the distance between the sensing devices and the computing server, the  $T_{ij}^D$  and  $T_{ij}^U$  of the tasks rise, as does the  $E_{ij}^{total}$  of the task. Similarly, as the data transmission rate and bandwidth of sensor networks increase, so does the data transmission and retrieval time of a job. Figure 3.6

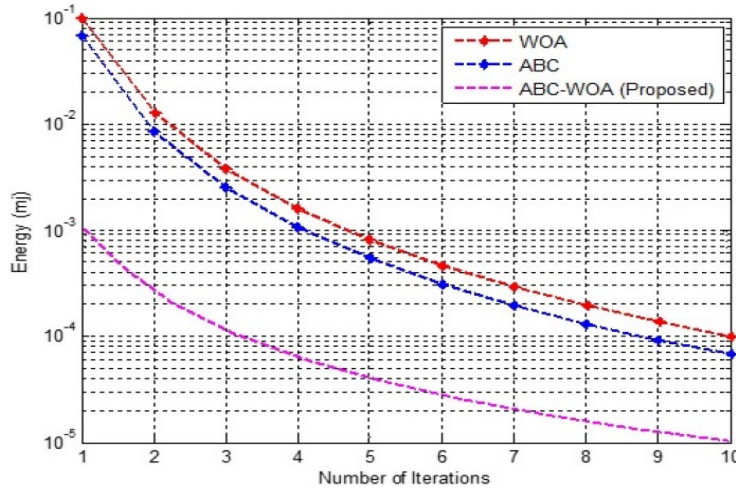


Figure 3.6: Convergence Plot Depicting Total Energy Varies with the Number of Iterations

presents the convergence plot, depicting how the total energy varies with the number of iterations for different methods: the proposed NSGA, GA, ACO, and PSO. Upon comparing the results, it becomes evident that the proposed NSGA outperforms the other methods in terms of energy consumption, displaying lower energy levels. These findings strongly suggest that the proposed NSGA algorithm is significantly more efficient in terms of energy consumption compared to the other methods under consideration. Its ability to converge quickly enables it to find optimal solutions that require less energy, making it a compelling choice for optimizing energy-related tasks and problems.

## 3.3 Summary of Context

This chapter presented an ABC-WOA hybrid optimization framework with blockchains, focusing on the dual challenges of security and resource efficiency in IoT environ-

ments. The approach enhances trust and guarantees secure data transmission by leveraging blockchain technology's transparency and immutability. Additionally, the ABC-WOA algorithm reduces time delay and energy consumption. The combined impact of improved security and efficient optimization indicates the framework's suitability for large-scale IoT settings, where minimizing computational overhead and ensuring reliable communication are crucial. The results support the use of ABC-WOA for performance improvement, advancing a secure and energy-efficient IoT-blockchain ecosystem.

\*\*\*\*\*

## Chapter 4

# Blockchain-based Node Authentication Algorithm for Securing Electronic Health Record Data Transmission

Healthcare systems utilizing IoT devices need secure and effective methods for managing and sharing sensitive patient data across multiple locations. Threats such as unauthorized access, data tampering, and privacy breaches can undermine patient trust and disrupt system operations. This chapter discusses these issues by describing a blockchain-based system for node authentication and data management designed for electronic health records (EHRs). The system features a four-layer architecture: Application, Authentication, Blockchain, and Cloud. The authentication module employs hashing, digital signatures, and a challenge-response protocol to verify node legitimacy before data transfer. The system integrates a blockchain network via Hyperledger Fabric to ensure immutability and distributed trust, while sensitive data is protected through homomorphic encryption, enabling computation on encrypted data. The cloud layer also enhances the system with RNN for accurate classification and processing of health records. The proposed system outperformed other systems in accuracy, achieving 99.01%, with a 99% security rate. Overall, this chapter establishes blockchain-integrated architecture as a robust solution for improving data integrity, privacy, and secure transmission in IoT-based healthcare environments. The key contributions of the chapter includes:

- Developing a novel node authentication algorithm using blockchain for secure access within the EHR system, specifically designed to address the

unique security challenges in IoT-based healthcare applications.

- Implementing an innovative combination of homomorphic encryption and blockchain mechanisms to protect sensitive EHR data during transmission, achieving both confidentiality and tamper-proof communication. This dual-layered security approach represents a new solution that enhances resilience against unauthorized access.
- Addressing critical research gaps in secure data transmission and reliable node authentication within healthcare, overcoming the existing vulnerabilities and inefficiencies in traditional methods.
- Reducing computational overhead and latency through a customized algorithm optimized for resource-constrained IoT environments, thereby enabling faster and more efficient secure communication compared to traditional security solutions.
- Highlighting unique contributions by enhancing the security, efficiency, and scalability of EHR systems, yielding immediate improvements in data security, reduced latency, and overall system performance for real-world healthcare deployments.
- Providing an immutable and transparent audit trail through a decentralized blockchain ledger, ensuring data integrity, traceability, and preventing unauthorized access. This contribution ensures that all access and modifications to EHR data are securely logged, fostering accountability and transparency.
- Conducting a comprehensive performance comparison with traditional authentication methods demonstrates the superior efficiency, scalability, and security of the proposed approach, which is particularly novel in its tailored application for secure IoT healthcare environments.

## 4.1 The System Model

In this section, we discussed the proposed layered system architecture and adopted an adversarial model and methodology. We also conferred the algorithm and discussed the evaluated performance matrices in detail.

### 4.1.1 System Architecture

Healthcare is the sector with the largest growth in terms of data and revenue. An increase in the number of EHRs brings the need to secure sensitive data. Blockchain's distributed and privacy-proof features make it the best solution for securing EHRs. However, the authentication issues in IoT make blockchain-based eHealth frameworks more vulnerable to threats. The digitalization of hospitals has raised concerns related to privacy. Blockchain features like encrypted, distributed, immutable make it more suitable and more effective for these systems. In this study, we employ our proposed algorithm via Hyperledger Blockchain. Figure 4.1 shows the adopted system architecture which is categorized into four layers, i.e., Application Layer, Authentication Layer, Blockchain Layer, and Cloud Layer.

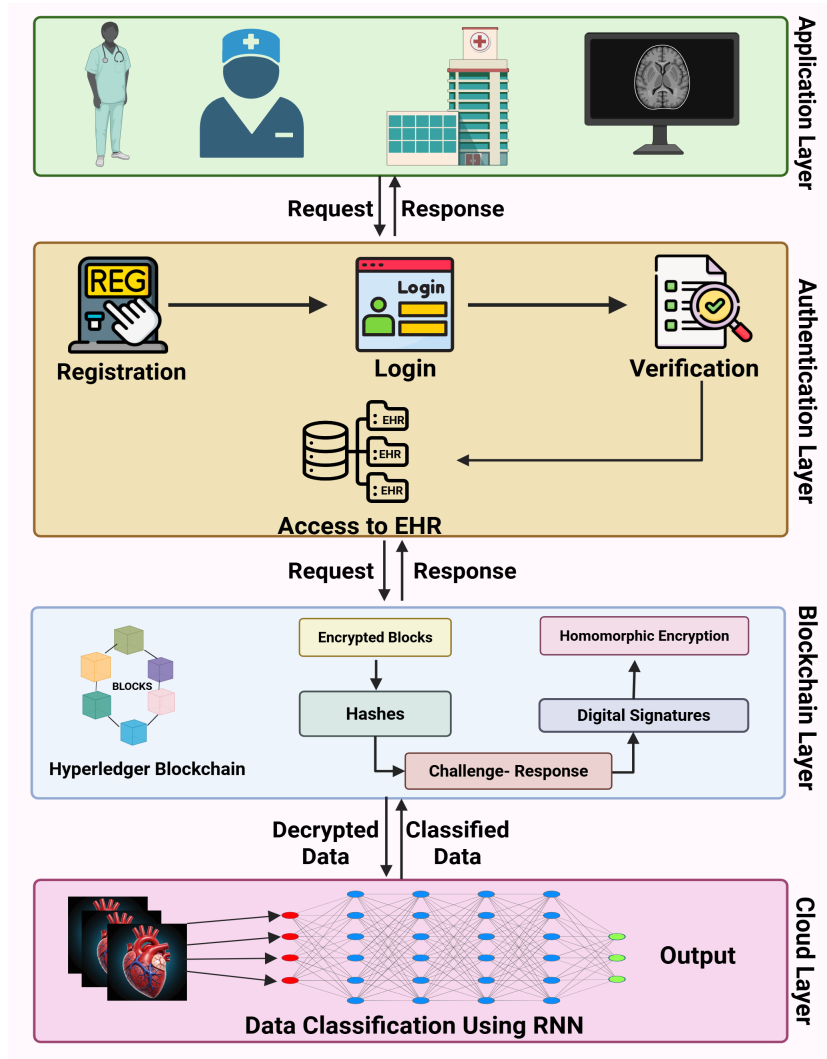


Figure 4.1: The Proposed System Model Architecture

#### 4.1.1.1 Application Layer

The Application Layer in the proposed architecture functions as the key interface connecting end users, such as medical professionals, patients, and medical institutions, with the blockchain-based system, thereby enabling smooth interactions and communication. It facilitates the processing of user requests and the provision of responses through a collaborative framework involving the Authentication Layer, responsible for the verification of identities and permissions; the Blockchain Layer, which ensures data integrity and secure access; and the Cloud Layer, which supports advanced data analysis and classification. The proposed system considers and offers customized functionalities for various stakeholders, including the provision of access to health records for patients, the facilitation of diagnostic data retrieval for physicians, and the capability for hospitals to oversee multiple users and records. Furthermore, it guarantees secure access to data and facilitates the visual representation of medical information, including EHRs. The requests generated by the users from the application layer are then sent to the authentication layer for further registration and verification of users.

#### 4.1.1.2 Authentication Layer

In this phase of the proposed system, authentication of nodes is implemented to verify or test the authenticity of the users. Authentication is a critical component of the proposed methodology to ensure that only legitimate nodes can access the system, particularly in sensitive environments like healthcare. Initially in this phase, a centralized server is employed that facilitates efficiency and scalability in handling node requests and challenges during the authentication phase. Besides, this phase involves registration, login, and verification steps. The registration of a user involves entering the credentials of a user which include first name, last name, username, and email address. This information is then saved into the database for further verification. In the authentication process of a node, the first step involves verifying the identity of the node using hash functions and digital signatures. The hash function is applied to the decoded request, denoted as  $H = Hash(\text{Decoded Request})$ . Following this, a digital signature is generated using the private key of the sender, represented as  $Signature = Sign(\text{Private Key}, H)$ . To complete the verification, the receiver uses the public key to verify the authenticity of the signature and the hash value, expressed as  $Verify(PublicKey, H, Signature)$  ensuring node identity validation. If the node is not authenticated, it will be

rejected. Otherwise, a challenge-response mechanism is implemented for further authentication. Where the challenge is generated by the server and sent to the node, in response the node provides a unique answer with its credentials which are then verified by the server and is mathematically represented as:

$$Is_{Authentic} = Verify_{Response}(Response, Node_{Credentials})$$

After the authentication phase, the user gets access to EHRs. A new session key is allocated to the user to perform operations on the EHR on the data encrypted using homomorphic encryption present in the blockchain.

#### 4.1.1.3 Blockchain Layer

Hyperledger Blockchain, in particular, Hyperledger Fabric, is a decentralized technology that aims at providing secure, efficient, and scalable data management with the shared ledger. It would surely enhance privacy, integrity, availability, and scalability through the sharing of data across multiple nodes and eliminating points of failure [162]. In this phase, every transaction goes into a block, which is chained up by unique IDs with an inbuilt immunity to modification and retrievability. The architecture implements endorsement peers, certificate authorities, and committing peers that engage with private channels to process and validate transactions securely. In Hyperledger, the Certificate Authority authenticates and grants users access to specific system features. The architecture of “individual chain per channel” allows for private data storage as well as improves scalability due to the segmentation of transactions in several channels [163]. This technology is effective in health care, where patient-specific EHRs are stored locally in blockchains, ensuring data integrity, privacy, and efficient access for authorized parties. Hyperledger Fabric offers a modular design that can handle dynamic data management in applications that require high security and flexibility [164]. Understanding cryptographic primitives is fundamental when working with Hyperledger blockchain platforms as they serve as building blocks that ensures security, integrity and functionality of the system. Some of the cryptographic primitives used in the proposed work are mentioned below:

- **Encryption:** is the practice of protecting sensitive information by transforming it from plaintext into ciphertext [165]. In the proposed methodology, homomorphic encryption is employed, allowing operations on encrypted data without decryption, ensuring the security of sensitive EHRs during transmission.

- **Hashing:** is the process of generating a fixed-length, unique hash value from input data, ensuring data integrity [166]. The methodology utilizes hashing to produce a unique digital representation of transmitted data, ensuring that any alteration during transmission is detectable.
- **Digital Signatures:** are used to check the authenticity and integrity of data using cryptographic technologies. In the proposed architecture the digital signatures are used to digitally sign a challenge for every request to a node by combining a private key with a hash value [167]. The corresponding public key is used for signature verification, ensuring that the request originates from a legitimate source and has not been tampered with.

These cryptographic primitives are utilized in Hyperledger Blockchain to overcome critical challenges in IoT-based EHR systems. It ends the single point of failure of traditional centralized systems, whereas its robust security framework means tamper-proof data management and seamless scalability. Combining Hyperledger Fabric with the machine learning model, this research increases the precision and speed associated with node authentication and safe data transfer while it provides an actual solution for complex IoT environments to maintain security for personal healthcare-related data. The blockchain involves the use of homomorphic encryption so that operations can be performed on encrypted data ensuring further security of the sensitive EHR data. Fig. 4.2 depicts Hyperledger Blockchain Architecture [168].

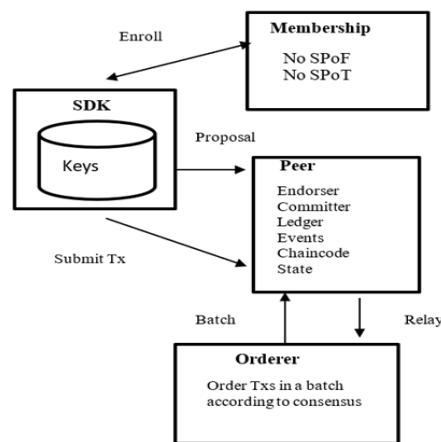


Figure 4.2: Hyperledger Blockchain Architecture

- **Homomorphic Encryption:** is also adopted in the proposed system architecture which is a type of encryption that makes an encrypted result that, when decoded, is the same as the result of operations done on plaintexts. By enabling certain calculations to be carried out on encrypted data, this homomorphic encryption creates an encrypted output that is equal to the outcome of carrying out the same procedures on unencrypted data [169]. Homomorphic encryption enhances the security framework since EHRs of sensitive information are kept encrypted during all the processing phases without any possibility of unauthorized access or exposure of sensitive information [170]. Data integrity is preserved as computations are performed on encrypted data by passing computations to an endpoint without modifying the original data, hence ensuring an accurate, tamper-free result. Data authenticity is also assured through homomorphic encryption that verifies legitimacy in computation and rules out the intervention of adversaries. The computation is also resistant to several attack vectors, such as brute-force attacks and data interception, since the data encrypted through this method remains encrypted throughout its lifecycle [165].

Homomorphic encryption also supports privacy compliance because it ensures secure processing in settings where decryption is not possible or is forbidden. Thus, it allows the possibility of following strict data protection rules. In the proposed methodology, it is evident how the system ensures the secure processing and transfer of sensitive EHRs, which ensures better confidentiality, integrity, and privacy through the application of homomorphic encryption within the system. The holistic approach accomplishes this by mitigating risks associated with unauthorized access and manipulation of healthcare data effectively, thus protecting the health data in complex IoT-based environments and strengthening the overall security posture of the system. Fig. 4.3 shows homomorphic encryption architecture. In the context of this work, homomorphic encryption is employed to ensure secure and searchable encryption of the data during transmission. Here's a brief description of homomorphic encryption and its role in the provided steps:

- **KeyGen():** The KeyGen () function must first make a Common Key (CK) before it can make a Public Key (PK), a Secret Key (SK), and a Verification Key (VK).
- **Enc ():** When the SK, the dataset (N), and the dataset label (L) are given to an encryption algorithm, the ciphertext is made (c). The acronym "Enc

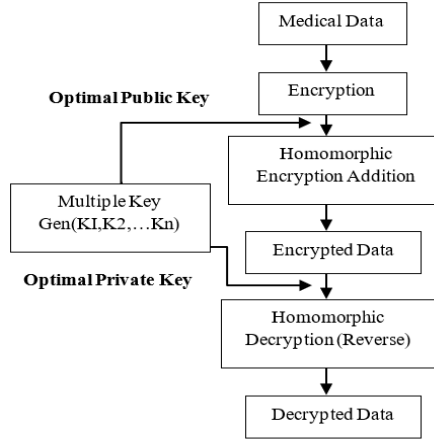


Figure 4.3: Homomorphic Encryption Architecture

()” is an abbreviation for “Enc” (SK, L, N).

- **Eval ():** Every Data User (DU) could request the evaluation algorithm stationed at the physical base station for processing. Eval () is a symbol for the parameters PK, homomorphic function (f), and ciphertext (C) that make up the Eval () function (PK, f, C).
- **Dec ():** The DU verifies the correctness of the computed data received from base station through the decryption procedure and then determines whether to accept it. The expression Dec (SK, DUQ, C), where DUQ is the DU-raised point, is a representation of the Dec () function.

The basic property of homomorphic encryption is that for any  $m_1$  and  $m_2$ ,

$$D(Em_1 \circ Em_2) = m_1 \circ m_2, \quad (4.1.1)$$

where Original message or data represented as M, encryption function as E, The ciphertext is C, The decryption function is D and  $m_1$  and  $m_2$  as the plaintext messages Represents some mathematical operations like addition or multiplication. The decrypted data is forwarded to the cloud server for further data classification, the algorithm incorporates a machine learning model called RNN.

#### 4.1.1.4 Cloud Layer

The cloud server is utilized for the classification of data. It uses RNN as a deep learning classifier. RNN is a particular type of neural network architecture that

maximizes its capabilities to handle data sequences. One notable feature of RNNs is their capacity to maintain a hidden state, which records data regarding the former inputs in a sequence [171]. In this research, RNNs are used for the machine learning model in the data classification process. It takes sequential input data and produces corresponding output predictions. Finally, the performance of the RNN is evaluated using metrics such as recall, precision, and accuracy. These metrics provide insights into how well the RNN can classify the input data.

The formula for the current state

$$h_t = f(h_{(t-1)}, x_t) \quad (4.1.2)$$

$h_t$  = Current state

$h_{(t-1)}$  = Previous state

$x_t$  = input state

The formula for Application of Activation function:

$$h_t = \tanh(W_h h_{t-1} + W_x x_t) \quad (4.1.3)$$

$W_h$  = Weight at the recurrent neuron

$W_x$  = Weight at the input neuron

$\tanh$  = Hyperbolic Tangent Activation function

Output Formula:

$$Y_t = W_y h_t \quad (4.1.4)$$

$Y_t$  = output

$W_y$  = Weight at the output layer

These equations illustrate the recurrent characteristics of the network, as the hidden state relies on both the present input and the preceding hidden state. This enables the RNN to apprehend sequential dependencies within the data [172]. The selected features for classification are ROW\_ID', 'SUBJECT\_ID', and 'HADM\_ID' mentioned in the DIAGNOSES\_ICD dataset. ROW\_ID' is selected to ensure each row is uniquely identifiable, 'SUBJECT\_ID' is selected to learn patient-specific patterns, such as repeated diagnoses and the progression of diseases, and 'HADM\_ID' is selected to group diagnoses that happened during the same hospital visit. Further, an adversarial model is employed to check the vulnerabilities of the system.

### 4.1.2 Adversarial Model

The adversarial model assumes that attackers have the encrypted data and the intercepted network traffic but do not possess the encryption keys or the cryptographic parameters, as demonstrated in Table 4.1 [173, 174]. Attackers can make brute-force attempts, perform replay attacks, and inject malicious data, but their capabilities are limited to ordinary computational resources, excluding quantum computing. Their objective is to extract sensitive information, breach authentication protocols, and disrupt communication. In response to these threats, the methodology applies homomorphic encryption for confidential data, challenge-response authentication for prevention against replay attacks, dynamic key exchange to refresh session keys, and blockchain immutability for maintenance of transaction integrity and detection of tampering.

Table 4.1: Adversarial Model Elements

| Element                     | Description                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Attacker's Knowledge        | The attacker has access to encrypted data but not the encryption key.                                                            |
| Attacker's Capabilities     | The attacker can perform brute-force attempts and observe network traffic.                                                       |
| Constraints on the Attacker | The attacker has access only to standard computational resources (no access to high-performance computing or quantum computers). |
| Attack Goals                | The attacker aims to extract confidential information from encrypted messages or disrupt system performance.                     |

### 4.1.3 Proposed Methodology

The presented methodology starts with receiving and transferring node requests. From the beginning, a client submits a request that is later encoded for added security. The request encoded is then transferred to the server for decoding back to its original state. This way, the data only travels between the client and server over a secure pathway. Proceeding with node authentication, the method applies a Hyperledger Blockchain-based EHR Management System. The decoding request is then passed through hashing, making it generate a unique hash value that represents the data uniquely. After that, generating a digital signature from the private key and the hash value is performed. It is the signature that verifies

the node's authenticity with the corresponding public key. Authentication is necessary to ensure that only authorized devices can access the system, especially in environments that handle sensitive information like healthcare where data security and patient confidentiality are paramount in preventing unauthorized access. If verification of the signature is successful, then the identity of the node is verified, and it can be carried further in the process. This approach, after authenticating the node, then employs a challenge-response mechanism to further authenticate the node. The server generates a unique challenge that it sends to the node; the node responds to it with an answer that would depend on its credentials. If the response is correct, the node is considered authentic, and the process continues to the next step. If the answer is incorrect, the request is denied, and only authentic nodes are granted access. Once authentication has taken place, the protocol exchanges session keys.

A new key is calculated using a randomly selected rule and the old key so that each session has a different encryption key. The old key is then overwritten from memory to eliminate any chance of its recovery or usage for malicious purposes. Then, the dataset receives an all-rounded preprocessing before feeding into RNN for training. This includes handling missing data where NaN values are replaced with column mean values in numeric columns and non-numeric values are filtered out for compatibility with the RNN model, followed by splitting the dataset into features represented by  $X$  and the target  $y$ . The data are also reshaped to a 3D array to be ready for RNN processing: samples  $\times$  timesteps  $\times$  features. All the feature values are scaled between 0 and 1 using MinMaxScaler to normalize normalization for optimal performance by the neural network. At last, the data is passed on to the RNN model for training with the function `model.fit()` and further used to adapt weights and learn underlying patterns from the data. Fig. 4.4 shows the proposed systems flowchart in diagrammatical representation.

#### 4.1.4 Proposed Algorithm

This section proposes an algorithm for a blockchain-based, hybrid node authentication and secure data transmission protocol for IoT applications.

---

**Algorithm 2:** Node Request Handling and Authentication

- 1: **Input:** Node Request
- 2: **Output:** Authentication Status, Secure Data Transmission Status
- 3: **Step 1: Receive/Transfer Node Requests**
- 4:  $\text{Encoded\_Request} \leftarrow \text{Encode}(\text{Request})$

```

5: Transfer Encoded_Request to Server
6: Decoded_Request  $\leftarrow$  Decode(Encoded_Request)
7: Step 2: Authentication of Node
8: H  $\leftarrow$  Hash(Decoded_Request)
9: Signature  $\leftarrow$  Sign(Private_Key,H)
10: if Verify(Public_Key,H,Signature) = False then
11:     return Authentication_Status = False
12: else
13:     proceed to Step 3
14: end if
15: Step 3: Challenge-Response Authentication
16: Challenge  $\leftarrow$  Generate_Challenge()
17: Response  $\leftarrow$  Generate_Response(Challenge, Node_Credentials)
18: Is_Authentic  $\leftarrow$  Verify_Response(Response, Node_Credentials)
19: if Is_Authentic = False then
20:     return Authentication_Status = False
21: else
22:     Authentication_Status = True
23:     proceed to Step 4
24: end if
25: Step 4: Session Key Exchange
26: K  $\leftarrow$  f(Random_Rule, Previous_Key)
27: Delete Previous_Key
28: Step 5: Homomorphic Encryption
29: Encrypted_Data  $\leftarrow$  Homomorphic_Encrypt(Data, Public_Key)
30: Decrypted_Data  $\leftarrow$  Homomorphic_Decrypt(Encrypted_Data, Private_Key)
31: Step 6: Secure Data Transfer
32: Encrypted_DataTransfer  $\leftarrow$  Secure_Transfer(Encrypted_Data, Control_Layers,
    Forwarding_Layers)
33: Step 7: Dynamic Key Update
34: Dynamic_Key  $\leftarrow$  Update_Key_Dynamically(Previous_Key)
35: Step 8: Data Retrieval
36: Training_Data, Testing_Data  $\leftarrow$  Retrieve_Training_and_Testing_Data()
37: Step 9: Storage in EHR System
38: Store Data in the EHR Management System
39: Step 10: Machine Learning Classification
40: Classification_Model  $\leftarrow$  Train_RNN(Training_Data)

```

```

41: Classification_Results ← Test_RNN(Classification_Model, Testing_Data)
42: Performance_Metrics ← Evaluate_Performance(Classification_Results)
    return Authentication_Status = "Access Allowed"
43: return Data_Transmission_Status = "Success"
44: return Performance_Evaluation = Performance_Metrics

```

---

### 4.1.5 Evaluation Metrics

Performance metrics like accuracy, precision, encryption time, decryption time, security, and recall can be defined as:

*Accuracy:* Accuracy measures the proportion of correct (True) predictions, including both True Positives (TP) as well as True Negatives (TN), divided by total number of predictions.

$$Accuracy = (TP + TN) \div (FP + FN + TP + TN), \quad (4.1.5)$$

where false positives are FP and FN represents false negatives.

*Precision:* Precision is defined as the ratio of successfully anticipated positive cases compared to the overall predicted positive occurrences.

$$Precision = (TP + FP) \div TP \quad (4.1.6)$$

*Recall:* The ratio of accurately predicted true cases to the total instances that genuinely belong to the positive class.

$$Recall = (TP + FN) \div TP \quad (4.1.7)$$

*F1 Score:* The F1 Score represents a harmonic average of precision as well as recall. It offers a singular metric that addresses precision and memory considerations.

$$F1score = (2 \times (Precision \times Recall)) \div (Precision + Recall) \quad (4.1.8)$$

*Encryption Time:* Encryption time  $T_e$  (in milliseconds) represents the total time required to encrypt the data of size  $n$  (in bytes), typically measured in seconds or milliseconds.

$$T_e = T_{end} - T_{start} \times 1000 \quad (4.1.9)$$

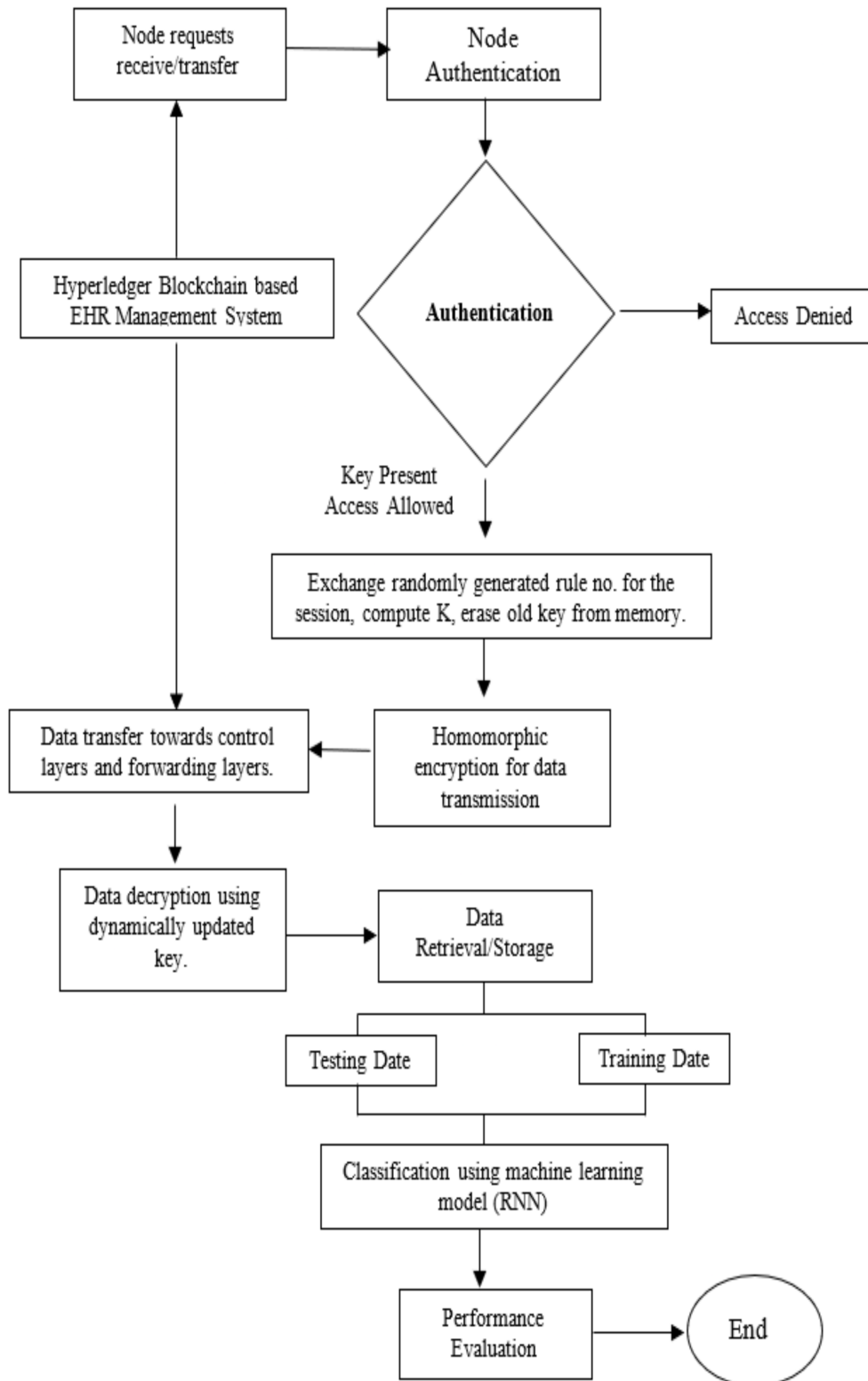


Figure 4.4: The flowchart of the Proposed System Model

$T_{start}$ : Encryption start time

$T_{end}$ : Encryption end time

Multiply by 1000 to convert time to ms.

*Decryption Time:* Decryption time  $T_d$  (in milliseconds) is the total time required to decrypt the data ne (encrypted data), providing insight into the time efficiency of the decryption process.

$$T_d = T_{end} - T_{start} \times 1000 \quad (4.1.10)$$

$T_{start}$ : Decryption start time

$T_{end}$ : Decryption end time

Multiply by 1000 to convert time to ms.

*Security:* Security is a qualitative measure, often quantified by factors such as key size, algorithm complexity, and resistance to known cryptographic attacks. A secure encryption method typically involves a higher key length, complex algorithms, and robust protection against attacks.

## 4.2 Experimental Study

This section is divided into two sub-sections. The simulation platform outlines the environment and tools used to conduct the experiments and the results and discussion section presents and analyses the findings from the simulations.

### 4.2.1 Experimental Setup

The interactions with the blockchain network are simulated by using a custom class named Hyperledger. The class simulates queries and function invocation on Hyperledger Fabric chain code, representing the business logic of the blockchain. Although, in this case, the interactions are simulated, the class gives a very realistic idea of how a real blockchain platform handles transactions-creation of blocks, data queries, and invocation of functions of chain code. Fernet encryption ensures the encryption of blockchain data to protect its confidentiality and integrity. The process of handling blockchain and data encryption also ensures authenticity through digital signatures in the form of Rivest-Shamir-Adleman (RSA).

On the machine learning side, the model utilized is an RNN, specifically a complex

RNN model built with Keras. The model is trained on data, and predictions are made based on real-world inputs provided by users. The dynamic key exchange mechanism in the proposed security framework is meticulously designed to ensure robust protection of encryption keys throughout their lifecycle. The dataset used in the model is stored locally on the system. The dataset can contain various columns with numeric values, such as diagnostic codes and other relevant patient information. The dataset name is “DIAGNOSES\_ICD.CSV” [175]. Data inputs for the machine learning model are encoded and decoded using base64 encoding to ensure safe transmission and are encrypted to provide a secure environment for handling sensitive data. Details of Software’s, tools and parameters used in the simulation are provided in Table 4.2.

Table 4.2: Software, Parameters used in the Simulation

| Parameters                       | Details                                                                          |
|----------------------------------|----------------------------------------------------------------------------------|
| Dataset Size                     | 2000 number of blocks + Patient Health Record                                    |
| Software                         | Hyperledger fabric                                                               |
| Hardware                         | GPU                                                                              |
| Parameters                       | Block height, number of blocks, no. Transact, no. PHR, delay, signature creation |
| Performance Metric               | Accuracy, precision, encryption time, decryption time, security and recall       |
| Number of Simulations            | Number of tests performed on a single dataset                                    |
| Number Of Rounds or Transactions | 5000                                                                             |

#### 4.2.2 Results and Discussion

This section describes the analysis of the results based on various parameters as described below:

**Hyperledger Blockchain-based EHR Management System:** During registration, users choose a unique username to differentiate themselves within the system. Once registered, they can log in using their Credentials to access authorized patient EHRs are stored on the cloud. Upon authentication, the cloud EHR administrator validates the user’s identity and access rights. The user’s account begins a transaction for accessing the patients EHR, which the cloud EHR manager retrieves upon verification of compliance with privacy standards. Authorized

users can view, analyze, update records, input new data, and manage patient information securely, utilizing blockchain and cloud technology to maintain data privacy and security.

The simulations analyzed the number of sent patient health records over 5000 rounds, conducting up to 3060 repetitions. The dataset included 2000 blocks, using Patient Health Records for calculations. Hyperledger Fabric was employed for a reliable simulation environment, and a GPU was used to enhance calculation speed. Simulations varied parameters such as block height, number of blocks, transactions, PHRs, latency, and signature generation. Performance evaluation measured the method’s correctness and effectiveness.

Here, the proposed method is compared with the baseline [91] method, and the results show that the proposed method achieves higher accuracy. In contrast to the proposed method, [91] could handle temporal information, which is input that arrives in sequences like a phrase. While [91] has limitations when it comes to processing temporal data, the suggested model was built with this in mind. The sum of simulations is proportional to the sum of tests performed on the dataset. The performance of the proposed blockchain-based node authentication method for securing EHR data transmission is evaluated using performance metrics as shown in Fig. 4.5. The proposed method’s performance is also evaluated based

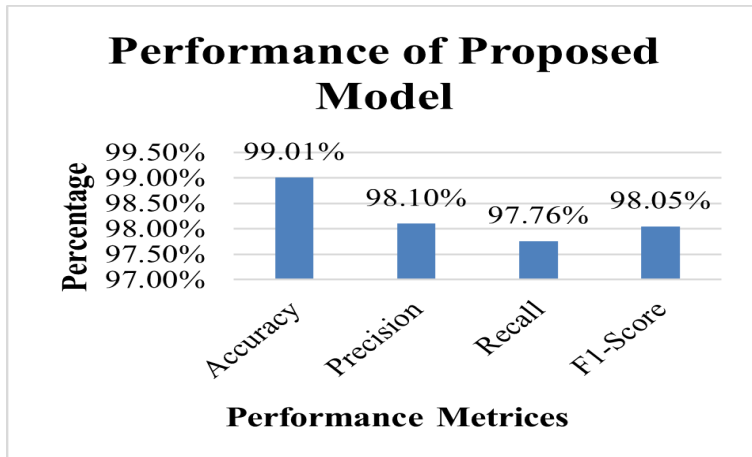


Figure 4.5: Performance Metrics of the Proposed Method

on encryption and decryption times for different file sizes. Table 4.3 shows the Encryption and decryption time of the proposed method, illustrating a linear increase in both metrics as file sizes grew. For instance, a 5 MB file took 330 milliseconds to encrypt and 360 milliseconds to decrypt, while a 20 MB file required 2254 milliseconds for encryption and 2603 milliseconds for decryption. This con-

sistent trend demonstrates the method’s scalability. The results underscore the robustness and efficiency of the blockchain-based node authentication algorithm, effectively managing encryption and decryption within acceptable time frames and ensuring secure, timely data transmission for EHR systems while maintaining data security and integrity.

Table 4.3: Encryption and Decryption Time of the Proposed Method

| File size (MB) | Encryption time (ms) | Decryption time (ms) |
|----------------|----------------------|----------------------|
| 5              | 330                  | 360                  |
| 10             | 1100                 | 1247                 |
| 15             | 1725                 | 1807                 |
| 20             | 2254                 | 2603                 |
| 25             | 3750                 | 4068                 |

#### 4.2.2.1 Comparative Study

In consideration to the studies that are presented in Table 5, a comparative analysis was conducted to assess key aspects. The ultimate design criterion remains that of access to distributed data in such a way that access can be both secure and efficient while maintaining its confidentiality and integrity. Most studies except one propose decentralized access, allowing several participants to access and contribute to the system based on a centrally managed authority. Identity management, which is crucial for the identification of users and regulation of access, is also adopted in several studies, but it is not taken as generally accepted. Likewise, authentication of the user, which is a fundamental element, is missed in a few studies. Overall, data integrity and data privacy, critical measures that determine the accuracy and security of information, are emphasized in all studies.

Table 4.4: Feature Comparison Across Related Studies and the Proposed Method

| Features                    | Authors of the study |                     |                    |                   |                       |                 |
|-----------------------------|----------------------|---------------------|--------------------|-------------------|-----------------------|-----------------|
|                             | MKP-ABE (2024) [132] | CP-ABE (2024) [133] | SPAKE (2023) [134] | TMIS (2022) [136] | Ethereum (2019) [142] | Proposed method |
| <i>Decentralized access</i> | ×                    | ✓                   | ✓                  | ✓                 | ✓                     | ✓               |
| <i>Identity Management</i>  | ✓                    | ×                   | ✓                  | ×                 | ✓                     | ✓               |

|                                                          |          |          |         |         |          |      |
|----------------------------------------------------------|----------|----------|---------|---------|----------|------|
| <i>User authentication</i>                               | ✓        | ✓        | ✓       | ×       | ✓        | ✓    |
| <i>Data Integrity</i>                                    | ✓        | ✓        | ✓       | ✓       | ✓        | ✓    |
| <i>Data privacy</i>                                      | ✓        | ✓        | ✓       | ✓       | ✓        | ✓    |
| <i>Machine learning-based classification of EHR data</i> | ×        | ×        | ×       | ×       | ×        | ✓    |
| <i>Latency</i>                                           | Moderate | Moderate | Low     | Low     | High     | Low  |
| <i>Scalability</i>                                       | Limited  | High     | Limited | Limited | Moderate | High |

The proposed method stands out as it uniquely incorporates machine learning-based classification of data, which is absent in other studies. Furthermore, the proposed approach demonstrates low latency, high speed, efficiency and scalability, addressing the limitations found in many of the reviewed studies, such as moderate or limited scalability and higher latency. This combination of advanced features, particularly the integration of machine learning, positions the proposed method as a more comprehensive and efficient solution.

Data confidentiality, data integrity, user authentication, decentralized accessibility, and identity management are some of the important aspects that other researchers have studied. In addition, other researchers have ignored the topic of improving cryptographic security, so the proposed research stands out. This proves that the suggested study provides a more thorough and improved technique compared to previous research.

The security of the proposed method is compared with MKP-ABE and KP-ABE [78]. Fig. 4.6 compares the accuracy of different techniques, with the y-axis representing accuracy in percentage (ranging from 90.00% to 100.00%) and the x-axis representing the various techniques used. The proposed method achieves the highest accuracy at 99.01%, followed by the neural network [91] at 98.00%, IoT-based CPS. [81] at 94.20%, and Blockchain-Assisted Secure Data Management Framework (BSDMF) [82] at 97.20% and revised elliptic curve cryptography multi-signature scheme (RECC-MSS) [90] have lower accuracies of 93.25%, respectively. Fig 4.6 effectively demonstrates the performance of the developed approach compared to the other existing techniques.

Fig. 4.7 and Fig. 4.8 demonstrates that the proposed method takes less time for encryption and decryption from MKP-ABE, AES, ECC, RSA and KP-ABE.

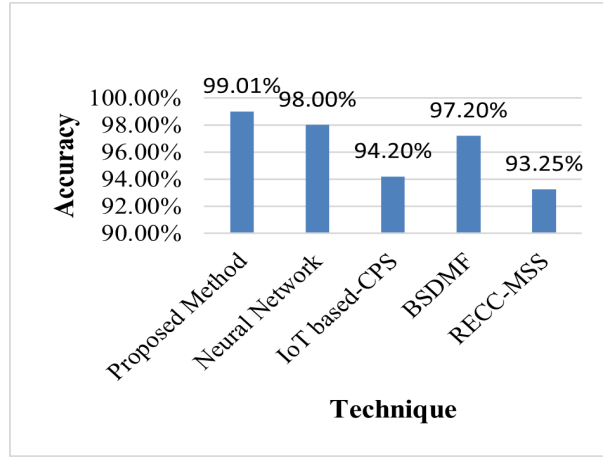


Figure 4.6: Performance Metrics of the Proposed Method

The encryption time (ms) of MKP-ABE (362, 1202, 2053, 2473, 4008), KP-ABE (701, 1552, 2428, 3004, 4569), ECC (912, 1853, 2869, 3457, 4865), RSA (1242, 2112, 3228, 3871, 5364) and AES(1538, 2448, 3634, 4248, 5701) which is much more than the proposed method as shown in table 4 for different file sizes. The decryption time (ms) of MKP-ABE (403, 1325, 2101, 2624, 4138), KP-ABE (843, 1644, 2558, 3146, 4701), ECC (1107, 2027, 3016, 3588, 5025), RSA (1378, 2286, 3382, 4015, 5501) and AES (1689, 2612, 3776, 4411, 5976) which is much more than the proposed method as shown in table 4 for different file sizes. Also, Fig. 4.9 shows that the proposed model has superior performance with a security rate of 99%, compared to MKP-ABE, AES, ECC, RSA and KP-ABE at 98.7%, 89.9%, 93.2%, 91.2% and 94.5%. The high-security performance of the proposed method is attributed to its integration of blockchain technology. And homomorphic encryption, which provides robust node authentication and secure data transmission. The immutable, distributed nature of blockchain integrated with advanced encryption techniques, ensure that sensitive EHR data is well-protected against various security threats. While MKP-ABE and KP-ABE offer significant security through attribute-based encryption, the proposed method's additional layer of security and transparency afforded by blockchain technology results in the highest security performance.

#### 4.2.2.2 Observations

The proposed system uses blockchain technology for managing EHRs, combined with homomorphic encryption methods to make data sharing very secure and ef-

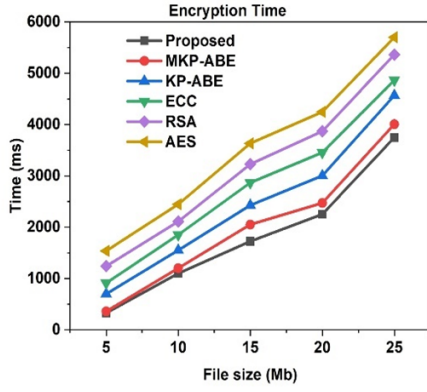


Figure 4.7: Comparison of Encryption Time of Proposed Method with Existing Methods

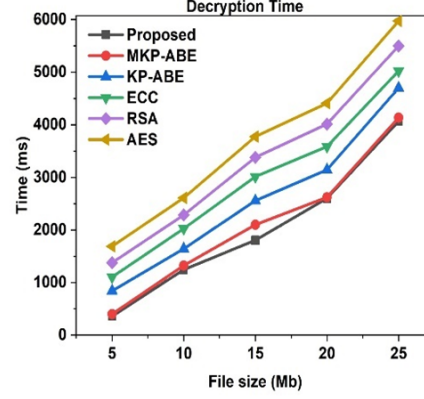


Figure 4.8: Comparison of Decryption Time of Proposed Method with Existing Methods

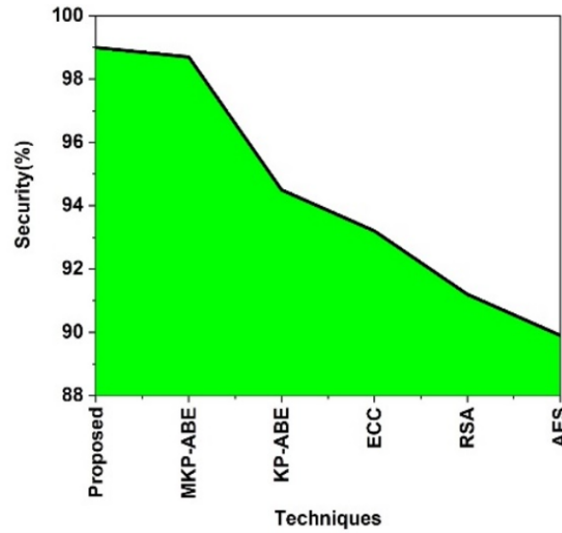


Figure 4.9: A Comparison of the Security of the Suggested Approach and Existing Approaches

ficient. The proposed system achieved 99% security rate and 99.01% accuracy, demonstrating systems stability. Unlike other methods like MKP-ABE and KP-ABE, this system offers better decentralized access, identity management, and strong security. It also handles increasing amounts of data smoothly, as both encrypting and decrypting information become faster as needed. Additionally, it uses advanced RNN to organize and classify data effectively, showing that it's practical for use in healthcare. However, there are still some challenges to overcome. These include expanding the system to work with large IoT networks,

integration with legacy systems, and making it adaptable to changing environments. Traditional authentication methods in IoT-based EHR systems include password-based, token-based (e.g., OAuth, JWT), certificate-based, biometric, and multi-factor authentication (MFA). While these methods offer simplicity or strong security, they are often vulnerable to attacks, prone to centralized failures, or complex to manage. Blockchain-based authentication, such as Hyperledger Fabric, provides superior security, scalability, and resilience by leveraging decentralization, eliminating single points of failure, and ensuring data integrity with an immutable ledger. Although it may have slightly higher latency, its robust framework is better suited for securing sensitive healthcare data in modern IoT environments. More research is needed to address these issues and ensure the system can be widely used and easily adopted in different areas.

### 4.3 Summary of Context

A blockchain-based framework for enhancing the security of EHRs transmission in IoT-enabled healthcare environments. As more people use digital health services, challenges such as unauthorized access, privacy violations, and data manipulation require robust solutions. To address these issues, the chapter proposes a layered design that includes Application, Authentication, Blockchain, and Cloud layers. Each layer contributes to reliable data flow, secure verification of nodes, and efficient data classification.

The methodology focuses on node authentication through hashing, digital signatures, and challenge-response procedures. This ensures that only authorized individuals can access critical data. Hyperledger Fabric enables the blockchain, which is immutable, decentralized, and resistant to tampering. Homomorphic encryption further enhances confidentiality by allowing computations on encrypted data without revealing the original records. The cloud layer employs RNNs to process and classify medical information, improving management of sequential health data with better accuracy and the performance validation is supported by RNN pattern analysis.

Evaluations demonstrate that the proposed system achieves high classification accuracy and security, handles varying workloads effectively, and remains scalable and efficient. It exhibits lower latency, reduced computational overhead, and stronger threat protection compared to other methods.

\*\*\*\*\*

## Chapter 5

# Blockchain-Integrated Deep Learning Framework for Securing Smart Healthcare Communication Networks

The rapid growth of IoT is due to its ability to enhance efficiency, optimize operations, and improve decision-making across different industries. As IoT devices increase, they produce large amounts of data, which can overwhelm traditional centralized systems. To solve this, Fog Computing has become an important technology that acts as an intermediary between the cloud and IoT devices, processing and managing data closer to the IoT nodes. Fog nodes placed at the network edge greatly reduce latency, lower bandwidth costs, and allow faster localized decision-making. In addition to fog nodes, cloud servers are used, offering scalable storage, high data processing capacity, and a centralized platform for analyzing the IoT generated data. The expansion of IoT-based healthcare networks, along with concerns about data security and device trustworthiness, has become increasingly important. Blockchain, a decentralized ledger technology, can strengthen IoT ecosystems by ensuring data integrity, transparency, and traceability across nodes. Blockchain uses consensus mechanisms to validate transactions. As IoT device data volume grows, ML techniques offer great potential. These methods can analyze data, forecast trends, optimize resource use, detect anomalies, and automate complex tasks, making IoT systems more adaptable and responsive to changing environments. Combining these technologies can create a resilient, secure, and efficient IoT framework capable of meeting modern demands. This study discusses the development of a deep learning-based engine integrated

into a healthcare IoT system. The first layer of the architecture is the IoT layer, where users interact with various devices through Fog Servers. Before joining the communication network, these devices are authenticated using a Curve Fitting mechanism. By fitting a polynomial curve to the expected behavior of IoT node data, deviations can be identified. Fog servers act as intermediaries between IoT devices and the cloud, managing and processing data locally. They help initialize channels and start communication. The data generated through this process is stored in the blockchain layer, which creates a secure digital ledger of communication details and provides extensive information about transactions. This layer also produces data based on various QoS parameters, including Throughput, BER, Latency, SINR, and PDR. The blockchain layer, integrated with the cloud layer, stores and processes this data. The cloud layer uses a neural network-based classification system to sort the data into three categories: Good, Moderate, and Malware. The key Contributions of the study includes:

- A secure, blockchain-integrated IoT framework for healthcare, integrating IoT devices, fog computing, and cloud-based machine learning, is proposed. The architecture ensures real-time data acquisition, low-latency processing, and secure storage using blockchain. By leveraging QoS metrics and neural networks, it enhances efficiency and reliability for applications like remote monitoring and emergency care.
- A secure blockchain layer is utilized for ledger generation of the communicating network.
- Implementation of a cloud-based data evaluation layer that facilitates the segregation and processing of data, enabling the creation of a ranking model structured around three primary categories of transactions.
- Implementing a deep neural network to train and classification of data and categorize data, thereby improving the decision-making processes within the blockchain layer.
- To evaluate the performance of the proposed model, a detailed comparison is done with the models presented by Subhita et al. [43], Pratima et al. [13], and Burhan et al. [26].

## 5.1 System Model

The proposed work incorporates smart healthcare architecture which utilizes a deep neural engine for training of data and rank generation. The proposed work is divided into four Sections, IoT and Fog Layer, Cloud Layer, Blockchain layer and workflow.

### 5.1.1 System Architecture

The introduction of electronic health records has led to an increase in data generation within the healthcare sector, and is projected to increase revenue in the industry, thus amplifying the need for data security. Blockchain, with its decentralized, encrypted and unchangeable structure offers a robust solution to protecting electronic health records. Nonetheless, authentication issues in IoT environments can put blockchain-based eHealth systems at risk. Along with increased digitalization of hospitals, issues regarding the privacy of patients have also peaked. In this research the proposed algorithm is employed using a Hyperledger Blockchain. The architecture of the system is illustrated in Figure 5.1, which has been divided into five distinct layers: IoT Layer, Fog Layer, Blockchain Layer, Cloud Layer and Application Layer.

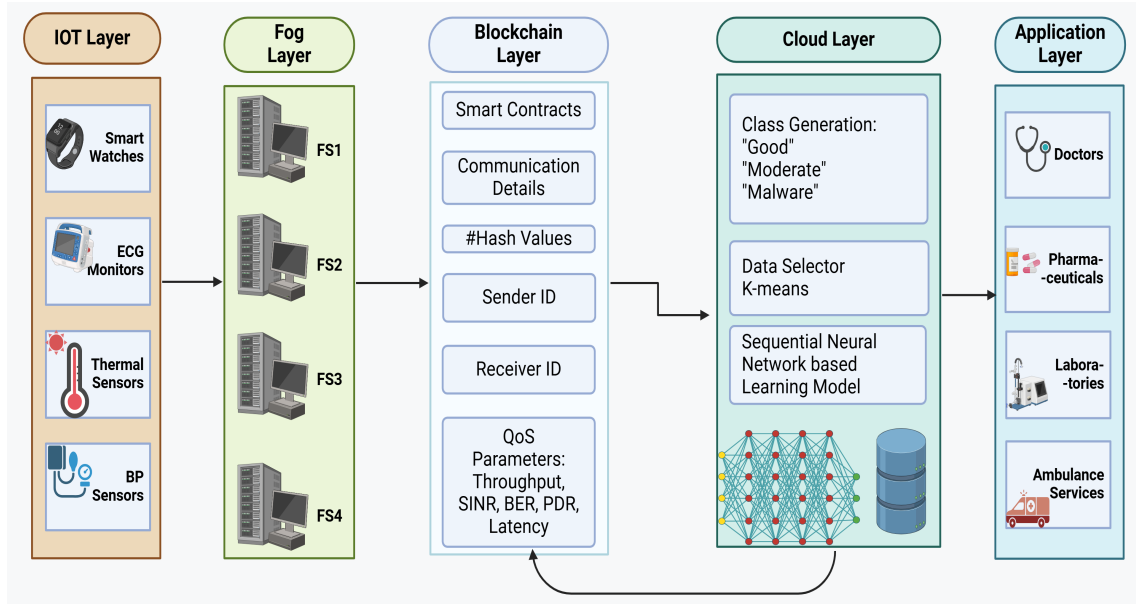


Figure 5.1: The Blockchain-based Smart Healthcare System Architecture

#### **5.1.1.1 IoT and Fog Layer**

The IoT layer incorporates the smart healthcare devices which gathers and transmits real-time patient data for analysis, diagnosis and monitoring. These IoT devices are very small in size and have very low storage and computation power. So, there is a need of such type of server which can manage the storage, provide better computation capabilities and helps in communication with other devices which is incorporated in the fog layer. The fog layer includes fog servers which helps to communicate various IoT devices with each other. These fog servers en-route the communicating devices to send data packets to the receiving node or device. Due to in near proximity of IoT network these fog servers helps to reduce latency and data transmission time across devices. For healthcare applications needing immediate actions and continuous data analysis, these servers allow real-time data processing for faster response. Fog computing provides localized storage to devices for faster response and processing, but it also sends important data to cloud for further processing and storage.

#### **5.1.1.2 Blockchain Layer**

The blockchain layer was used to record the transactions created by the user as well as the service layer. Blockchain is evolutionary technology which stores and verifies transactions automatically rather than processing manually. This makes it easier for industries to transact easily, Fastly and securely without need of a TTPs (Trusted Third Party). In blockchain every transaction committed is connected to the previous block with the help of hash, creating a chain of blocks. [176] The distributed and immutable blockchain ledger does not allow alterations to the data as any changes made will create different hash making it ideal for storing records securely. SHA-256 is one of the most popular cryptographic hashes used widely which is utilized in our blockchain [177]. Blockchain also verifies transactions using various consensus mechanisms like PoW, Paxos, Raft, pBFT which helps to maintain security and consistency without a central authority.

Google Firebase is used to store user data in the planned blockchain system. A variety of resources and services are available on Firebase, a cloud-based system for hosting applications. Cloud storage, identification, storing, and real-time information databases are just a few of the things it provides. Project configuration is required for the application to access Firebase services [178, 179]. The firebaseConfig object stores the setting information. The firebaseConfig object have

several properties like `storageBucket`, `appId`, `measurementId`, `apiKey`, `authDomain`, `databaseURL`, `projectId`. The specific values to these properties are particular to different Firebase Projects and helps to establish connection between Firebase services and applications [180, 181]. The pseudo-code outlines the process of creating and setting up the `firebaseConfig` object, which involves defining its properties and assigning appropriate values to each one.

(i) The following properties are used to initialize the `firebaseConfig` object:

- **apiKey:** The unique identifier for accessing Firebase services.
- **authDomain:** The domain that handles Firebase Authentication, allowing users to securely log in.
- **databaseURL:** The URL for Firebase’s real-time database, where blockchain-related data can be stored.
- **projectId:** The unique ID for the Firebase project, organizing resources within the Firebase platform.
- **storageBucket:** The Firebase cloud storage location, enabling secure storage of blockchain data files.
- **appId:** The unique identifier for the specific Firebase app, essential for initializing Firebase services.
- **measurementId:** The ID for Google Analytics, allowing tracking and analytics of app interactions, useful for monitoring blockchain interactions and usage.

(ii) The `apiKey` property value is set to “AIzaSyCeKT-ChcZr8BuYyZFWUM-nXiY71cirITdc”.

(iii) The `authDomain` property value is set to “rohitsdn-920e8.firebaseio.com”.

(iv) The `databaseURL` property value is set to “https://console.firebase.google.com/u/0/project/rohitsdn-920e8/storage/rohitsdn-920e8.appspot.com”.

(v) The `projectId` property value is set to “rohitsdn-920e8”.

(vi) The `storageBucket` property value is set to “rohitsdn-920e8.appspot.com”.

(vii) The `appId` property value is set to “1:955344448689:web:36eac17bf93a174X-XXXXXX”.

(viii) The `measurementId` property value is set to “G-D0LL9SXXXX”.

#### **5.1.1.3 Cloud Layer**

The cloud layer is the topmost layer of the proposed architecture. It plays important role in storing, managing and analysing data. The proposed system employs the K-means clustering algorithm to group the data, followed by a statistical analysis of the resulting clusters to assign class labels. Using a rulebase, we were able to categorize the gathered data as either Good, Moderate, or Malware. The data is further passed into a deep neural engine for ranking of transactions based on the scores generated. The Deep Neural Network (DNN) comprises of 5 fully connected layers utilizing a non-linear activation function to learn complex patterns easily namely ReLU. The utilization of DNN is done over Decision Trees (DT), Support Vector Machines (SVM) and Reinforcement Learning (RL) is due to its power to learn complex patterns, scalability, multi-class support, and efficient optimization. Since, SVM is a binary class classifier it is not best suited for the environment, DT and RL can be used for multi-class classification but DT overfits easily in a scalable environment and RL does not rely on training data and gains data through experience by interacting with the environment and is not well suited for non-sequential problems therefore increasing computational complexity. Hence, making DNN best for our system. This neural network than uses connected layers to train the feature dataset and to generate classification scores which helps to rank transactions based on their scores.

#### **5.1.1.4 Application Layer**

The Application Layer is the last and most critical interface within the proposed blockchain-integrated deep learning framework for smart healthcare communication networks. It is responsible for providing the end users including doctors, pharmaceutical companies, laboratories and ambulance services with analyzed, processed, and securely transmitted information so that they are able to make real-time decisions based on accurate information. This layer serves as the main point of interaction of the healthcare personnel with the data coming from the IoT devices like smartwatches, ECG monitors, thermal sensors, and blood pressure monitors. After passing the fog layer for preliminary processing, the blockchain layer for security validation, and the cloud layer for intelligent deep classification via a deep neural network, the application layer grants role-based access to pertinent users.

The application layer enhances collaborative decision-making across the health-

Table 5.1: Adversarial Model for Proposed System

| Aspect                     | Description                                                                                                                                | Significance in Proposed Work                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Model               | Adversary can observe QoS metadata but lacks cryptographic keys; it aims to misclassify traffic, disrupt consensus, or infer private data. | Establishes realistic assumptions for evaluating system robustness.                                                                        |
| Sybil/51% Collusion Attack | Injection of multiple false IoT identities and collusion of validators to disrupt PBFT operations.                                         | Tests authentication via polynomial curve fitting and validates the resilience of consensus under collusion in the healthcare IoT context. |
| Privacy Inference          | Traffic pattern analysis to deduce healthcare usage.                                                                                       | Validates confidentiality mechanisms using encryption and hashing.                                                                         |
| Defence & Metrics          | Curve-fitting authentication, PBFT consensus, adversarial training, encryption; evaluated by accuracy, TDR, FDR, latency, throughput.      | Ensures comprehensive assessment of both security and performance.                                                                         |

care ecosystem which ultimately leads to better outcomes and more efficient healthcare management. Moreover, it also provides low latency service delivery and enables real-time collaboration across the healthcare ecosystem. Therefore, by classifying, validating, and securing the data, the system eliminates misinformation, data delays, and tampering problems that are prominent in traditional IoT healthcare networks.

### 5.1.2 Adversarial Model

The adversarial model is designed to identify potential threats, and associated defences are outlined to evaluate the robustness of the blockchain-DNN framework. It outlines potential attack scenarios and their mitigation techniques, supporting secure, privacy-preserving, and efficient operation within healthcare IoT environments [150, 174]. The detailed outline of these threats and defences is summarized in Table 5.1.

### 5.1.3 Proposed Methodology

The smart healthcare IoT devices are deployed which are communicating data via Fog servers and are authenticated using a 2nd degree polynomial curve. Curve fitting is used to compute polynomial signature and if  $P_i(x, y)$  matches the expected pattern then device is mark as authenticated as shown in Algorithm 5.1.4. The polynomial curve fitting guarantees that only nodes with coherent  $(x, y)$  coordinates and valid keys are permitted leveraging a light-weight cryptography to verify nodes [43]. If the node is authentic, apply Rayleigh and Rician fading models to simulate real-world wireless communication conditions. After starting the IoT communication through both the channels the QoS parameters are then calculated for the fading channels including throughput, PDR, BER, SINR, Latency. For Every authenticated device the communication is done using Fog nodes and the performance metrics are stored. The information is subsequently added to the Firebase blockchain, which creates a secure record by aggregating the data. Statistical analysis and K-means clustering are then used to create three clusters. The selection of three clusters was supported by the literature review [43], which showed that similar studies often used this number to classify network traffic into Good, Moderate, and Malware categories. However, K-means cannot classify clusters as Good, Moderate, or Malware due to its unsupervised nature. For that standard deviation of Each cluster will then be evaluated based on how close its points are to the cluster center C, which helps determine the “efficiency” of the cluster as shown in Algorithm 5.1.4. After that a deep neural engine is used to train the feature dataset X and classification scores are generated. These scores are than assigned to the source and terminal nodes. After the assignment of scores, average score from all occurrences as either source or terminal is calculated. This classification score helps blockchain system to identify consistently performing nodes and reduce security risks. Figure 5.2 shows the workflow of the system.

### 5.1.4 Proposed Algorithms

This section proposes algorithms for a blockchain-based, node authentication and secure data transmission protocol for IoT applications. Algorithm 5.1.4 shows the Use of Polynomial curve fitting and Fading Channels for secure IoT communication, while Algorithm 5.1.4 shows the IoT Node Ranking Based on QoS Metrics Using Clustering and DNN.

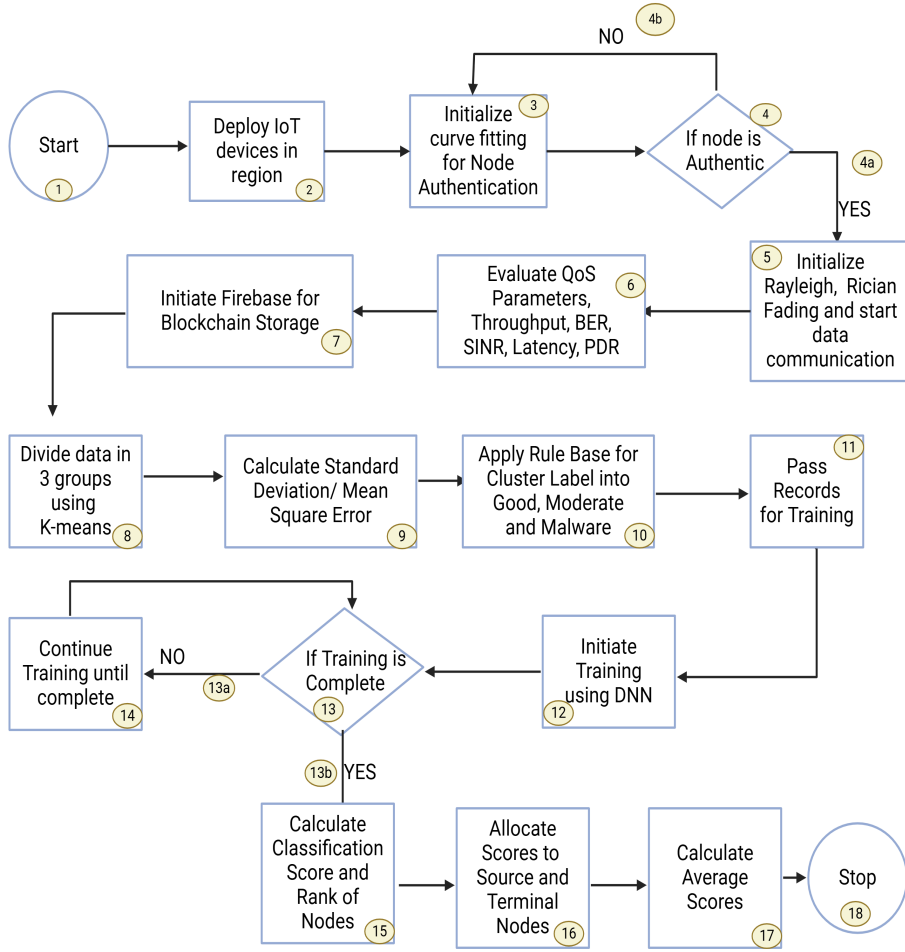


Figure 5.2: Flowchart for the Proposed Model

**Algorithm 3:** Secure IoT Communication via Polynomial Curve Fitting and Fading Channels

**Require:** Deployment area  $A$ , fog nodes  $(f_1, f_2, \dots, f_n)$ , polynomial coefficients

$\alpha_i, \beta_i$

**Ensure:** Secure communication parameters for each verified IoT device

**1. Initialize Parameters:** Define deployment area  $A$  and set up fog nodes. Initialize polynomial coefficients for curve fitting.

**2. Deploy IoT Devices Randomly:**

**for** each IoT device  $d_i$  **do**

Assign random coordinates  $(x_i, y_i)$  within  $A$ ; Generate node key  $k_i$

**end for**

**3. Verification Using Polynomial Curve Fitting:**

**for** each device  $d_i$  attempting communication **do**

Compute polynomial signature  $P_i(x, y)$ :

$$P_i(x, y) = \sum_{j=0}^n \alpha_j x^j + \sum_{j=0}^m \beta_j y^j + k_i$$

**if**  $P_i(x, y)$  matches expected pattern **then**

    Mark device as authenticated

**else**

    Deny access

**end if**

**end for**

#### 4. Channel Selection and Communication:

**if** device  $d_i$  is authenticated **then**

    Choose channel: Rayleigh or Rician fading model with line-of-sight  $K$

**end if**

#### 5. Evaluate Performance Metrics for Fading Channels:

**for** each fading channel **do**

    Calculate **Throughput**:

$$\text{Throughput} = B \cdot \log_2(1 + \text{SINR})$$

    Evaluate **BER**:

$$\text{BER}_{\text{Rayleigh}} = Q\left(\sqrt{\frac{2 \cdot \text{SINR}}{1 + \text{SINR}}}\right), \quad \text{BER}_{\text{Rician}} = Q\left(\sqrt{\frac{2 \cdot K \cdot \text{SINR}}{1 + \text{SINR}}}\right)$$

    Calculate **SINR**:

$$\text{SINR} = \frac{P_{\text{signal}}}{P_{\text{interference}} + P_{\text{noise}}}$$

    Measure **Latency**:

$$\text{Latency} = \frac{1}{\text{Throughput}}$$

    Calculate **PDR**:

$$\text{PDR} = 1 - \text{BER}$$

**end for**

#### 6. Route Communication via Fog Nodes:

**for** each authenticated device  $d_i$  **do**

    Route communication through nearest fog node  $f_j$ ; Collect performance metrics

**end for**

---

**Algorithm 4:** IoT Node Ranking Based on QoS Metrics Using Clustering and DNN

**Input:** Network dataset `rohitmaliknetwork.route_info` with QoS metrics: Throughput, BER, SINR, Latency, and PDR.

**Output:** Ranked nodes based on QoS performance.

**1. Collect QoS Data:**

**for** each route  $i$  in `rohitmaliknetwork.route_info` **do**

    Extract QoS parameters: `Throughput(i)`, `BER(i)`, `SINR(i)`, `Latency(i)`, `PDR(i)`

**end for**

**2. Combine Data into Matrix:**

Construct data matrix `data` = [`Throughput`, `BER`, `SINR`, `Latency`, `PDR`].

**3. Standardize Data:**

Apply z-score standardization: `data_scaled` = `zscore(data)`.

**4. Apply k-Means Clustering:**

Set the number of clusters,  $k = 3$ .

Apply k-means:  $(\text{idx}, \mathbf{C}) = \text{kmeans}(\text{data\_scaled}, k)$ , where `idx` represents cluster assignments and `C` are cluster centroids.

**5. Evaluate Cluster Standard Deviations:**

**for** each cluster  $j = 1$  to  $k$  **do**

    Extract points in cluster  $j$ : `cluster_points` = `data_scaled[idx == j, :]`.

    Calculate distances to centroid `C[j]`:

`distances` =  $\sqrt{\sum(\text{cluster\_points} - \mathbf{C}[j])^2}$ .

    Compute standard deviation: `cluster_std[j]` = `std(distances)`.

**end for**

**6. Assign Cluster Labels:**

Identify clusters with the highest and lowest standard deviations.

Label clusters as follows:

- "Highly Efficient" for the cluster with the lowest standard deviation.
- "Efficient" for the intermediate standard deviation cluster.
- "Malware/Not Efficient" for the cluster with the highest standard deviation.

**7. Prepare Training Data for DNN:**

Map each cluster label to a numeric value: "Malware/Not Efficient" = 1, "Efficient" = 2, "Highly Efficient" = 3.

Construct feature matrix  $\mathbf{X} = \text{data\_scaled}^T$  and labels  $\mathbf{Y}$ .

#### 8. Define and Train DNN Model:

Define DNN architecture:

- Input layer (5 features)
- Fully connected layer (128 neurons)
- ReLU activation layer
- Fully connected layer (64 neurons)
- ReLU activation layer
- Fully connected layer (32 neurons)
- ReLU activation layer
- Fully connected layer (3 neurons)
- Softmax layer
- Classification layer

Train DNN with  $\mathbf{X}$  and  $\mathbf{Y}$ .

#### 9. Predict Scores with DNN:

**for** each record  $i$  in  $\mathbf{X}$  **do**

    Predict class score  $\text{scores}(i)$  for each record using DNN.

    Calculate final score:  $\text{final\_scores}(i) = 100 - \left| \frac{\text{predicted\_score} - \text{actual\_label}}{\text{actual\_label}} \right| \times 100$ .

**end for**

#### 10. Allocate Scores to Source and Terminal Nodes:

**for** each route  $i$  **do**

    Allocate half of  $\text{final\_scores}(i)$  to the source node and half to the terminal node.

**end for**

#### 11. Compute Average Node Scores:

**for** each unique node **do**

    Calculate the average score from all occurrences as either source or terminal.

**end for**

---

### 5.1.5 Performance Metrics

In this section, we analyze the performance of the proposed model ensuring system's security, reliability, robustness and efficiency using the following evaluation

parameters:

**Throughput:** This refers to the successful delivery of data packets over the communication network within a given time frame. Higher throughput indicates better network performance and efficient utilization of resources.

$$Throughput = B \cdot \log_2(1 + SINR)$$

**BER:** It indicates the percentage of bits that were incorrectly received out of the total number of bits transmitted during a specified time interval. A lower BER signifies more reliable communication, which is especially critical in environments with high interference or mobility.

$$BER_{Rayleigh} = Q\sqrt{\frac{2 \cdot SINR}{1 + SINR}}, BER_{Rician} = Q\sqrt{\frac{2 \cdot K \cdot SINR}{1 + SINR}}$$

**SINR:** SINR measures the quality of a wireless communication link, considering both the signal strength and the interference/noise present. Higher SINR values indicate better link quality and increased probability of successful data reception.

$$SINR = \frac{P_{signal}}{P_{interference} + P_{noise}}$$

**Latency:** Latency is the amount of time it takes for a data packet to be transmitted from the source to its destination. Lower latency is essential for time-sensitive applications and reflects the network's responsiveness.

$$Latency = \frac{1}{Throughput}$$

**PDR:** It represents the fraction of data packets successfully received by the destination relative to the total packets transmitted. A high PDR reflects the effectiveness of the routing and transmission mechanisms under different network conditions.

$$PDR = 1 - BER$$

**TDR and FDR:** TDR measures the proportion of actual positive cases that are correctly identified by the system and FDR refers to measure of proportion of actual negative cases that are correctly identified by system.

$$TDR = \frac{TP}{TP + FN}, FDR = 1 - TDR$$

TP (True Positive): Number of correctly detected malware samples  
FN (False Negative): Number of malware samples incorrectly classified as benign

## 5.2 Experimental Study

This section is divided into three sub-sections. The experimental setup outlines the simulation platform, environment and tools used to conduct the experiments and the results and discussion section analyses the findings from the simulations and after that the observations are presented.

### 5.2.1 Experimental Setup

Matlab Simulation and Google Colab are used to create the suggested intelligent healthcare network system. Quality of Service (QoS) and several quantitative factors such as throughput, BER, PDR, SINR and latency are also evaluated using a blockchain database. This was achieved by running simulations using the given system model and collecting data for each one: PDR, SINR, Latency, Throughput, and BER. The dataset is generated randomly and with around 10000 entries of the QoS parameters. The data is generated randomly every time the simulations are performed, and for training and testing purpose a 70-30 split was done. This data was than subsequently fed into the deep neural learning mechanism. The model training process took approximately 1 day using an i5 CPU and 4 cores GPU. Once model is trained, inference and decision-making operations occur in the order of nanoseconds. Since all subsequent computations are based on the output of this classification step, the overall computational overhead during real-time operation is minimal. The neural learning mechanism than generates classification scores and ranks the transactions as “Good”, “Moderate” or “Malware”. The specifications of the proposed system with reference to blockchain, fog nodes, number of communicating IoT nodes, the system model specifications and system used are stated in Table 2 while the details of parameters and hyperparameters related to DNN [182] are discussed in Table 3.

Table 5.2: System Specifications and Ordinal Measures of System Model

| System Specifications    |                                     |
|--------------------------|-------------------------------------|
| RAM                      | 16GB                                |
| Processor                | i5 8350U CPU @ 1.70 GHz<br>(8 CPUs) |
| Memory Type              | DDR4                                |
| SSD Capacity, Type       | 1TB, NVMe                           |
| System Model Information |                                     |

|                          |                                     |
|--------------------------|-------------------------------------|
| Blockchain Type          | Hyperledger                         |
| No. of Nodes             | 50-500                              |
| No. of Fog Nodes         | 4                                   |
| No. of Packets           | 1000                                |
| Packet Size              | 1500*8 (bytes)                      |
| Transmission Power       | 20 dBm                              |
| Noise Power              | -90 dBm                             |
| Bandwidth                | 20*106 Hz                           |
| Authentication Threshold | 500                                 |
| K-Factor (Rician)        | 10                                  |
| Channel of Communication | Rayleigh channel, Rician Channel    |
| Simulation Area          | 1000 $m^2$                          |
| Evaluation Parameters    | Throughput, PDR, Latency, BER, SINR |

Table 5.3: Parameters and Hyperparameters of Deep Neural Network used

|                                    |               |
|------------------------------------|---------------|
| <b>Hidden Layers</b>               | 3             |
| <b>Neurons in Hidden Layers</b>    | [128, 64, 32] |
| <b>Activation Function</b>         | ReLU          |
| <b>Output Layers</b>               | 3 (Classes)   |
| <b>Output Activation Functions</b> | SoftMax       |
| <b>Loss Function</b>               | Cross-Entropy |
| <b>Optimizer</b>                   | Adam          |
| <b>Initial Learning Rate</b>       | 0.001         |
| <b>Maximum Epochs</b>              | 100           |
| <b>Mini-Batch Size</b>             | 32            |

## 5.2.2 Results and Analysis

This section describes the analysis of the results based on various parameters like Throughput, PDR, SINR, BER, Latency, TDR, and FDR, and also includes a comparative study of the proposed framework with existing studies.

### 5.2.2.1 Comparative Study

A comparison of the studies in the referenced table has been conducted to highlight the key points. The main goal across all methods has been to provide secure dis-

tributed access to data while maintaining confidentiality and data integrity. Most reviewed works offer some level of decentralized access and aim to ensure a degree of integrity and privacy, which are essential for secure information management. Scalability is not consistently addressed; some studies demonstrate only moderate ability for larger deployments. The proposed framework is unique because it leverages machine learning for data classification, a feature not consistently present in previous studies. It also achieves high scalability and operational efficiency, overcoming limitations found in related work. This combination of secure decentralized access, focus on integrity and privacy, and advanced classification makes the proposed solution more comprehensive and effective than earlier approaches, as shown in Table 5.4.

Table 5.4: Comparative Analysis of Proposed Framework with Related Studies

| <b>Parameter / Feature</b> | <b>Menon et al., 2023 [43]</b> | <b>Sharma et al., 2022 [13]</b> | <b>Moghadasi &amp; Masdari, 2024 [24]</b> | <b>Khan et al., 2024 [26]</b> | <b>Malik et al., 2025 [150]</b> | <b>Proposed</b> |
|----------------------------|--------------------------------|---------------------------------|-------------------------------------------|-------------------------------|---------------------------------|-----------------|
| Throughput                 | Moderate                       | Low                             | High                                      | High                          | Low                             | High            |
| BER                        | Moderate                       | High                            | Moderate                                  | Moderate                      | High                            | Low             |
| Latency                    | Moderate                       | Moderate                        | Low                                       | Low                           | Moderate                        | Low             |
| SINR                       | Low                            | Low                             | Moderate                                  | Moderate                      | Low                             | High            |
| Scalability                | Moderate                       | Moderate                        | Low                                       | High                          | High                            | Very High       |
| Decentralized Access       | Yes                            | Yes                             | Yes                                       | Yes                           | Yes                             | Yes             |
| Data Integrity             | Yes                            | Yes                             | Yes                                       | Yes                           | Yes                             | Yes             |
| Data Privacy               | Yes                            | Yes                             | Yes                                       | Yes                           | Yes                             | Yes             |
| AI-based Classification    | Yes (Neural Engine)            | No                              | Yes (DRL)                                 | Yes (AI-based NN)             | Yes (RNN)                       | Yes (DNN)       |

The QoS parameters are collected and compared with Subhita et. al [43], Pratima et. al [13], and Burhan et. al [26] to check the feasibility of the developed system model. The performance of the proposed approach is evaluated and compared against existing methods. Fig. 5.3 presents the throughput of the proposed model, which quantifies the number of transactions processed by the system within a specified time period, and is evaluated with existing research.

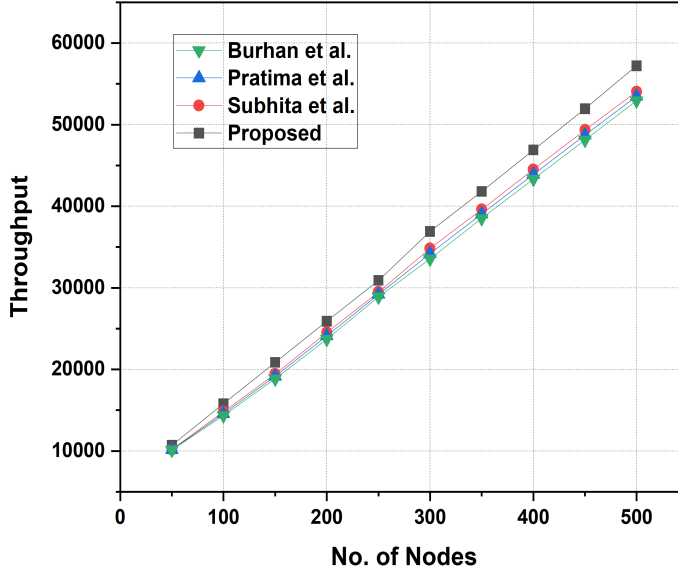


Figure 5.3: Throughput Comparison of the Proposed System with Other Related Works

The proposed model produced 5.34%, 7.07% and 7.86% more throughput than [43], [13], and [26], respectively. The proposed work's throughput significantly grows with an increasing number of nodes.

Then, using BER which quantifies the rate of errors in transmitted bits, as illustrated in Figure 5.4, the effectiveness of the suggested works is examined. The proposed system performed 9.83%, 11.64% and 16.53% lower than [43], [13] and [26] respectively, signifying the smaller number of errors occurred. The proposed model performed significantly better as the number of nodes increases.

Figure 5.5 presents the comparison of PDR of the suggested work with the previous related works. The proposed system's packet delay rate is found 0.3%, 0.57% and 0.8% better than [43], [13] and [26] respectively.

Figure 5.6 presents the SINR, which helps to identify the quality of the received signal relative to interference and noise. The proposed model performed significantly better than the compared related works. It performed 3.16%, 4.33% and 5.15% better than [43], [13], and [26], respectively. The significant increase in SINR leads to fewer errors, greater performance, and ensures reliable data transmission.

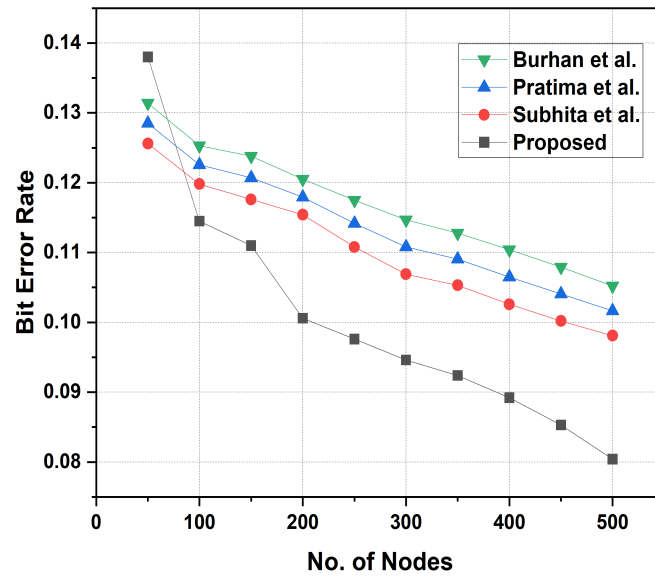


Figure 5.4: Comparison of BER of Proposed System with Other Related Works

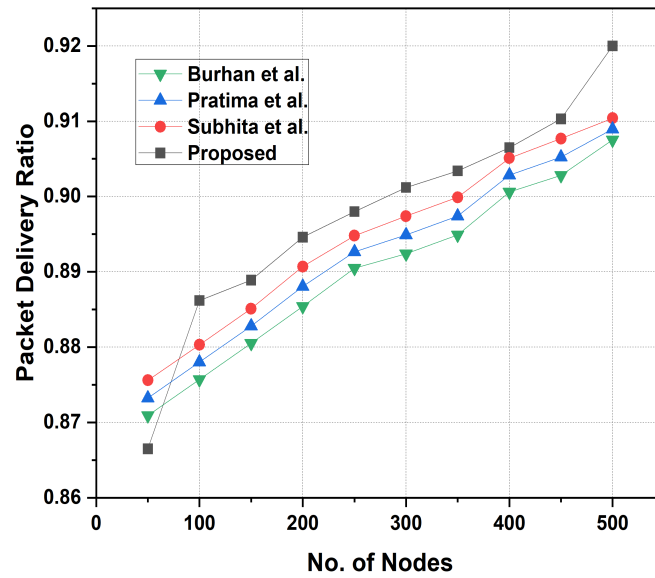


Figure 5.5: PDR Comparison of the Proposed System with Other Related Works

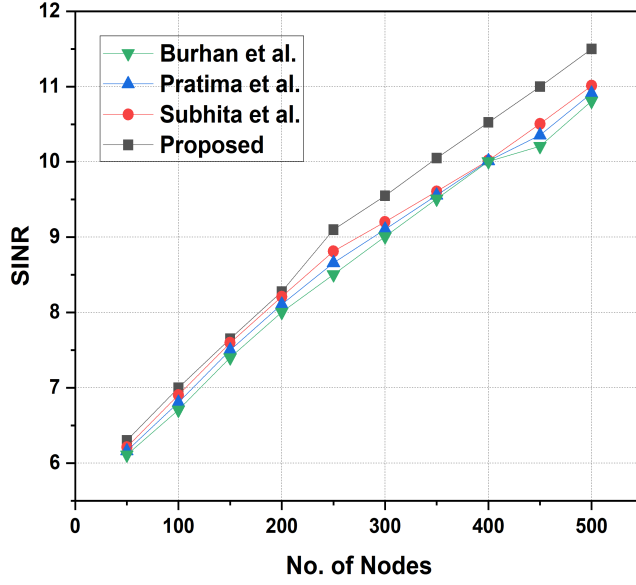


Figure 5.6: Comparison of SINR of Proposed System with Other Related Works

Figure 5.7 presents the Latency of the system which indicates the time delay in data transmission. By 4.19% compared to [43], 3.02% compared to [13] and 2.05% compared to [26], the suggested work reduced latency compared to the current systems. Hence, when contrasted with current methods, the suggested strategy provides a stronger solution to healthcare records management.

Also, To address concerns regarding blockchain-specific vulnerabilities such as Sybil attacks, 51% attacks, and privacy risks in smart healthcare environments, the proposed framework leverages a DNN-driven classification mechanism that achieves a high TDR ranging from 90.15% to 95.00% and a correspondingly low FDR ranging from 9.85% to 5.00% across varying network sizes (50 to 500 nodes) as shown in Fig. 5.8. This indicates the system's strong capability to correctly identify malicious behaviours and anomalous node activities, which is critical in defending against Sybil and 51% attacks. Furthermore, the integration of intelligent rule-based labelling not only supports adaptive trust management but also strengthens resistance to multi-node collusion attacks.

As the network's unit and operations counts rise, the computing complexity also rises sharply. Moreover, in a PoW blockchain consensus [43], the mining process requires substantial computational resources, posing challenges for IoT devices with limited capabilities. Therefore, a comparison of PoW, Raft, Paxos and

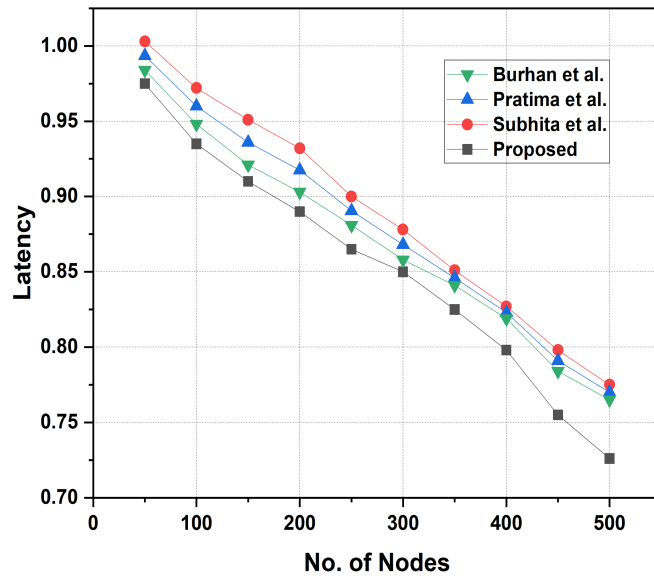


Figure 5.7: Analysis of the Suggested System's Latency in Relation to Previous Research

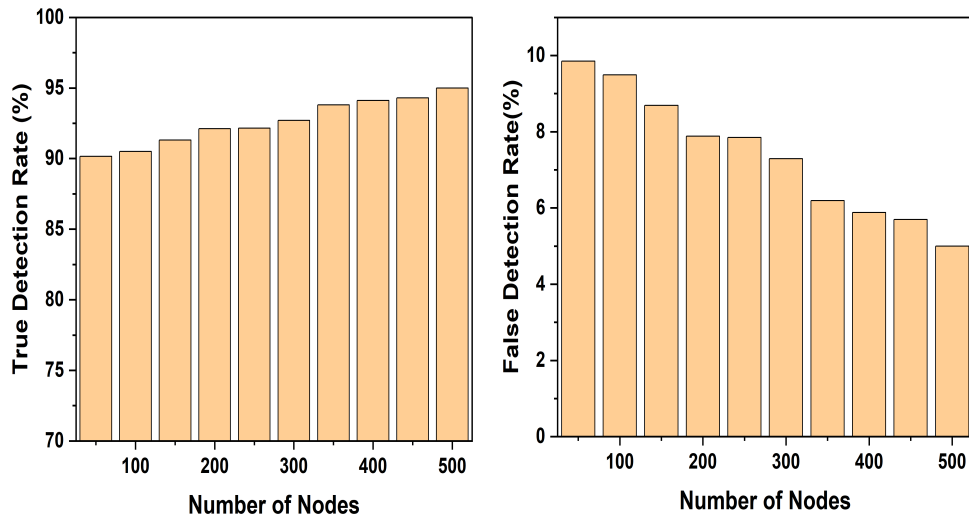


Figure 5.8: Analysis of TDR and FDR with respect to the Increasing Number of Nodes

pBFT consensus mechanisms is done as in a Firebase-based blockchain application this can offer valuable insights into performance, reliability, and application-specific suitability. In Fig. 5.9 a pictorial comparison is done which indicates that pBFT mechanism performs better than PoW, Raft and Paxos. pBFT took 0.0015 seconds PoW took 1333.2127 seconds, Raft took 0.0028 seconds and Paxos took 0.0087 seconds to complete the consensus. pBFT outperformed all other consensus mechanisms as in PoW the process of mining can be very computationally intensive, Paxos designed for general distributed systems performs better in a permissionless environment and can still consume significant resources in our permissioned blockchain and Raft relies on leader election and log replication can create delays resulting in increased latency posing a challenge for resource-constrained IoT devices, which signifies that the Firebase-based blockchain application values security, fault tolerance, and deterministic consensus in a permissioned environment, with a need for low-latency and energy-efficient operations. This comparison ensures that the chosen mechanism aligns with the application's specific technical and operational requirements.

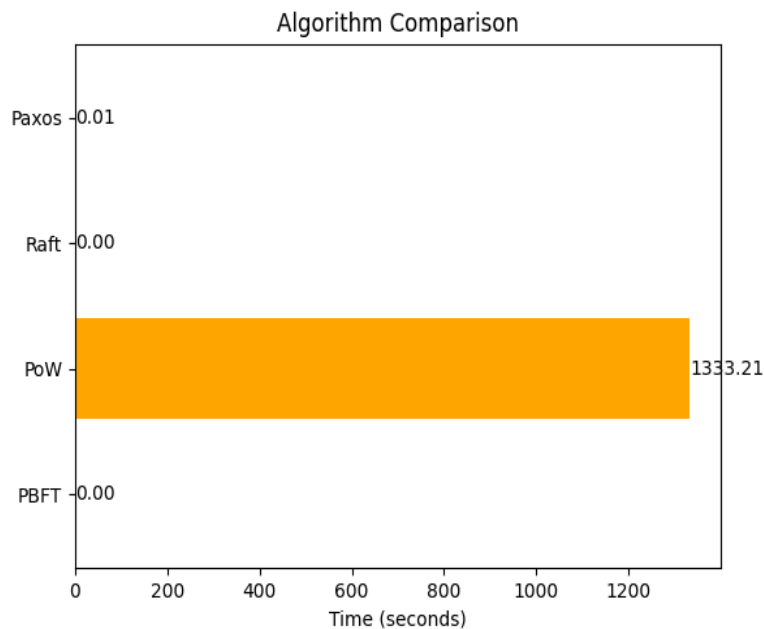


Figure 5.9: Comparison of Various Blockchain Consensus Mechanisms

### 5.2.2.2 Observations

During the comparison of all parameters that are discussed above, it is found that [26] performs worst in all test cases because the framework uses the metaheuristic optimized neural networks. Due to this, the processing times increased and affected the latency and throughput. The system is unable to reduce the delay while managing transactions in high-density networks, and that affects the PDR and latency. This system utilizes an Ethereum-based blockchain, which enhances system security and increases propagation delays, resulting in higher BER and lower throughput in concurrent access scenarios. [13] performs better than [26] because it uses Ciphertext Policy Attribute-Based Encryption that allows for fast, targeted access without any heavy cryptographic operations per transaction, and this improves the throughput and latency. This system deploys real-time user revocation and maintains the access security without slowing down system response which helps to provide a better PDR and latency. But this system lacks a neural network mechanism, leading to non-adaptive performance, so it is not able to give the best possible solution for these given parameters.

The [43] performs better than [13]. [43] uses the integration of the Dragonfly algorithm for intelligent data filtering and a neural network for lightweight classification, which helps reduce computational overhead and latency and enhance the throughput of the system. The layered mechanism makes it a distributed system, and that helps improve the PDR. The proposed architecture is efficient but does not support the scalability and reliability of the system. The system uses a distributed architecture but lacks a layered neural network to enhance efficiency. Additionally, its use of a lightweight blockchain for login and logout compromises security.

The proposed model learns complex non-linear relationships and temporal patterns using historical data of key QoS parameters like throughput, BER, PDR, SINR, and latency. The training ensures more accurate predictive resource allocation by the DNN relative to the diverse operating conditions within the network. Improved DNN learning translates into better resource management strategies such as optimal channel utilization, which simultaneously improves Throughput and reduces BER. Generalization of the model over noisy channels like Rayleigh and Rician helps in recognizing and mitigating repetitive error-prone patterns enabling more robust error control. PDR is further enhanced by the model's ability to predict stable transmission intervals as well as period of packet minimization during adverse conditions, which is especially useful for dynamic channel

circumstances. Enhanced system predictability improves the SINR by smartly distinguishing between signal versus interference drawing from prior instances to improve signals. The dynamically determined rerouting and rescheduling of the DNN minimizes queuing delays thereby improving latency. The incorporation of polynomial curve fitting techniques for authenticated devices lowers network contention and enhances the determinism while operating attacks.

Also, to reduce the computational complexity of the system no security at intermediate level is provided, only the security being generated by blockchains encryption is there. To reduce the computation overhead inside the blockchain system a comparison of various consensus mechanisms is done to check which consensus algorithm among pBFT, Raft, Paxos and PoW best fits the proposed environment. pBFT does not require intensive cryptographic puzzles but instead relies on message exchanges between nodes to reach consensus, significantly reducing computational demands while still providing strong fault tolerance and resistance against malicious nodes. This balance allows IoT devices to participate in a secure and decentralized framework without exhausting their limited resources.

### 5.2.2.3 Discussion

The proposed system demonstrates its novelty through the integration of blockchain technology with deep learning in a healthcare-specific five-layer architecture consisting of the IoT layer, fog layer, blockchain layer, cloud layer, and application layer. Unlike conventional approaches that focus only on security or data storage, the presented framework combines secure communication, intelligent transaction classification, and QoS-aware optimization within a single model. The fog layer reduces latency by processing data closer to IoT devices and supports communication through Rician and Rayleigh channels, while the blockchain layer ensures secure authentication, decentralized ledger generation, and transaction integrity using Hyperledger. The cloud layer performs data evaluation and classifies transactions into Good, Moderate, and Malware categories using a Deep Neural Network, improving decision-making and threat detection. The authentication of dynamic IoT nodes is strengthened through a curve-fitting verification mechanism before allowing blockchain participation, thereby reducing malicious access and false authentication. Important QoS parameters such as latency, BER, SINR, PDR, throughput, TDR, and FDR are integrated to evaluate both security and communication efficiency simultaneously. Hyperledger was selected due

to its permissioned architecture, lower latency, privacy preservation, and better suitability for healthcare communication systems, while Firebase supports real-time cloud synchronization and efficient transaction handling during simulation. Since the work is validated in a controlled simulation environment, practical deployment challenges such as large-scale communication bottlenecks and industrial implementation remain part of future work.

### 5.3 Summary of Context

A blockchain-integrated deep learning framework designed to improve the security of intelligent healthcare communication networks. The architecture is organized into five layers: IoT, Fog, Blockchain, Cloud, and Application, each serving a specific role in ensuring secure, efficient, and real-time healthcare data management. IoT devices gather patient information, while fog servers provide localized computation to reduce latency. The blockchain layer secures transactions with unalterable records and consensus mechanisms, and the cloud layer uses clustering and deep neural networks for data classification and ranking. The application layer delivers processed and validated information to end users such as doctors and healthcare providers.

An adversarial model is introduced to identify potential threats, including Sybil and privacy inference attacks, along with corresponding defenses such as polynomial curve fitting and consensus validation. The methodology combines lightweight cryptographic authentication, clustering, and neural classification to balance efficiency and robustness. Comparative studies show that the framework enhances throughput, decreases latency, and improves error control compared to existing methods. The chapter also offers insights on consensus mechanisms, highlighting pBFT as the most effective for resource-limited IoT healthcare systems. Overall, the discussion emphasizes how integrating blockchain, fog, and deep learning can tackle ongoing challenges in secure and scalable healthcare communication networks.

\*\*\*\*\*

## Chapter 6

# Conclusion and Future Scope

IoT is an innovative technology that enables devices to interact and work with applications such as smart health care, industrial automation, and intelligent transport systems. Smart devices, automated factories, and intelligent vehicle systems are good examples of IoT applied in real life. While IoT systems and devices continue to evolve and integrate with new advancements, they face numerous challenges, such as real-time resource limitations, poor visibility of devices, and the persistent threat of cyber attacks. Issues like distrust, data breaches, hacking, and the lack of robust peripheral devices have caused IoT systems to become patchy in structure and workflow. Blockchain technology provides a unique solution with its distributed ledger, which ensures data integrity, immutability, and transparency of system processes within the IoT framework. Thanks to its distinctive consensus approach, blockchain offers a peaceful and secure environment for mechanisms lacking strong central governance. As a result, IoT and blockchain are closely linked, each supporting the other's operation. Additionally, blockchain enhances device identity authentication, ensures data sharing confidentiality, and allows unobstructed access to resources, making it ideal for large-scale IoT systems where sensitive data is regularly accessed.

To verify the proposed trust and resilience of IoT and blockchain integration, comprehensive simulations were conducted using Python and MATLAB. These studies varied device density, communication range, and transaction complexity to assess system performance and optimisation efficiency. Results demonstrated improved security and throughput with minimal latency, resource use, and vulnerability to attacks, which are clearly acceptable. This confirms that the results are effective and the framework is scalable, offering a resilient solution to the demands future IoT ecosystems will present.

## 6.1 Conclusion

Chapter 1 of this thesis outlines and defines the IoT paradigm, which connects billions of devices for data collection, sharing, and processing across various domains such as healthcare, transport, and smart cities. IoT offers real-time services but also introduces challenges due to its highly distributed architecture, resource-limited devices, and security vulnerabilities. To address these issues, blockchain technology is adopted and extended as a complementary tool to IoT, providing data integrity, transparency, and trust through its distributed ledger and consensus mechanisms. The integration of blockchain and IoT creates a hybrid environment that enhances security, authentication, and reliable data sharing among devices. However, this integration also presents significant challenges, including blockchain system scalability, computational and storage limitations, and latency issues on resource-constrained IoT devices. This chapter highlights the importance of tackling these challenges to fully realise the potential of combined blockchain-IoT systems and serves as a foundation for further research into efficient, secure, and scalable systems for the future IoT-enabled environment.

This chapter reviews existing research on blockchain integrated with IoT systems and highlights achievements in the field. It explains how blockchain has been proposed as a solution to address IoT challenges, particularly regarding data security, transparency, and trust in socio-technical gaps. The reviewed literature is organised into four main areas of blockchain-IoT integration: security and privacy, scalability, consensus mechanisms, and resource management. The chapter also stresses the importance of blockchain in enhancing IoT architecture through decentralised authentication and data sharing, secure data storage, and immutable records, while also recognising the challenges of implementing resource-intensive blockchain processes on resource-constrained IoT devices. It underscores the necessity for seamless architecture-level integration between blockchain platforms and IoT infrastructures to facilitate smooth interoperation and improve overall effectiveness. Critical evaluation shows a lack of comprehensive models for scalable, resource-efficient blockchain-centric IoT systems. This highlights the need to develop security-preserving frameworks within optimised models to meet the diverse performance requirements of real-world IoT systems.

In Chapter 3, a novel hybrid optimisation method is introduced to improve resource allocation and security in blockchain-based IoT applications. To enhance decision-making regarding resource allocation, security, latency, and other metrics within IoT ecosystems, the proposed optimisation model, Hybrid ABC-WOA, is

developed. The hybrid model merges the exploration ability of the ABC algorithm with the exploitation strength of WOA to optimise task scheduling and secure data management. Data with specific computational and security needs are allocated for resource selection, aiming to minimise trust issues, processing time, energy consumption, and overall system efficiency. This flexibility enables effective parallel execution, addresses task imbalance, and boosts resilience against malicious attacks through resource and demand-driven allocation.

The Hybrid ABC-WOA model was evaluated utilising key performance indicators including time delay, energy consumption, resource utilization, and security overhead. The experimental results demonstrated that the proposed model markedly surpassed individual ABC and WOA approaches. Comparative analyses with baseline algorithms verified the consistent superiority of the hybrid methodology across different task sizes and workloads. These findings underscore the model's potential as a viable solution for secure task scheduling, energy-efficient resource management, and blockchain-enabled trust management within IoT-based environments.

Chapter 4 introduces a novel method for node authentication to secure data transmissions in IoT healthcare environments using blockchain. The proposed system employs Hyperledger Fabric, RNN, and homomorphic encryption to process, store, and classify EHRs securely and efficiently. The model is organised into multiple layers, including the application, authentication, blockchain, and cloud layers, each playing a vital role in ensuring end-to-end security and effective data management. Access control is handled through a challenge-response authentication system that combines hashing and digital signatures, protecting the system from unauthorised access and malicious devices. Once authenticated, encrypted data is processed within the blockchain layer, while RNN is used at the cloud layer for accurate classification and anomaly detection.

The proposed framework still faces typical IoT systems challenges, such as ensuring data privacy, addressing authentication gaps, and reducing latency. Integrating blockchain with homomorphic encryption provides secure communication, enabling unalterable computations on encrypted data. RNN enhances the architecture and boosts the overall anomaly detection accuracy to 99.01%, ensuring effective capture of abnormal data flow behaviours. Compared to existing schemes like MKP-ABE, RSA, and ECC, the proposed method offers greater accuracy, lower latency, and improved security. This demonstrates that the framework remains suitable for IoT applications in healthcare, as it effectively balances load, maintains data confidentiality, and enhances resilience against cyber threats.

Chapter 5 discusses the design and evaluation of a blockchain-integrated deep learning system aimed at safeguarding communication privacy within smart health IoT networks. The model features a multi-layered setup that includes an IoT layer, fog layer, blockchain layer, cloud layer, and application layer. In the IoT and fog layers, devices create and send real-time healthcare data, which is processed locally to minimise latency and bandwidth use. The blockchain cloud layer hosts the DNN that categorises transactions with blocks as Good, Moderate, and Malware, while also ensuring secure transaction logging through tamper-proof storage; the blockchains verify via cryptographic hashes and consensus mechanisms. This configuration enhances trust, resilience, and efficiency in healthcare communication by guaranteeing secure data management and quicker response times. The proposed framework, with its seamless integration of blockchains and neural networks, boosts defence systems by improving classification accuracy and data processing for critical medical applications.

The proposed system has been implemented on MATLAB and Google Colab, with its performance tested on IoT networks of various sizes from 50 to 500 devices. The evaluation of QoS parameters included throughput, packet delivery ratio (PDR), SINR, latency, and BER. The results show that the framework outperformed other studies in the literature in terms of throughput (by 5.34%), BER (by up to 16.53%), latency, PDR (by 0.8%), and other parameters. Additionally, the deep neural engine demonstrated high accuracy, with low false detection rates and true detection rates ranging from 90.15% to 95%. The analysis of agreement mechanisms highlighted a clear advantage of pBFT over PoW, Raft, and Paxos in latency and energy efficiency, making it the most practical Byzantine fault tolerance method for permissioned healthcare blockchains. Therefore, the framework is demonstrably secure and scalable, making it highly suitable for real-time healthcare applications.

Chapter 6 serves as the central point of integration, combining the key findings and outcomes discussed in the preceding chapters. It provides a comprehensive conclusion by summarizing the major contributions of this research, with a focus on enhancing the security and efficiency of IoT systems through blockchain integration and advanced optimization models. The proposed frameworks collectively demonstrate significant improvements in secure resource allocation, anomaly detection, and communication reliability. The outcomes emphasize the role of blockchain and intelligent optimization techniques in achieving secure, efficient, and balanced IoT ecosystems.

### 6.1.1 Limitations

The proposed blockchain models in the context of IoT security systems also have potential constraints. The limitations of the proposed works are as follows:

- The combination of blockchain, deep learning, homomorphic encryption, fog computing, and hybrid optimization algorithms can raise the computational complexity, energy usage, and resource needs, which may not be suitable to resource-constrained IoT devices.
- Privacy preservation, regulatory compliance (such as GDPR and HIPAA), and interoperability with existing healthcare legacy systems are not comprehensively addressed, creating challenges for practical implementation.
- Advanced security threats such as insider attacks, Sybil attacks, 51% attacks, and smart contract vulnerabilities are not extensively analyzed, which may affect the reliability of blockchain-based IoT security systems in real-world scenarios.
- Scalability issues may arise when the number of IoT devices, transactions, and users increases significantly, as blockchain networks may experience higher latency, congestion, and reduced throughput in large-scale deployments.
- Dependence on large and high-quality datasets for training deep learning models may affect classification accuracy when insufficient, imbalanced, or noisy healthcare data is available.

## 6.2 Future Scope

This chapter examines potential pathways for the development and expansion of the proposed research pertaining to the integration of blockchain technology to optimize IoT environments through the application of hybrid strategies. The focus is on enhancing scalability, security, and adaptability in real-world IoT deployments, while also ensuring efficient resource utilization and seamless system operation.

- The integration of lightweight and energy-efficient blockchain mechanisms can be employed to reduce computational overhead, latency, and power consumption in resource-constrained IoT healthcare systems.

- The proposed blockchain-based IoT security models can be further improved by considering priority-based task handling, real-time patient monitoring requirements, and emergency response constraints to ensure effective operation in large-scale healthcare environments.
- To address scalability and heterogeneity challenges in larger IoT networks, future improvements can involve dynamic, context-aware, and AI-driven approaches that respond to real-time network conditions, workload variations, and resource availability.
- Future research can be extended to include fault-tolerance mechanisms such as task replication, checkpointing, redundancy, and backup consensus strategies to guarantee secure and uninterrupted execution in the event of server, fog node, or network failure.
- The proposed frameworks can be expanded to incorporate real-time failure detection and recovery strategies such as dynamic task migration, adaptive re-scheduling, and automatic recovery plans to maintain continuous healthcare services during node or communication failures.
- Adding security-aware decision-making can enable proactive detection of malicious nodes, insider threats, Sybil attacks, and denial-of-service attacks, while improving secure task offloading and trust-based node selection in blockchain-enabled IoT systems.
- Future studies can also focus on integrating privacy-preserving methods such as federated learning, explainable AI, and secure multi-party computation to strengthen data confidentiality and improve intelligent decision-making in healthcare IoT applications.
- Further work could focus on handling highly dynamic data generation and transaction management in real-time IoT scenarios, including burst workloads, strict latency requirements, and adaptive user behavior in smart healthcare systems.

\*\*\*\*\*



# Bibliography

- [1] Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, 5(1), 41-44.
- [2] Salman, O., Elhajj, I., Kayssi, A., & Chehab, A. (2015, November). An architecture for the Internet of Things with decentralized data and centralized control. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-8). IEEE.
- [3] Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17-31.
- [4] Li, B., Ye, R., Gu, G., Liang, R., Liu, W., & Cai, K. (2020). A detection mechanism on malicious nodes in IoT. *Computer Communications*, 151, 51-59.
- [5] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
- [6] Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., & Corchado, J. M. (2019). Blockchain technology in IoT systems: review of the challenges. *Annals of Emerging Technologies in Computing (AETiC)*, 3(5), 17-24.
- [7] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).
- [8] Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, 14(1).
- [9] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home.

In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

- [10] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information security journal: A global perspective*, 27(3), 162-182.
- [11] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, 141, 199-221.
- [12] Sobin, C. C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications*, 112(3), 1383-1429.
- [13] Sharma, P., Jindal, R., & Borah, M. D. (2022). Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *the Journal of Supercomputing*, 78(6), 7700-7728.
- [14] Pinon, M. M. B., Nascimento, M. H., de AB Junior, J., Tavares, T. F. D., & de Souza Silva, V. L. (2018). Applications and Advantages of the Internet of Things (IoT) at Industry (189-194). *ITEGAM-JETIA*, 4(15), 189-194.
- [15] Okafor, N. (2023). Advances and Challenges in IoT Sensors Data Handling and Processing in Environmental Monitoring Systems. *Authorea Preprints*.
- [16] Papadokostaki, K., Mastorakis, G., Panagiotakis, S., Mavromoustakis, C. X., Dobre, C., & Batalla, J. M. (2016). Handling big data in the era of internet of things (IoT). In *Advances in mobile Cloud computing and Big Data in the 5G Era* (pp. 3-22). Cham: Springer International Publishing.
- [17] Jang, J., Jung, I. Y., & Park, J. H. (2018). An effective handling of secure data stream in IoT. *Applied Soft Computing*, 68, 811-820.
- [18] Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In *The fusion of internet of things, artificial intelligence, and cloud computing in health care* (pp. 105-134). Cham: Springer International Publishing.
- [19] Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in internet of things: features, techniques and research challenges. *Int. J. Comput. Intell. Res*, 13(7), 1617-1627.

- [20] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, 1(2), 1-7.
- [21] Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, August). Internet of Things (IoT): Taxonomy of security attacks. In 2016 3rd international conference on electronic design (ICED) (pp. 321-326). IEEE.
- [22] Abughazaleh, N., Bin, R., & Btish, M. (2020). DoS attacks in IoT systems and proposed solutions. *Int. J. Comput. Appl*, 176(33), 16-19.
- [23] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2018). A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics*, 9(8), 1399-1417.
- [24] Moghaddasi, K., & Masdari, M. (2024). Blockchain-driven optimization of IoT in mobile edge computing environment with deep reinforcement learning and multi-criteria decision-making techniques. *Cluster Computing*, 27(4), 4385-4413.
- [25] Le, M., Huynh-The, T., Do-Duy, T., Vu, T. H., Hwang, W. J., & Pham, Q. V. (2024). Applications of distributed machine learning for the internet-of-things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.
- [26] Khan, B. U. I., Goh, K. W., Khan, A. R., Zuhairi, M. F., & Chaimanee, M. (2024). Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities. *Processes*, 12(9).
- [27] Merah, M., Aliouat, Z., Harbi, Y., & Batta, M. S. (2023). Machine learning-based clustering protocols for Internet of Things networks: An overview. *International Journal of Communication Systems*, 36(10), e5487.
- [28] Vabalas, A., Gowen, E., Poliakoff, E., & Casson, A. J. (2019). Machine learning algorithm validation with a limited sample size. *PloS one*, 14(11), e0224365.
- [29] Hemmatian, F., & Sohrabi, M. K. (2019). A survey on classification techniques for opinion mining and sentiment analysis. *Artificial intelligence review*, 52(3), 1495-1545.

- [30] Nasteski, V. (2017). An overview of the supervised machine learning methods. *Horizons. b*, 4(51-62), 56.
- [31] Salkuti, S. R. (2020). A survey of big data and machine learning. *International Journal of Electrical & Computer Engineering* (2088-8708), 10(1).
- [32] Singh, A., Thakur, N., & Sharma, A. (2016, March). A review of supervised machine learning algorithms. In *2016 3rd international conference on computing for sustainable global development (INDIACom)* (pp. 1310-1315). Ieee.
- [33] Praveena, M., & Jaiganesh, V. (2017). A literature review on supervised machine learning algorithms and boosting process. *International Journal of Computer Applications*, 169(8), 32-35.
- [34] Patruni, M. R., & Saraswathi, P. (2022). Securing Internet of Things devices by enabling Ethereum blockchain using smart contracts. *Building Services Engineering Research and Technology*, 43(4), 473-484.
- [35] Klassen, S., Weed, J., & Evans, D. (2018). Semi-supervised machine learning approaches for predicting the chronology of archaeological sites: A case study of temples from medieval Angkor, Cambodia. *PloS one*, 13(11), e0205649.
- [36] Van Engelen, J. E., & Hoos, H. H. (2020). A survey on semi-supervised learning. *Machine learning*, 109(2), 373-440.
- [37] Esparza, G. G., de-Luna, A., Zezzatti, A. O., Hernandez, A., Ponce, J., Álvarez, M., ... & de Jesus Nava, J. (2017, June). A sentiment analysis model to analyze students reviews of teacher performance using support vector machines. In *International Symposium on Distributed Computing and Artificial Intelligence* (pp. 157-164). Cham: Springer International Publishing.
- [38] Franc, V., Zien, A., & Schölkopf, B. (2011, June). Support Vector Machines as Probabilistic Models. In *ICML* (Vol. 11, pp. 665-672).
- [39] Käming, N., Dawid, A., Kottmann, K., Lewenstein, M., Sengstock, K., Dauphin, A., & Weitenberg, C. (2021). Unsupervised machine learning of topological phase transitions from experimental data. *Machine Learning: Science and Technology*, 2(3), 035037.

- [40] Dong, L. Y., Ji, S. J., Zhang, C. J., Zhang, Q., Chiu, D. W., Qiu, L. Q., & Li, D. (2018). An unsupervised topic-sentiment joint probabilistic model for detecting deceptive reviews. *Expert Systems with Applications*, 114, 210-223.
- [41] Kaur, M., & Mohta, A. (2019, November). A review of deep learning with recurrent neural network. In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 460-465). IEEE.
- [42] Ray, S. (2019, February). A quick review of machine learning algorithms. In *2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon)* (pp. 35-39). IEEE.
- [43] Menon, S., Anand, D., Kavita, Verma, S., Kaur, M., Jhanjhi, N. Z., ... & Ray, S. K. (2023). Blockchain and machine learning inspired secure smart home communication network. *Sensors*, 23(13), 6132.
- [44] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at SSRN 3440802.
- [45] Jena, A. K., & Dash, S. P. (2021). Blockchain technology: introduction, applications, challenges. In *Blockchain Technology: Applications and Challenges* (pp. 1-11). Cham: Springer International Publishing.
- [46] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4), 352-375.
- [47] Alotaibi, B. (2019). Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sensors Journal*, 19(23), 10953-10971.
- [48] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, 5(1), 31-37.
- [49] Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain meets cloud computing: A survey. *IEEE Communications Surveys & Tutorials*, 22(3), 2009-2030.
- [50] Moosavi, N., & Taherdoost, H. (2023). Blockchain technology application in security: A systematic review. *Blockchains*, 1(2), 58-72.

- [51] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 261-266). IEEE.
- [52] Ge, C., Liu, Z., & Fang, L. (2020). A blockchain based decentralized data security mechanism for the Internet of Things. *Journal of Parallel and Distributed Computing*, 141, 1-9.
- [53] Niranjanaamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, 22(Suppl 6), 14743-14757.
- [54] Paul, P., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). Blockchain technology and its types—a short review. *International Journal of Applied Science and Engineering (IJASE)*, 9(2), 189-200.
- [55] Andreev, R. A., Andreeva, P. A., Krotov, L. N., & Krotova, E. L. (2018). Overview of blockchain technology: types of blockchain and their applications. *Intelligent Systems in Manufacturing*, 16(1), 11-14.
- [56] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *Ieee Access*, 9, 61048-61073.
- [57] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, 7, 22328-22370.
- [58] Liang, Y., Lu, C., Zhao, Y., & Sun, C. (2021). Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management. *IEEE Access*, 9, 90757-90766.
- [59] Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE access*, 9, 43620-43652.
- [60] Ni, Z., Wang, W., Kim, D. I., Wang, P., & Niyato, D. (2019, May). Evolutionary game for consensus provision in permissionless blockchain networks with shards. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
- [61] Salimitari, M., Joneidi, M., & Chatterjee, M. (2019, December). Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based iot

- networks. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.
- [62] Wang, J., Ding, Y., Xiong, N. N., Yeh, W. C., & Wang, J. (2020). GSCS: General secure consensus scheme for decentralized blockchain systems. *IEEE Access*, 8, 125826-125848.
  - [63] Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2022). Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Computer Networks*, 214, 109118.
  - [64] Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, 10(2).
  - [65] Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, 6(2), 93-97.
  - [66] Naru, E. R., Saini, H., & Sharma, M. (2017, February). A recent review on lightweight cryptography in IoT. In 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) (pp. 887-890). IEEE.
  - [67] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, 129, 77-89.
  - [68] Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, 37, 2653-2659.
  - [69] Gupta, P., Sinha, A., Kr. Srivastava, P., Perti, A., & Singh, A. K. (2020). Security implementations in IoT using digital signature. In *Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2020* (pp. 523-535). Singapore: Springer Singapore.
  - [70] Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2018, June). A practical performance comparison of ECC and RSA for resource-constrained IoT devices. In 2018 Global Internet of Things Summit (GIIoTS) (pp. 1-6). IEEE.

- [71] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, 22(2), 572.
- [72] Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, 23(3), 2067-2087.
- [73] IŞIK, Ş., ÖZKAN, K., & ERGİN, S. (2019). Biometric person authentication framework using polynomial curve fitting-based ECG feature extraction. *Turkish Journal of Electrical Engineering and Computer Sciences*, 27(5), 3682-3698.
- [74] Honar Pajoo, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors*, 21(3), 772.
- [75] Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2021). Blockchain technology for smart city and smart tourism: latest trends and challenges. *Asia Pacific Journal of Tourism Research*, 26(4), 454-468.
- [76] Murphy, J., & Mishra, S. (2022). Challenges and solutions to blockchain-based management of IoT devices in smart cities. *Issues in Information Systems*, 23(4).
- [77] Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. 2020 IEEE International Conference on Blockchain (Blockchain), 490-495. <https://doi.org/10.1109/Blockchain50366.2020.00071>
- [78] Velmurugan, S., Prakash, M., Neelakandan, S., & Martinson, E. O. (2024). An efficient secure sharing of electronic health records using IoT-based hyperledger blockchain. *International Journal of Intelligent Systems*, 2024.
- [79] Ishmaev, G. (2020). The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data. 411-432.
- [80] Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research

opportunities. *Transportation research part e: Logistics and transportation review*, 142, 102067.

- [81] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, 22(4), 1448.
- [82] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Alman-sour, F. M. (2024). Blockchain-assisted secured data management frame-work for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing*, 28(1), 59-72.
- [83] Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain application in healthcare systems: a review. *Systems*, 11(1), 38.
- [84] Ullah, F., & Al-Turjman, F. (2023). A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Computing and Applications*, 35(7), 5033-5054.
- [85] Kamble, S. S., Gunasekaran, A., Subramanian, N., Ghadge, A., Belhadi, A., & Venkatesh, M. (2023). Blockchain technology's impact on supply chain integration and sustainable supply chain performance: Evidence from the automotive industry. *Annals of Operations Research*, 327(1), 575-600.
- [86] Baralla, G., Pinna, A., Tonelli, R., & Marchesi, M. (2023). Waste man-agement: A comprehensive state of the art about the rise of blockchain technology. *Computers in Industry*, 145, 103812.
- [87] Bhatia, M. S., Chaudhuri, A., Kayikci, Y., & Treiblmaier, H. (2023). Imple-mentation of blockchain-enabled supply chain finance solutions in the agri-cultural commodity supply chain: a transaction cost economics perspective. *Production Planning & Control*, 1-15.
- [88] Wang, H., Wang, C., Li, M., & Xie, Y. (2023). Blockchain technology invest-ment strategy for shipping companies under competition. *Ocean & Coastal Management*, 243, 106696.
- [89] Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, 25(3), 2203-2221. <https://doi.org/10.1007/s10586-021-03260-0>

- [90] Uganya, G., Bommi, R. M., Muthu Krishnammal, P., & Vijayaraj, N. (2023). Revised elliptic curve cryptography multi-signature scheme (RECC-MSS) for enhancing security in electronic health record (EHR) system. *Journal of Intelligent & Fuzzy Systems*, 45(6), 11993-12012.
- [91] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, 22(2), 572.
- [92] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6, 32979-33001. <https://doi.org/10.1109/ACCESS.2018.2842685>
- [93] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: challenges and solutions. *Blockchain: Research and Applications*, 2(2), 100006. <https://doi.org/https://doi.org/10.1016/j.bcra.2021.100006>
- [94] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 173-190, 2018, doi: <https://doi.org/10.1016/j.future.2018.05.046>.
- [95] Hu, J., Reed, M. J., Al-naday, M., & Thomos, N. (2021). Hybrid Blockchain for IoT - Energy Analysis and Reward Plan.
- [96] Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184-1195. <https://doi.org/10.1109/JIOT.2018.2812239>
- [97] Pajoooh, H. H., Rashid, M., & Alam, F. (2021). Multi-Layer Blockchain-Based Security Architecture for. 1-26.
- [98] Wang, Y., Li, J., Liu, W., & Tan, A. (2021). Efficient Concurrent Execution of Smart Contracts in Blockchain Sharding. *Security and Communication Networks*, 2021. <https://doi.org/10.1155/2021/6688168>
- [99] Samaniego, M., & Deters, R. (2017). Blockchain as a Service for IoT. *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social*

Computing; IEEE Smart Data, IThings-GreenCom-CPSCCom-Smart Data 2016, January 2020, 433-436. <https://doi.org/10.1109/iThings-GreenCom-CPSCCom-SmartData.2016.102>

- [100] Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, 181, 103050. <https://doi.org/https://doi.org/10.1016/j.jnca.2021.103050>
- [101] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *sensors*, 18(8), 2575.
- [102] Kuhrmann, M., Fernandez, D. M., & Daneva, M. (2022). On the pragmatic design of literature studies in software engineering: an experience-based guideline. *Empirical Software Engineering*, 22(6), 2852-2891. <https://doi.org/10.1007/s10664-016-9492-y>
- [103] Nogami, V. K. da C., Pilli, L. E., Mazzon, J. A., Vieira, F. G. D., & Veloso, A. R. (2022). Innovation in low-income market: A study based on the symbolic production and cultural reproduction. *BASE - Revista de Administracao e Contabilidade Da Unisinos*, 1-10. <https://doi.org/10.4013/base.2015.124.06>
- [104] Kaushik, D., Gulia, P., Gill, N. S., Yahya, M., Shukla, P. K., & Shreyas, J. (2026). Synergizing blockchain and AI to fortify IoT security: a comprehensive review. *Artificial Intelligence Review*, 59(2), 41.
- [105] Molose, R., & Isong, B. (2026). A Survey of Multi-Layer IoT Security Using SDN, Blockchain, and Machine Learning. *Electronics*, 15(3), 494.
- [106] Kshetri, N. (2022). Can Blockchain Strengthen the Internet of Things IT Professional, 19(4), 68-72. <https://doi.org/10.1109/mitp.2017.3051335>
- [107] Shala, B., Trick, U., Lehmann, A., Ghita, B., & Shiaeles, S. (2020). Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision. *IEEE Access*, 8, 119961-119979. <https://doi.org/10.1109/ACCESS.2020.3005541>
- [108] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, 1(1). <https://doi.org/10.1007/s43926-020-00001-4>

- [109] Li, W., Meng, W., Liu, Z., & Au, M. (2020). Towards Blockchain-Based Software-Defined Networking: Security. 2, 196-203.
- [110] Costa, H. J. D. M., Da Costa, C. A., Righi, R. D. R., Antunes, R. S., Santana, J. F. D. P., & Leithardt, V. R. Q. (2022). A fog and blockchain software architecture for a global scale vaccination strategy. *IEEE Access*, 10, 44290-44304.
- [111] Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics*, 10(17), 2110.
- [112] Mayer, A. H., Rodrigues, V. F., da Costa, C. A., da Rosa Righi, R., Roehrs, A., & Antunes, R. S. (2021). Fogchain: a fog computing architecture integrating blockchain and internet of things for personal health records. *IEEE Access*, 9, 122723-122737.
- [113] Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., & Jameel, S. M. (2021). Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet of Things*, 15, 100422.
- [114] Fetjah, L., Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2021). Towards a smart healthcare system: an architecture based on IoT, blockchain, and fog computing. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, 16(4), 1-18.
- [115] Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., & Hossain, E. (2020). A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE access*, 8, 118433-118471.
- [116] Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2020). Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access*, 8, 20118-20128.
- [117] Wu, D. & Nirwan, A. "A cooperative computing strategy for blockchain-secured fog computing." *IEEE Internet of Things Journal* 7.7 (2020): 6603-6609.
- [118] Manoj, K. Sai & P. S. Aithal. "Blockchain Cyber Security Vulnerabilities and Potential Countermeasures." *International Journal of Innovative Technology and Exploring Engineering* 9.5 (2020): 1516-1522.

- [119] Alam, T., & Benaida, M. (2020). Blockchain, fog and iot integrated framework: review, architecture and evaluation. arXiv preprint arXiv:2006.03596.
- [120] S., Monika., Navashree P., & S.Vivekanandan . "A BLOCK CHAIN-BASED ACCESS CONTROL FRAMEWORK FOR BIG DATA." IJARCCCE 10.4 (2021): 331-334. IJARCCCE. Web.
- [121] Umoren, O., Singh, R., Pervez, Z., & Dahal, K. (2022). Securing fog computing with a decentralised user authentication approach based on blockchain. *Sensors*, 22(10), 3956.
- [122] Nguyen, H., Nguyen, T., Leppänen, T., Partala, J., & Pirttikangas, S. (2022, June). Situation awareness for autonomous vehicles using blockchain-based service cooperation. In *International Conference on Advanced Information Systems Engineering* (pp. 501-516). Cham: Springer International Publishing.
- [123] Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. *Future Internet*, 14(7), 216.
- [124] Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring improved security in medical data using ecc and blockchain technology with edge devices. *Security and Communication Networks*, 2021(1), 6966206.
- [125] Baniata, H., & Kertesz, A. (2022). Prifob: a privacy-aware fog-enhanced blockchain-based system for global accreditation and credential verification. *Journal of Network and Computer Applications*, 205, 103440.
- [126] Wang, H., Wang, L., Zhou, Z., Tao, X., Pau, G., & Arena, F. (2019). Blockchain-based resource allocation model in fog computing. *Applied Sciences*, 9(24), 5538.
- [127] Maldonado-Ruiz, D., Torres, J., & El Madhoun, N. (2020, September). 3BI-ECC: a decentralized identity framework based on blockchain technology and elliptic curve cryptography. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 45-46). IEEE.

- [128] Alshahrani, M. Y. (2021). Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform. *Applied Sciences*, 12(1), 74.
- [129] Hossein, K. M., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Computer Communications*, 180, 31-47.
- [130] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50, 102407.
- [131] Li, C., Guo, J., Zhang, G., Wang, Y., Sun, Y., & Bie, R. (2019, August). A blockchain system for E-learning assessment and certification. In *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)* (pp. 212-219). IEEE.
- [132] Mahmood, K., Obaidat, M. S., Shamshad, S., Alenazi, M. J., Kumar, G., Anisi, M. H., & Conti, M. (2024). Cost-effective authenticated solution (CAS) for 6G-enabled artificial intelligence of medical things (AIoMT). *IEEE Internet of Things Journal*, 11(13), 23977-23984.
- [133] Shahzad, A., Chen, W., Shaheen, M., Zhang, Y., & Ahmad, F. (2024). A robust algorithm for authenticated health data access via blockchain and cloud computing. *Plos one*, 19(9), e0307039.
- [134] Sonkamble, R. G., Bongale, A. M., Phansalkar, S., Sharma, A., & Rajput, S. (2023). Secure data transmission of electronic health records using blockchain technology. *Electronics*, 12(4), 1015.
- [135] Mahmood, K., Obaidat, M. S., Ghaffar, Z., Alzahrani, B. A., Shamshad, S., Saleem, M. A., & Hussain, S. (2022). Cloud-assisted secure and cost-effective authenticated solution for remote wearable health monitoring system. *IEEE transactions on network science and engineering*, 10(5), 2710-2718.
- [136] Shamshad, S., Ayub, M. F., Mahmood, K., Rana, M., Shafiq, A., & Rodrigues, J. J. (2021). An identity-based authentication protocol for the telecare medical information system (TMIS) using a physically unclonable function. *IEEE Systems Journal*, 16(3), 4831-4838.
- [137] Fasila, K. A., & Mathew, S. (2022). Fast and Efficient Security Scheme for Blockchain-Based IoT Networks. *Computers, Materials & Continua*, 73(1).

- [138] Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., & Yamin, M. (2021). Blockchain-based secured access control in an IoT system. *Applied Sciences*, 11(4), 1772.
- [139] Shamshad, S., Mahmood, K., Hussain, S., Garg, S., Das, A. K., Kumar, N., & Rodrigues, J. J. (2021). An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber-physical systems. *IEEE Internet of Things Journal*, 9(7), 5142-5149.
- [140] Shamshad, S., Mahmood, K., Kumari, S., & Chen, C. M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, 55, 102590.
- [141] Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, 8, 32031-32053.
- [142] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehers sharing of mobile cloud based e-health systems. *IEEE access*, 7, 66792-66806.
- [143] Singh, A., Kaur, H., & Kaur, N. (2024). A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network. *Cluster Computing*, 27(3), 3537-3557.
- [144] Farooq, M. S., Khan, S., Rehman, A., Abbas, S., Khan, M. A., & Hwang, S. O. (2022). Blockchain-based smart home networks security empowered with fused machine learning. *Sensors*, 22(12), 4522.
- [145] Ichikawa, D., Kashiya, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, 5(7), e7938.
- [146] Srivastava, G., Crichigno, J., & Dhar, S. (2019, May). A light and secure healthcare blockchain for iot medical devices. In *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)* (pp. 1-5). IEEE.
- [147] Meng, W., Li, W., & Zhu, L. (2019). Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. *IEEE Transactions on Engineering Management*, 67(4), 1377-1386.

- [148] Akkaoui, R. (2021). Blockchain for the management of internet of things devices in the medical industry. *IEEE Transactions on Engineering Management*, 70(8), 2707-2718.
- [149] Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2020). Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future internet*, 12(3), 44.
- [150] Malik, R., Dua, S., & Shoran, P. (2025). Blockchain-based node authentication algorithm for securing electronic health record data transmission. *Cluster Computing*, 28(8), 539.
- [151] pogu Jayanna, S., Ramya, G., Rupa, A., Krushna, S. V., Fouziya, M. D., & Ranjith, J. (2024). Enhancing IoT Networks with AI-Optimized Blockchain and Edge Computing for Improved Scalability and Performance. *Nanotechnology Perceptions*, 350-367.
- [152] Goyat, R., Kumar, G., Conti, M., Devgun, T., Saha, R., & Thomas, R. (2023). BENIGREEN: Blockchain-Based Energy-Efficient Privacy-Preserving Scheme for Green IoT. *IEEE Internet of Things Journal*, 10(18), 16480-16493.
- [153] Aldyafiah, I. M., Zhao, W., Upadhyay, H., & Lagos, L. (2023). The design and implementation of a secure datastore based on ethereum smart contract. *applied sciences*, 13(9), 5282.
- [154] Namasudra, S., Sharma, P., Crespo, R. G., & Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consumer Electronics Magazine*, 12(2), 83-93.
- [155] Patthi, S., Karthiga, M., Sinha, K. P., Mandala, S. K., Anusha, P. V., Bhagyalakshmi, L., ... & Alagarsamy, M. (2025). Integration of Internet of Things Blockchain and Artificial Intelligence for Scalable and Secure Precision Environmental Management. *Sustainable Computing: Informatics and Systems*, 101251.
- [156] Rhidoy, H. M., Miraz, M. H., & Salam, I. (2025). Optimising Blockchain Scalability for Real-Time IoT Applications. *arXiv preprint arXiv:2603.27643*.

- [157] Gholami, M., Ghaffari, A., Derakhshanfard, N., Ibrahimoglu, N., & Ali, A. (2025). Blockchain integration in IoT: applications, opportunities, and challenges. *Computers, Materials, & Continua*, 83(2), 1561.
- [158] Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., & Chaudhry, R. (2025). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Networking and Applications*, 18(1), 53.
- [159] Zhang, F., Yu, P., Guo, S., Huang, W., & Qi, F. (2025). Computing Sandbox Driven Secure Edge Computing System for Industrial IoT. *IEEE Transactions on Network and Service Management*.
- [160] ODUWALE, A. M., ALESE, B., OBE, O., & ODENIYI, O. (2025). BLOCKCHAIN-DRIVEN PRIVACY AND RISK MANAGEMENT FOR INTERNET OF THINGS (IoT) SYSTEMS. *Journal of Advanced Science and Optimization Research*.
- [161] Chowdhury, S., Mayilvahanan, P., & Govindaraj, R. (2022). Optimal feature extraction and classification-oriented medical insurance prediction model: machine learning integrated with the internet of things. *International Journal of Computers and Applications*, 44(3), 278-290.
- [162] Drescher, D.: *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress, New York (2017).
- [163] Fernandes, A., Rocha, V., Da Conceicao, A. F., & Horita, F. (2020, March). Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (pp. 130-138). IEEE.
- [164] Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, 20(22), 6587.
- [165] Vanin, F. N. D. S., Policarpo, L. M., Righi, R. D. R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2022). A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. *Sensors*, 23(1), 14.
- [166] Khair, M., El Moucary, C., & Zakhem, W. (2018). Introducing Usage-Based Encryption for a Secure and Versatile Access Control Scheme of Electronic

Health Records on Cloud. *Research Journal of Applied Sciences, Engineering and Technology*, 15(9), 344-355.

- [167] Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. *Sensors*, 23(15), 6762.
- [168] <https://slideplayer.com/slide/12633599/>.
- [169] Adams, R., Kewell, B., & Parry, G. (2017). Blockchain for good? Digital ledger technology and sustainable development goals. In *Handbook of sustainability and social science research* (pp. 127-140). Cham: Springer International Publishing.
- [170] Vengadapurvaja, A. M., Nisha, G., Aarth, R., & Sasikaladevi, N. (2017). An efficient homomorphic medical image encryption algorithm for cloud storage security. *Procedia computer science*, 115, 643-650.
- [171] Alzubi, J. A., Alzubi, O. A., Beseiso, M., Budati, A. K., & Shankar, K. (2022). Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. *Expert Systems*, 39(4), e12879.
- [172] Cui, Q., Wu, S., Liu, Q., Zhong, W., & Wang, L. (2018). MV-RNN: A multi-view recurrent neural network for sequential recommendation. *IEEE Transactions on Knowledge and Data Engineering*, 32(2), 317-331.
- [173] McCarthy, A., Ghadafi, E., Andriotis, P., & Legg, P. (2022). Functionality-preserving adversarial machine learning for robust classification in cybersecurity and intrusion detection domains: A survey. *Journal of Cybersecurity and Privacy*, 2(1), 154-190.
- [174] Zhao, W., Alwidian, S., & Mahmoud, Q. H. (2022). Adversarial training methods for deep learning: A systematic review. *Algorithms*, 15(8), 283.
- [175] <https://www.kaggle.com/datasets/hussameldinanwer/diagnosis-icd-mimic-iii>.
- [176] Deng, X., Li, K., Wang, Z., Li, J., & Luo, Z. (2022, July). A survey of blockchain consensus algorithms. In *2022 international conference on*

- blockchain technology and information security (ICBCTIS) (pp. 188-192). IEEE.
- [177] Sumagita, M., Riadi, I., Sh, J. P. D. S., & Warungboto, U. (2018). Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 7(4), 373-381.
  - [178] Zhang, H., & Cheng, S. (2022). Application of Internet of Things Technology Based on Artificial Intelligence in Electronic Information Engineering. *Mobile Information Systems*, 2022(1), 2888925.
  - [179] Gupta, R., Verma, S., & Janjua, K. (2018, August). Custom application development in cloud environment: Using salesforce. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 23-27). IEEE.
  - [180] Gandam, A., Sidhu, J. S., Verma, S., Jhanjhi, N. Z., Nayyar, A., Abouhawwash, M., & Nam, Y. (2021). An efficient post-processing adaptive filtering technique to rectifying the flickering effects. *PLoS One*, 16(5), e0250959.
  - [181] Ghosh, G., Kavita, Anand, D., Verma, S., Rawat, D. B., Shafi, J., Marszałek, Z., & Woźniak, M. (2021). Secure Surveillance Systems Using Partial-Regeneration-Based Non-Dominated Optimization and 5D-Chaotic Map. *Symmetry*, 13(8), 1447. <https://doi.org/10.3390/sym13081447>
  - [182] Liao, L., Li, H., Shang, W., & Ma, L. (2022). An empirical study of the impact of hyperparameter tuning and model optimization on the performance properties of deep neural networks. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 31(3), 1-40.

## List of Publications

1. **Rohit Malik, Sakshi Dua, and Preety Shoran**"Blockchain-based node authentication algorithm for securing electronic health record data transmission." Cluster Computing 28.8 (2025): 539. (SCI)Q1
2. **Rohit Malik, Sakshi Dua, and Preety Shoran** "A Novel Blockchain-Integrated Deep Learning Framework for Securing Smart Healthcare Communication Networks" Computational Intelligence, Wiley 37, no. 12-14 (2025): e70113.(SCI)Q1
3. **Rohit Malik, Sakshi Dua, Preety Shoran, Ajay Nain** Blockchain-Enabled Federated Learning for Enhancing Security in IoT-Driven Healthcare Systems (Communicated).
4. **Rohit Malik, Sakshi Dua, Preety Shoran, Ajay Nain** A Systematic Review of Blockchain-based Security Solutions for IoT: Concepts, Challenges and Applications (Communicated).

## Papers Presented in Conferences

1. **Rohit Malik, Sakshi Dua, Preety Shoran, Ajay Nain** Blockchain and big data as emerging solutions for fog challenges: An impeccable study(RACS 2022).
2. **Rohit Malik, Sakshi Dua, Preety Shoran, Ajay Nain** Enhancing Security and Resource Optimization in IoT Applications with Blockchain Inclusion (INCOFT)2023.

## Patents

1. Designing an efficient framework for big data security in Fog-enabled IoT environment.-202411068980
2. Optimizing SDN-Based Edge Computing with Deep Belief Networks for Predictive Analytics and Intrusion Detection.