# LIGHTWEIGHT SECURITY MODELS FOR GREEN COMPUTING IN INTERNET OF THINGS

*Thesis submitted to the Jawaharlal Nehru University*

*in partial fulfillment of the requirements*

*for the award of the degree of*

**DOCTOR OF PHILOSOPHY**

**IN**

**COMPUTER SCIENCE AND TECHNOLOGY**

**By**

**RINKI RANI**

**Supervisor**

**Dr. Sushil Kumar**

**SCHOOL OF COMPUTER & SYSTEMS SCIENCES**
**JAWAHARLAL NEHRU UNIVERSITY**
**NEW DELHI – 110067, INDIA**

**June, 2022**

School of Computer & Systems Sciences
जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067

# CERTIFICATE

This is to certify that the thesis entitled **"Lightweight Security Models for Green Computing in Internet of Things"**, being submitted by ***Ms. Rinki Rani*** to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi**, in partial fulfillment of the requirement for the award of the **Degree of Doctor of Philosophy in Computer Science and Technology**, is a bonafide research work carried out by her under the supervision of ***Dr. Sushil Kumar***.

This research work embodied in the thesis is original and has not been submitted for the award of any other Degree.

June 24, 2022
Dr Sushil Kumar
(Supervisor),
Assistant Professor,
SC&SS, JNU,
New Delhi-110067

24-06-2022
Prof. T.V. Vijay Kumar
Dean, SC&SS
Jawaharlal Nehru University
New Delhi-110067

School of Computer & Systems Sciences
जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067

# DECLARATION

This is to certify that the thesis entitled **"Lightweight Security Models for Green Computing in Internet of Things"**, being submitted to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi**, in partial fulfillment of the requirement for the award of the **Degree of Doctor of Philosophy in Computer Science and Technology**, is a bonafide research work carried out by me.

This research work embodied in the thesis is original and has not been submitted for the award of any other Degree.

Rinki Rani
Enrollment No: 14/10/MT/012
Ph.D. Scholar,
SC&SS, JNU
New Delhi-110067

# ACKNOWLEDGEMENT

Being a part of this prestigious university in itself is a lifetime opportunity. Doing Research work for the degree of Ph.D. was a wonderful experience, but it came with a lot of challenges. Though there were some difficulties, new experiences which helped me in the evolution of my personality and career. In the course of work, many people have supported and guided either directly or indirectly which certainly helped me in this journey. Without the support of these worthy people, it would be very difficult to complete my doctoral work smoothly.

Before everyone, I want to thank god for giving me strength and for making my path smooth with fewer obstacles. I would like to express my sincere gratitude to my supervisor Dr. Sushil Kumar for his support in every way possible. His guidance, support, faith and friendly behavior helped a lot during my Ph.D. Your guidance has always inspired me to work hard for completion of my thesis. I, thank you, sir, for everything.

I wish to thank my senior, Dr. Omprakash Kaiwartya, for his guidance. I am really grateful for your help, inspiring behavior and time, which motivated and had given me direction during my research work.

I would like to convey my gratitude to Prof T.V.Vijay, Dean of School of Computer and Systems Sciences, administrative staffs, and librarian for ensuring a suitable environment in the school which aided in completing my research work. I would give my sincere thanks to my fellow colleagues, Intyaz, Ankita, Archana, Neeru, Indu etc., juniors Ritesh, Parveen, Bhawana, Pinky and Ankit etc and my seniors Kirshna, Aanchal, Reena, Pankaj etc for sharing their experiences and knowledge with me and gave their timely support during my research work. I am really thankful for all the help and encouragement.

I want to thank my father, Mr. Harlal, and mother, Mrs. Kamlesh Rani, to whom I want to dedicate my thesis, for helping me at every step. You people are the lights which have lightened up my path. Without your guidance and support, it would not have been possible. Thank you, father and mother, for trusting me.

Finally, I want to thank my sister Mrs. Renu Rani, and brother Mr. Sumit Kumar and brother in law Mr. Arvind Sharma, and my niece Aarohi and my friend Mrs. Nancy Raghav for their love, kindness, and support, which was most important when I used to feel low.

*Rinki Rani*

# TABLE OF CONTENTS

# List of Figures

# List of Tables

# Abbreviations

| Abbreviations | Descriptions |
|---|---|
| ABE | Attribute based Encryption |
| ABI | Application Binary Interface |
| ABKS | Attribute-Based Keyword Search |
| AC | Authorization Contract |
| ACC | Access Control Contract |
| AES | Advanced Encryption Standard |
| AI | Artificial Intelligence |
| ASMS | Addressing Security in Medical Sensor |
| BFS | Breadth First Search |
| BLE | Bluetooth Low Energy |
| BSNS | Body Sensor Network Security |
| C | Ciphertext |
| CA | Certificate Authority |
| CH | Cluster Head |
| CKA | Chosen-Keyword Attack |
| CM | Cluster Member |
| COAP | Constrained Application Protocol |
| CPA | Chosen Plain-text Attack |
| CP-ABKS | CipherText-Policy Attribute-Based Keyword Search encryption |
| CSSI | Computational Supersingular Isogeny |
| CWSN | Cluster-based Wireless Sensor Network |
| DDS | Data distribution services |
| DFS | Distributed File Storage |
| DOS | Denial of Service |
| DST | Dempster–Shafer theory |
| DT | Direct Trust |

| | |
|---|---|
| EASI | Efficient Algorithms for Super-singular Isogeny |
| eMHR | Electronic Health Record |
| $EC_{avg}$ | Average Energy Consumption |
| ECC | Elliptic Curve Cryptosystem |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECH-tree | Energy-Efficiency Hierarchical Clustering index tree |
| EETE | energy efficient trust evaluation |
| END | Endomorphism |
| EPQU | Efficient Post-Quantum Undeniable signature |
| EU-ACMA | Existentially Unforgeable under an Adaptively Chosen Message Attacks |
| GIS | Geographic Information system |
| GPS | Global Positioning System |
| HIDS | Hybrid Intrusion Detection System |
| HTTP | Hypertext transfer protocol |
| IaaS | Infrastructure as a service |
| IBC | Identity Based Cryptography |
| IoE | Internet of Everything |
| IoT | Internet of Things |
| IIOT | Industrial Internet of Things |
| IP | Internet Protocol |
| IoE | Internet of Everything |
| IT | Indirect Trust |
| JS | Judge Contract |
| KCIB | Key Compression for Isogeny-Based cryptosystems |
| LDTS | Lightweight and Dependable Trust System |
| LMS | Local Medical Supervisor |
| LPQS | Lightweight Postquantum ID-based Signature |
| LoRaWAN | Long range wide area network |
| MATLAB | Matrix Laboratory |

| | |
|---|---|
| MNs | Mobile nodes |
| MMPs | Mobility Management Protocol |
| MPK | Master Public Key |
| MQTT | MQ telemetry transport |
| MSIDH | Microsoft's Supersingular Isogeny Diffie-Hellman |
| MSK | Master Secret Key |
| ND | Node Degree |
| NGeH | Next Generation eHealth |
| NTRU | Nth degree Truncated polynomial Ring Units |
| NS-3 | Network Simulator-3 |
| PaaS | Platform as a service |
| PBFT | Practical Byzantine Fault Tolerance |
| PI | Past Interaction |
| PK | Public Key |
| PKG | Public Key Generator |
| PKI | Public key infrastructure |
| PP | Public Parameters |
| PQC | Post-Quantum Cryptography |
| QoS | Quality of Service |
| RC | Register Contract |
| RFID | Radio Frequency Identification |
| SaaS | Software as a service |
| SFBF | Secure Fog-enabled Blockchain Framework |
| SHA | Secure Hash Algorithm |
| SIAPC | Supersingular Isogeny Auxiliary Point Computation |
| SIDH | Supersingular Isogeny Diffie-Hellman |
| SK | Secret Key/Session key |
| SHES | Smart Hospital Emergency System |
| SMTP | Simple mail transfer protocol |
| TA | Trusted Authority |

| | |
|---|---|
| TCP | Transmission control protocol |
| TSRF | Trust-aware Secure Routing Framework |
| UDP | User datagram packet |
| VK | Validation Key |
| WSN | Wireless Sensor Network |

# List of Publications

**Journals**

1. Rinki Rani, Sushil Kumar et al. "Towards Green Computing Oriented Security: A Lightweight Postquantum Signature for IoE," *Sensors*, vol. 21, no. 5, pp. 1883, 2021. **(SCI-indexed)**
2. Rinki Rani, Sushil Kumar, and Upasana Dohare, "Trust evaluation for lightweight security in sensor enabled internet of things: game theory oriented approach," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8421,2019. **(SCI-indexed)**
3. Rinki Rani, Sushil Kumar , "Secure IoT centrci Blockchain for Next Generation eHealth Services in IoT Environment" in IEEE transactions on network and service management (**Communicated )**

**Conferences**

1. Rinki Rani, and C. P. Katti, "End-to-End security in delay tolerant mobile social network," *International Conference on Application of Computing and Communication Technologies*, Springer, Singapore, 2018. (**Presented**)
2. Rinki Rani, and Sushil Kumar, "Fog-enabled Secure Data Deduplication and Encrypted Search for Internet of Things", *International Conference on Networks and Cryptology,* CRC Press, 2020. (**Presented** and **Best Paper**)

# ABSTRACT

The Internet of Things (IoT) is a broad range of umbrella that connects “smart” version of traditional devices such as electric bulb, air conditioner, refrigerator and the devices expected to have an internet connection, and that can communicate with the network independently. These devices use intelligent frameworks which are seamlessly integrated into the information network where you can connect anywhere, anytime and with any media. In recent times, IoT has shown tremendous potential for future development where applications are increasing rapidly and are playing significant role in day-to-day life such as smart home, smart city, farming and self-driven cars. However, devices used in such environment are battery driven and storage constrained with less processing power. It affects implementation of IoT and raises various issues such as security and energy consumption. In recent decade, security of IoT devices has been a cause of concern and has had the inevitable consequences of allowing both small and large-scale attacks due to lack of appropriate security guidelines document. The existing security techniques for secure communication cannot be applied directly in WSN-based-IoT. Therefore, security is an interesting and open research topic for IoT.

In sensor-enabled Internet of Things (IoT), nodes are deployed in an open and remote environment, therefore, are vulnerable to various internal attacks. Because of the less computation complexity and high resistance to the internal attacks, trust evaluation is an efficient alternative to resolve the pre-mentioned issues in the public key infrastructure (PKI). Therefore, trust plays a pivotal role in securing communication for sensors enabled IoTs. Literature surveys various trust evaluation schemes based on energy due to unnecessary transmission involved during trust calculation process. In such models, the wrong information communicated from malicious nodes may misguide the network. Thus, in this thesis, an

energy efficient trust evaluation scheme is proposed with cooperative behavior of nodes to maintain the trust of individual networks and to mitigate the malicious activity in the network.

Cryptographic system depends on solving mathematical problems such as integer factorization and discrete logarithms. Major recent schemes depend on these two mathematical problems which are infeasible to solve on any classical computer. However, these problems can easily be solved by quantum computers in polynomial time. For instance, Shor's quantum algorithm can solve the integer factorization in polynomial-time. Moreover, it can not only forge a signature but also recover private keys. Thus, such system poses serious threats to the modern cryptography. To effectively block these threads, many cryptographers are developing new quantum-resistant algorithms that are unbreakable in the era of quantum computers. Several Post-Quantum cryptography (PQC) classes have been proposed which are currently believed to be quantum resistant namely: lattice-based, hash-based, code-based PQC and isogeny-based. Prime issues in IoT security are related to key size, signature and the encryption computation of the post-quantum based cryptosystems. In this context, use of isogeny curve for post-quantum cryptography is considered to be most practical solution to energy required for the shortest key's computation. Additionally, it reduces the overall time needed for the crypto operations than post-quantum based cryptosystems and therefore appropriate replacement in sensors and IoT applications.

The Internet of Things (IoT) plays a crucial role in shaping the future of the next-generation eHealth (NGeH) system with unsurpassed context-aware, mobile, and personalized services. The growing demand for personalized NGeH services raises privacy, accuracy, and scalability concerns due to the increase in extremely sensitive patient eHealth data. Hence, the technical design of the NGeH system should consider these issues to effectively secure eHealth data from unauthorized breaches, certify accuracy in data sharing, and efficiently manage the increase in eHealth data. In this context, a novel, secure fog-enabled blockchain framework (SFBF) for NGeH services in the IoT environment to efficiently monitor patients in real time and to manage and securely access patients' electronic medical health records (eMHRs) is proposed. Efficiency and feasibility of the model are demonstrated, and results shows that latency and throughput are inversely proportional and enhances the network's scalability.

The performance of the proposed schemes is analyzed by mathematical model and empirical evidence. Simulations are carried out in realistic IoT environment and results are generated with the help of NS-3, MATLAB, Microsoft Visual Studio and Yeoman. The different parameters have been observed like detection rate, energy consumption, clock cycles, computation cost, communication cost, average latency and throughput. The performance of the schemes is comparatively analyzed with state-of-the-art models.

# Chapter 1

# Introduction to Internet of Things

## 1.1. Overview of IoT

The Internet of Things (IoT) is one of the important technology of 21st century. It plays a significant role in enhancing the quality of human's life. It is an environment where objects, people or animals have the capability of processing the data without any human intervention. It is based on interoperable communication protocols where physical devices use intelligent framework which are seamlessly integrated into the information network [1,2]. IoT is a notion which is based on 3A which means establish connection anytime, anywhere and with any media. IoT nodes are responsible of gathering lightweight data and deliver it to sink which is a wireless base station. These nodes are also capable of accessing and authorizing cloud-based resources for collecting and extracting data. Further, with the help of analyzing tools it make decisions. These nodes can be anything from smartwatches, laptops, iPads to electronic devices such as refrigerator, digital locks or ACs, which can automatically set the temperature of your room for right amount of time. The applications of IoT technologies are multiple, and provide relevant information about the environment. IoT applications are increasing day by day and it plays a significant role in healthcare, smart city, agriculture, banking, billing system and many cross-cutting business applications. The total installed base of IoT connected devices worldwide is expected to be 13.8 billion in 2021 while the world population is 7 billion. As per researcher's prediction, the projected amount will be 30.9 billion units by 2025 which is 4 times the world population.

## 1.2. Applications of IoT

IoT has transform the people's life and made it easier than ever before. In this aspect, various applications are used in day-to-day life such as smart home, smart city, smart healthcare

system, farming, wearables, smart grids, industrial internet, self-driven car, IoT retail shops, and smart supply chain management system, and these are explained below.

### 1.2.1 Smart Homes

Smart Homes plays a vital role in revolutionizing the shape of today's world and it will become as common as smartphones. IoT provides better energy, water and time management. The source management helps in reducing the cost of management of the house which is the one of the biggest cost for the homeowner. Use of home appliances such as refrigerator, washing machine, air conditioner etc. in a controlled way is necessary for reducing electricity, water and other resources consumption [3,4].

### 1.2.2. Smart City

Smart City solves the major problems of the people living in the cities such as pollution, transportation, power shortage, and water supply and drainage. IoT-enabled devices and sensors can collect the weather data which help in managing traffic, cut air pollution, improve agriculture and keep citizens safe and clean. Overall, IoT helps in improvising the quality of citizen's life [5,6].

### 1.2.3. Smart Healthcare System

IoT provides various applications in Healthcare field. IoT in healthcare provides healthcare services everywhere, every time and in right manner. It includes smart use cases of context-aware sensor networks to gather information related to patient's activities and patient's environment. Wireless body area network (WBAN) collect vital information such as blood pressure and cardiac index from patient's body. Few examples of smart healthcare services are remote patient monitoring to assess the patient's health condition and emergency medical response services to provide immediate assistance to sustain life under concrete circumstances [7].

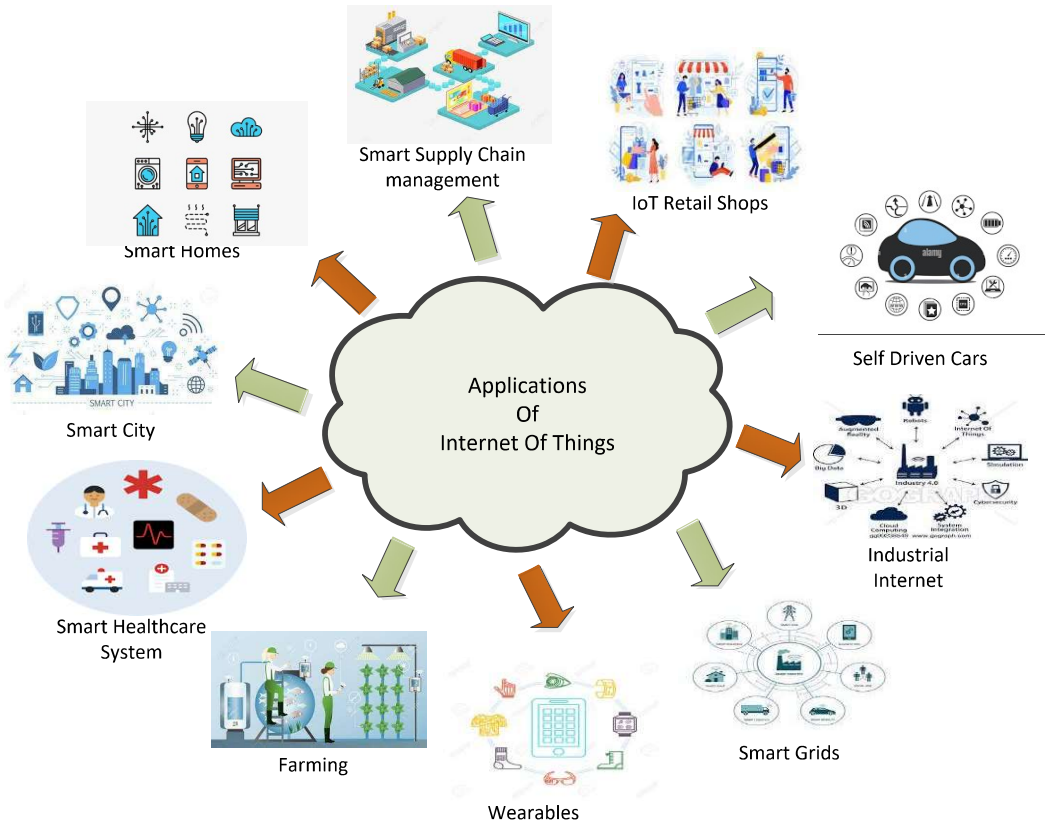



**Figure 1.1**. Applications of IoT.

### 1.2.4. Farming

Internet of Things will benefit the Farming sector. Tools are being developed for monitoring climate conditions, green house management, crop management, cattle monitoring and management, precision farming. These allow farmers in predictive analytics for smart farming which helps in crop harvesting time, reduces the risks of diseases and infestations etc. With so many developments happening on tools farmers can use for agriculture, the future is sure promising [8,9].

### 1.2.5. Wearables

Business and social change have reshaped the IoT and wearables. It is developing new value, improving and leading to new ways of making money and delivering greater value to customers. Many wearables have been devised like defibrillators to monitor the heart rhythm

for early heart attack detection, Apple Watch Health app helps to evaluate patient response to medication or smart contact lenses which record changes in eye dimension. Such wearable devices have given patients a new life [10].

### 1.2.6. Smart Grids

Smart grid provides a variety of operation and energy measures which includes renewable energy resources, advanced metering infrastructure or smart distribution boards with home control. This new technology helps in avoiding large-scale blackouts and provide better energy distribution for health center, police department, traffic lights, phone system and grocery store operating during emergencies [11,12].

### 1.2.7. Industrial Internet

Industrial Internet of Things (IIoT) is to use the sensors and actuators to enhance manufacturing and industrial processes. IIoT intersect the information technology and operational technology. It provides better visibility of supply chain, predicts points of failure and even trigger maintenance processes autonomously [13,14].

### 1.2.8. Self-driven cars

A number of companies are investing in self-driving cars such as Tesla, Google and Uber. Self-driving car relies on Artificial Intelligence (AI) to work. In this, a number of sensors are embedded into the cars and data get transmitted to the cloud server and AI makes the decision. This will take few more years to evolve because it requires accuracy and people lives depends on it [15].

### 1.2.9. IoT Retail Shops

IoT has revolutionized the relationship of brand, product and customer. It bridges the gap of online store and a retail store. IoT provides personalized retail marketing and content delivery, wireless shipment tracking devices and optimal staffing level indicators. Due to efficiency of IoT in retail shops many brands have started using IoT in retail which is expected to grow to $94.44 billion through 2025. With the growth of IoT, GPS and RFID technology

will allow brands to track each individual item through the entire delivery process. It will also help retailer to go cashless by deducting money from your digital wallets [16].

#### 1.2.10. Smart Supply Chain management

Supply-chains have been using in the market for a while now and it has revolutionized supply management. Sensors and actuators helps in tracking goods while they are in transit. It aim to increase the efficiency in the supply management processes or to keep quality high in order to provide the services that customers demand [17].

## 1.3. IoTs: A Layer perspective

### 1.3.1. Perception Layer

First layer of IoT architecture is perception layer. In this layer, sensors and actuators are used to collect the raw data such as temperature, sounds, intruder detection and smoke. The key devices that are being used for data collections are RFID, sensors, cameras, etc. In IoT, plethora of data gets generated. The generated data gets transferred to transport layer where actions take place based on the collected information. Two types of devices are used which are:

**Sensors:** Sensors are the devices which converts signals from one energy domain to electrical signal. These devices are very small in sizes and measure physical input from the environment such as humidity or temperature. Due to small sizes, sensors take less power to accomplish their task. There are different types of sensors such as motion sensors, which detects the movement of large objects. Such devices helps in surveillance or monitoring of a patient.

**Actuators:** Sensors collect the information and then the data is processed, analyzed, and reported by actuators. These transforms the electrical signals into physical actions when required. For example, if there is any need to switch off the lights based on the temperature, actuator will analyze the data and trigger the switch off event. Actuators are an integral part of IoT networks

**Machine and devices:** These are the prominent part that have sensors and actuators.

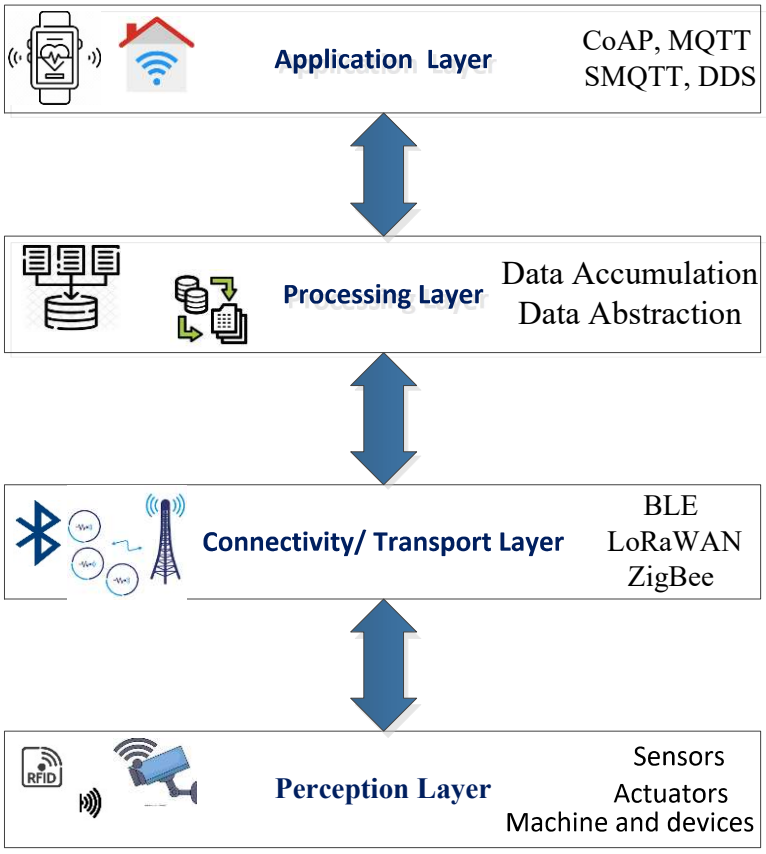



**Figure 1.2**. Architecture layer of IoT.

### 1.3.2. Connectivity/ Transport layer

This layer transmits the data from sensors to the processing layer. The connectivity is done in two phases: one transmission occurs from sensors to gateways, and second transmission is gateways to the processing layer. This layer maintains the communication of the network by using TCP or UDP/IP stack and various gateways. IoT gateways use specific communication protocol to transfer the data. Specific communication protocols are used to transfer the data from sensors to IoT gateways. Such communication channel have unique set of rules and standards. Some of the protocols are BLE, LoRaWAN, ZigBee and Sigfox. Further, data is aggregated at the gateways and send it to a backend system. It uses Ethernet, W-Fi, satellite, or cellular protocols to transmit the data to the backend. If sensors are self-

sufficient to transmit the data to a large distance then gateways can be omitted. In such cases, the sensory devices read the data and transfer it to a backend system.

### 1.3.3. Processing layer

Processing layer collects the data from the above two layers and convert it into meaningful information. It happens in two stages: Data accumulation, and Data abstraction.

**Data accumulation:** Data comes from various IoT networks and in different forms, speeds and sizes. In this phase, essential data is separated from the large stream of data. Unstructured raw data gets converted to readable form and transmit to the next stage.

**Data abstraction:** After completion of data accumulation, data is processed with the help of advanced analytics tools and gets filtered. It converts the data to value added information.

Interoperability plays a vital role at processing layer due to variety of devices and architectures. Accumulation and data abstraction helps data analytics in fetching intelligence factors of the data.

### 1.3.4. Application Layer

Application layer is the last layer of the IoT system and covers application level messaging. This layer connects end devices with the network. A dedicated application in the device implements this layer. Application layer is implemented by the application running in the device. For example, in a computer, application layer protocols such as HTTP, HTTPs, SMTP are implemented by browser. This layer is responsible for data formatting and presentation of the accumulated data. It helps users in decision making, and also to build artificial intelligence powered software for analytics solutions. The IoT devices are interconnected and can be accessed from any smart device such as smart phone or desktop. These smart devices have features like remote monitoring, alert system, and decision making. In IoT, HTTP protocol is not used because such kind of protocol cannot be execute on devices with constraint memory and processing power. Hence, new protocols are designed for IoT such as CoAP, MQTT, SMQTT, DDS.

## 1.4. Design issues of IoT

IoT plays a prominent role in day-to-day life such as healthcare service or smart home. However, such applications are facing various design issues which are interoperability, data mining, cloud computing, energy consumption, mobility, scalability, security and privacy, quality of service, GIS based visualization, self-configuring and self-organization, and reliability, and all are explain in further section.

### 1.4.1. Interoperability

Interoperable means the capability of devices to communicate or transfer data with each other regardless of different environment and networks. IoT is a dynamic global network infrastructure where devices are made by different manufactures which cannot be integrate. Second issue of IoT interoperability occurs due to limited connectivity between different transport protocols. Another issue of interoperability is there are no set of rules at application level which causes inability to process and combine data coming from different devices. Interoperability is a major challenge to handle the communication among heterogeneous devices belongs to different platforms. Diverse elements in IoT should seamlessly cooperate and communicate with each other to realize the full potential of IoT network [18,19].

### 1.4.2. Data mining

Data mining refers to the process of extracting useful information from the large amount of data. IoT collects huge amount of data from various small ubiquitous devices and large cloud servers. To obtain valuable information about the patient's health, home, and electricity consumption, data mining techniques are used. It helps in tracing hidden patterns and to make suitable decisions. For instance, sensor data from road and traffic can be used to analyze the optimal route for an ambulance. The data needs to be mine in real time considering the high speed, large volumes and dynamic natures of the real world [20,21].

### 1.4.3. Cloud computing

Cloud computing is the most important and centralized system of IoT. It helps to perform computing tasks and does not require on-site infrastructure for storage, processing and

analytics. Thus, increases processing power, and provides good storage capacity for low computing and low storage devices. It offers various services: Platform as a service (PaaS), infrastructure as a service (IaaS), and Software as a service (SaaS). The modelling of smart environment by integrating cloud computing and IoT causes various challenges such as data breach, data loss or network threats [20].

### 1.4.4. Energy consumption

In IoT environment, devices such as cameras, smart watches and speakers are always on watching, sensing and listening mode, whether user using it or not. The power consumption is minimal for one device, but over the period of time cost add up. If you forget to turn off your light, you can switch it off by swipe a button. But if your device is smart doesn't mean it is doing better job. As we know, IoT devices continuously talk with internet which consumes huge amount of energy [22,23].

### 1.4.5. Mobility

IoT network is made up of Mobile nodes (MNs) that utilizes Mobility Management Protocols (MMPs). MMPs provide transparent services and secure the sensing information of the MNs. Several issues and challenges impact the communication of mobile nodes such as packet loss, end-to-end delay, and increased handover latency [24].

### 1.4.6. Scalability

The explosive growth in the work of IoT need scalability to handle it. By adding additional resources scalability can be achieved but it remains a challenge for IoT developers. If such problems does not get resolved in early stages, it grows into problems that risk increased maintenance times and latency issues [25].

### 1.4.7. Security and privacy

As most of the devices in IoT are battery and storage constraint devices. As IoT devices have less processing and storage power this raises issues of security and privacy. Authentication, Identification and device heterogeneity are the pivotal issues in managing security and privacy

in IoT. For example, most of the devices in IoT environment communicates in plain text. It can lead to 'Man-in the-Middle' attack. Anyone who is capable of inspecting the network traffic can easily obtain the sensitive information such as login credentials [26,27].

### 1.4.8. Quality of service

Quality of Service (QoS) means to ensure the performance of the applications with limited network capacity. It affects the routing and data sharing capabilities of the communication links. Bad links in the routing protocols reduces the packet delivery time, end-to-end reliability and network lifetime. The key challenges and issues of IoT applications towards QoS are interoperability, reliability and end-to-end latency [28,29].

### 1.4.9. GIS based visualization

Big data technology plays a significant role within IoT processes, as visual analytics tools, generating valuable knowledge in real-time in order to support critical decision making. Integration of IoT and GIS helps in tracking the location of users and objects. Some of the famous examples are Uber rides, traffic conditions on maps. It offers number of benefits such as flow efficiency, cost efficiency and real-time response from the devices. Fusion of IoT and GIS has number of challenges such as storage and integration, and data security. The data generated by GIS has different formats such as images and videos and more which makes it difficult to integrate GIS into IoT [30].

### 1.4.10. Self-configuring and self-organization

IoT allows the interaction of ubiquitous devices without human intervention. Like any other infrastructure, IoT is also subject to disasters and adverse conditions. Network self-organization is needed to resist the hindrances in the communication [31].

### 1.4.11. Reliability

IoT systems have sensitive and substantial amount of data generating at regular interval of time. There are certain standard tests to ensure the reliability of the products. However,

defining the standard is not sufficient to maintain the reliability. Both hardware and software has to work in tandem to enhance the success rate of delivery in IoT [32].

## 1.5. Motivation

IoT has a significant economic potential, but is also consider as the vulnerable point for cybersecurity. IoT vulnerabilities comes from the devices that have low computational power and hardware limitations that don't allow strong security protocols and policies. The data collected by IoT devices are personal and need privacy. Most of the data collected in IoT devices are personal and need privacy. A number of security mechanism has been developed for IoT devices to protect them from cyber-attacks. But due to lack of appropriate security guidelines document, end-users are not able to prevent themselves from the data attacks. Hackers have developed various kinds of malware and phishing techniques to provoke the users to share sensitive data. Device manufacturers and security professionals can create an effective protective mechanism to prevent or neutralise cyber threats if they appropriately identify cyber risks.

The existing security techniques for secure communication cannot be applied directly in WSN-based-IoT because of the following reasons. First, energy of the sensor devices is constrained to make sensor network economically feasible [5], [6]. Second, unlike previous networks, sensor nodes are often deployed in remote areas, which increases the risk of physical attack [7]. Third, sensor devices in IoT have close interaction with the people and the surroundings, which augments the security problems [8]. Finally, IoT is a heterogeneous network, which consists of diverse kinds of sensor nodes for various types of applications [9]. Such heterogeneity may lead to noncooperative behavior of the sensor nodes with each other. To illustrate, a node thinks that its battery energy is the most valuable resource and decides not to forward others' data packets to save energy. This deteriorates the performance of the network and causes some serious attacks [10].

The public key infrastructure (PKI) plays a critical role in information security. In PKI, however, both the sender and the receiver authenticate each other with the help of certificates obtained from the certificate authority. This process can be time-consuming and complex. Identity-based cryptography (IBC) schemes remove these barriers and use public strings such

as email addresses or domain names for data encryption and signature verification, instead of digital certificates [4]. The security of IBC depends on solving some mathematical problems such as integer factorization and discrete logarithms. Major recent signature schemes depend on these two mathematical problems, which are infeasible to solve on any classical computer. However, these problems can easily be solved by quantum computers in polynomial time. For instance, Shor's quantum algorithm can solve the integer factorization in polynomial time [5]. Moreover, it can not only forge a signature but also recover private keys. Thus, such system poses serious threats to the modern cryptography. To effectively block these threads, many cryptographers are developing new quantum-resistant algorithms that are unbreakable in the era of quantum computers. Several postquantum cryptography (PQC) classes have been proposed which are currently believed to be quantum resistant, namely: lattice-based [6–8], hash-based [9],code-based PQC [10] and isogeny-based [11].

In IoT enabled system, it is essential to have a robust data encryption and authorization mechanism to preserve confidentiality, and prevent unauthorized access of sensitive data. Attribute-based encryption (ABE) gained much popularity to provide fine-grained access control over encrypted data [12, 13]. In addition to secure access control, efficient search over encrypted data is a vital concern in the IoT system. Searchable encryption has been extensively explored to retrieve the data of interest from system [14]. To furnish the searchable encryption and fine-grained access control, CipherText-Policy Attribute-Based Keyword Search encryption (CP-ABKS) has attained great interest from both academia and industrial communities [15]. In CP-ABKS, a user can decrypt the ciphertext only when his set of attributes matches the access policy, and generated trapdoor matches the indexes simultaneously. Although CP-ABKS is a solution for access control, but communication and computational cost increases linearly with the number of attributes [16]. This increment in cost is not feasible for resource-constrained IoT devices (biosensors) and may impede its wide range deployment, which demands an alternative solution [4, 6].

## 1.6. Problem statement

Despite of numerous advantages and potential applications of IoT, it has certain issues. Such issues needs to be addressed properly to enhance the efficiency and deployment of IoT

nodes in remote sensing environment. Billions of internet-enabled devices get connected to the huge network and it generates plethora of data. Such data comes from different framework which needs to be interoperable and device-to-device communication should be considered in such network. This lack of interoperability is a hurdle in the progress of everyday smart objects. Though old TCP/IP architecture used on the internet is heavy and degrades the performance of devices because of its data fragmentation and reassembly. IoT devices have low memory, energy and computation power which cannot sustain such heavy architecture. It is easy to exhaust the devices with few attacks because of its low power. Although several efforts have been done concerning to increase the lifetime of IoT network and to minimize the energy consumption. Such efforts do not incorporate security and overall performance of the network, and deteriorates the functionality of IoT.

Therefore, in this thesis, we propose energy efficient schemes for lightweight security that address the limitations of current methods based on energy usage due to unnecessary transmissions involved in the communication. In case of post quantum era, longer keys and more computation are required to maintain low level of security. Hence, the work proposes, lightweight postquantum ID-based signature scheme with reduced key sizes which is quantum-resistant. It has been shown that how such schemes can be used in real life scenario. Furthermore, the work is tested for comparative analysis of the performance with state-of-the-art schemes.

### 1.6.1. Objectives

In view of the above mentioned issues, following objectives were set to achieve the aim of security and energy efficiency for resource limited IoT netwok.

1. To design a light weight security model for internet of things to alleviate the malicious effects of illegitimate sensor nodes.
2. To design a signature scheme for protection against quantum attacks and with smaller key sizes.
3. To construct and deploy wireless body sensors using cloud technology to transfer medical records to the nearby fog server for data classification and remote monitoring with real-time responsive system for emergency situation.

4. To develop a certificate-less security mechanism for mobile social network.
5. To propose a model to provide secure environment for communication and data access between edge servers and cloud server.
6. To design a methodology which facilitates encryption of medical data and search mechanism based on keyword for maintaining the privacy of users.

## 1.7. Accomplishment and Contribution

The research has been performed to accomplish the above mentioned objectives and steps taken are explained as follows:

The comprehensive review and analysis of contemporary models concerning for security and energy efficiency in IoT considering to minimize the impact of attacks and maximize the longevity of the network. The literature based on IoT has been reviewed from scholarly digital libraries such as IEEE, MDPI, Sensor journal, Springer and ACM. Various issues have been identified in the literature survey and post vital issues have been addressed in the thesis.

In sensor-enabled Internet of Things (IoT), nodes are deployed in an open and remote environment, therefore, are vulnerable to a variety of attacks. Recently, trust-based schemes have played a pivotal role in addressing nodes' misbehavior attacks in IoT. However, the existing trust-based schemes apply network wide dissemination of the control packets that consume excessive energy in the quest of trust evaluation, which ultimately weakens the network lifetime. In this context, an energy efficient trust evaluation (EETE) scheme is proposed that makes use of hierarchical trust evaluation model to alleviate the malicious effects of illegitimate sensor nodes and restricts network wide dissemination of trust requests to reduce the energy consumption in clustered-sensor enabled IoT. Simulation results show that the EETE scheme outperforms the current trust evaluation schemes in terms of detection rate, energy efficiency and trust evaluation time for clustered-sensor enabled IoT**.**

Postquantum cryptography for elevating security against attacks by quantum computers in the IoT is still in its infancy. Most postquantum based cryptosystems have longer keys and signature sizes and require more computations that span several orders of magnitude in energy consumption and computation time, hence the sizes of the keys and signature are considered

as another aspect of security. To address these issues, the security solutions should migrate to the advanced and potent methods for protection against quantum attacks and offer energy efficient and faster crypto-computations. In this context, a novel security framework Lightweight Postquantum ID-based Signature (LPQS) for secure communication in the IoT environment is presented. The proposed LPQS framework incorporates a supersingular isogeny curve to present a digital signature with small key sizes which is quantum-resistant. It is evident that the size of keys and the signature of LPQS is smaller than that of existing signature-based postquantum security techniques for IoT. It is robust in the postquantum environment and efficient in terms of energy and computations.

Internet of Things (IoT) plays a crucial role in shaping the future of next generation eHealth (NGeH) system with unsurpassed context-aware, mobile, and personalized services. The growing demand of personalized NGeH services raises privacy, accuracy, and scalability concerns due to ever-rising extremely sensitive patient eHealth data. Hence, technical design of NGeH services should considered these issues to secure eHealth data from unauthorized breaches, certify accuracy in data sharing, and efficiently manage increasing eHealth data. In this context, a novel secure fog-enabled blockchain framework (SFBF) for NGeH services in IoT environment is proposed to efficiently manage and securely access patient's electronic medical health records (eMHRs). Security and simulation analysis are performed to demonstrate the efficiency and feasibility of SFBF.

The performance of the proposed schemes is analyzed by mathematical model and empirical evidence. Simulations are carried out in realistic IoT environment and results are generated with the help of NS-3, MATLAB, Microsoft Visual Studio and Yeoman. The different parameters have been observed like detection rate, energy consumption, clock cycles, computation cost, communication cost, average latency and throughput. The performance of the schemes is comparatively analyzed with state-of-the-art models.

## 1.8. Organization of the Thesis

The rest of the thesis is organized as follows. In chapter 2, literature survey of different security algorithms based on trust model are reviewed and further survey in categorized in cluster and non-cluster trust evaluation scheme. Survey of contemporary models for post-

Quantum and healthcare systems is also discussed. In chapter 3, an energy efficient trust evaluation scheme which uses the hierarchical trust evaluation model to alleviate malicious effects of illegitimate sensor nodes is proposed. A lightweight post-quantum ID-based signature (LPQS) scheme is discussed in chapter 4, which provide secure data transmission in the IoT environment and reduces the complexity of the system. In chapter 5, a secure fog-enabled blockchain framework (SFBF) for electronic healthcare system is proposed and security analysis is also performed to demonstrate the efficiency and feasibility of the proposed healthcare system. Finally, chapter 6 concludes the work presented in the thesis and some future work is also presented.

# Chapter 2

# Security Protocols Towards Green Computing in IoT: A Survey

---

Security and privacy of IoT devices have been a cause of concern for some time and hence studied intensively by the researchers. Various algorithms have been developed for key management, cryptography, secure routing, encryption, application security and protection of devices at production time. The security issues of IoT are not only associated with security of wireless medium, but also concern with access control, authentication, integrity and privacy of users. IoT network comprises of low power embedded devices which have less computation and storage power. Security algorithms are normally heavy weight and expensive to be execute on constraint devices. Trust management is also required in order to deal with internal attacks. Data authentication is require to maintain trust in the network. It can be achieve using strong cryptographic techniques or digital signatures. IoT network comprises of heterogeneous devices, integration of different IoT devices causes various compatibility and privacy issues.

In *Section, 2.1* various trust models in IoT have been reviewed and categorized in non-clustered and clustered trust evaluation approaches. In *Section 2.2,* post-quantum models are surveyed and security models for healthcare systems are reviewed in *Section 2.3*.

## 2.1 Trust model in IoT

In this section, related literature on trust evaluation approaches toward security concern in IoT has been reviewed focusing on non- clustered and clustered trust evaluation approaches.

### 2.1.1. Non-clustered Trust Evaluation Approaches

Several efforts in the research of trust evaluation have been made in recent years [33], [34], [35]. Cryptographic techniques-based storage system in IoT are used to provide the

scalability and secret data sharing. Although, IoT storage systems cannot handle the key management systems due to its complexity and availability. Shamir's secret sharing scheme provides small size secrets rather than large data management. In this technique, only first coefficient is used to save the secret. It also maintain the flexibility in the data management [36]. Still, the requirement of fixed infrastructure or central administration causes poor scalability and often makes this system prone to internal attacks. In order to improve the scalability and to provide the security from internal attacks, various trust computational processes have been presented by utilizing the numerical analysis and modeling tools, such as beta probability distribution and Dempster–Shafer theory (DST) model [37].

However, trust computation algorithms provide the security from the internal attacks but do not contribute toward optimizing the overall energy consumption. Direct trust depends on the node's own observation in promiscuous mode [38].

#### 2.1.1.1. Direct trust based on Bayesian theorem

Direct trust will be calculated by direct observation by the observer node. The node which sends the packet for transmission will overhear its successful delivery otherwise it will decrease the trust value of the observed node. The malicious node usually shows packet dropping or modifying packet attack. Therefore, observer node will determine trust value of its neighbor by using Bayesian inference which is general scheme for calculating the probability when there are lot of observations involved.

The prior distribution of unknown parameter $\theta$ is defined by a probability density function $f(\theta)$. The Bayesian inference associate with different parameters through likelihood function $f(\theta \vee q, p)$ where p is defined as packets send by node and q is the number of actual packets received by the node, and is defined by

$$f(\theta|q,p) = \frac{m(p \vee \theta, q) f(\theta, q)}{\int_0^1 m(p|\theta, q) f(\theta, q) d\theta} \tag{2.1}$$

Where $m(p \vee \theta, q)$ is the likelihood function which takes continuous value and follows binomial distribution:

$$m(p|\theta, q) = \binom{q}{p} \theta^p (1-\theta)^{q-p} \tag{2.2}$$

In theoretical framework, prior distribution for m can be continuous or discrete. It can take any value between 0 and 1. For the continuous probability distribution, beta distribution can be defined as:

$$Beta(\theta, \gamma, \delta) = \frac{\theta^{\gamma-1}(1-\theta)^{\delta-1}}{\int_0^1 \theta^{\gamma-1}(1-\theta)^{\delta-1} d\theta} \tag{2.3}$$

Where $0 \leq \theta \leq 1$, and $\gamma > 0, \delta > 0$. Then we have

$$f(\theta|q,p)\ Beta(\theta, \gamma + p, \delta + q - p) \tag{2.4}$$

The successful transmission ratio is defined by

$$S[\theta] = \frac{\gamma}{\gamma + \delta} \tag{2.5}$$

$$T^D{}_t = \sigma T^{DP}{}_t + (1-\sigma) T^{CP}{}_t \tag{2.6}$$

where $T^{DP}{}_t = S[\theta]_t = \frac{\gamma_t}{\gamma_t + \delta_t}$ in the same way for the control packet $T^{CP}{}_t = S[\theta]_t = \frac{\gamma_t}{\gamma_t + \delta_t}$.

#### 2.1.1.2.Indirect trust based on Dempster-Shafer theory

If we only consider the trust based on direct observation then we will not be able to detect various attacks by the malicious node. Let's say, in case of on-off attack, a malicious node intentionally behave differently with nodes or exhibit good or bad behavior alternatively. The malicious node behaves as a trustworthy node for a period of time and when trust value is established then it starts misbehaving. Detecting this kind of attacks are very troubling. Hence to achieve less biased trust it considers the opinion of other neighboring nodes in the region. In the literature, there are different authors which consider the neighbor's opinion as indirect trust. Although they directly have taken the arithmetic mean of trust values provided by the neighboring nodes, which is not appropriate because some of the nodes try to targets legitimate node by sending wrong recommendations which will decrease their trust value called as bad mouthing effect. For dealing with such kind of unreliable neighbors, DST is perfect. The DST evaluate the trust by considering all the hypothesis of nodes whether it is trustworthy or untrustworthy.

The trust is defined as

$$T = \rho T^D + (1-\rho) T^{ID} \tag{2.7}$$

Where $\rho$, $0 < \rho < 1$ is a weight assign to $T^D$.

Based on the trust model, the trust module calculates and updates trust value according to direct and indirect trust using Bayesian inference and weighted DST. The trust value is stored in the storage repository. Then routing protocol route the data and control packet based on the trustworthiness of nodes.

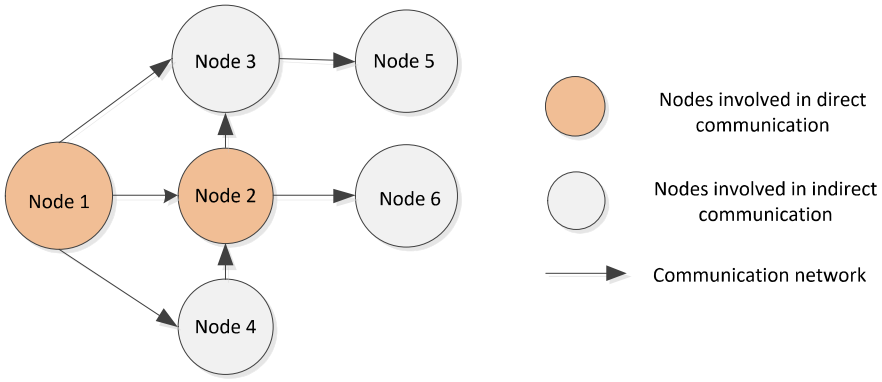



**Figure. 2.1** Trust model network in non-clustered environment

To explain the basic working of trust model, an example is shown in fig. 2.1. In this scenario, node 1 is defined to be observer node and observes node 2 whose trust value is denoted by $T_{AB}^D$. Node1 sends the data packet to node 6 using multihop communication via node 2. When node 6 will receive the data packet then node 1 will overhear the successful transmission. In the same way it is for the control packet. Node A will calculate the direct trust value $T_{AB}^D$ based on both data and control packet defined as

$$T_{AB}^D = \sigma T_{AB}^{DP} + (1 - \sigma) T_{AB}^{CP}$$

Where $T_{AB}^{DP}$ and $T_{AB}^{CP}$ are the trust value for the data packet and control packet transmission by the observer node A for the observed node B. $\sigma$ is the weight for the data packet and it ranges between $0 < \sigma < 1$. In case of indirect observation node 1 will receive the trust value recommendation from node 3 and 4, which are direct neighbor of node 2. On the basis of DST, the indirect trust value is measured.

However, if any node is out of range of the observer, then trust depends on the recommendations through the neighbors of the node which helps in preventing the bad-

mouthing attack. In order to counter the node's misbehavior attacks, a trust-aware secure routing framework (TSRF) has been proposed to mitigate the illegitimate recommendations of malicious nodes [39] with the help of multi hop trust path. TSRF analyzed various attacks such as Black hole, wormhole, Greyhole, Sybil and DOS, and developed countermeasures by combination of trust metric and other QoS metrics. The intensive computation incorporated due to the optimized routing algorithm makes the system slow and consumes the significant resources excessively. Focusing on the trust and energy in WSNs, a trust and energy aware routing protocol for wireless sensor network has been proposed for balancing the trust and energy in WSNs while detecting the malicious nodes during the trust evaluation process [40]. Although, this protocol is effective in enhancing the throughput and lifetime of the network while minimizing the load and delay. Yet, it is unable to capture the selfish nodes because of considering the communication trust only for the detection of malicious nodes in the system. Communication and data trust-based approach has been suggested in WSNs while utilizing Bayes theorem for direct communication and DST for indirect communication for resolving the problem of collusion attack, bad-mouthing attack, and selfish attack [41]. However, this approach does not comprise the mechanism for allocation of forgetting factor to reduce the number of malicious activities. Furthermore, the utilization of indirect trust in this approach not only improves the accuracy of the trust model, but also consumes more energy.

### 2.1.2. Clustered Trust Evaluation Approaches

Data collection and aggregation are the serious concern for clustered-based networks. In this context, energy-efficiency hierarchical clustering index tree (ECH-tree) using grid cells [42] and Smart-BEEM [43] have been proposed for IoT. These models focus only on the energy consumption while forming the clusters in the network. Further, while focusing on energy and trust formation in clusters, clustered based scheme for secure and efficient data transmission in WSNs has been proposed while utilizing the traditional PKI where every user is given a private key with a corresponding public key [44]. Furthermore, authenticity of users has been maintained with the help of a third party, known as a certificate authority (CA). The prominent issue while using PKI is the certificate management and the risk of central authority vulnerability which limits the use of cryptography in WSNs. A hierarchical dynamic trust

management protocol for cluster-based wireless sensor networks has been suggested while calculating the trust at intercluster and intracluster level using the social trust and QoS trust without centralized evaluation [45]. However, incorporating such a convoluted trust mechanism in the model at every CM is unachievable in the real scenario. A lightweight and dependable trust system for clustered WSNs (LDTS) has been proposed while focusing on the reduction of the communication overhead [46] and is shown in fig 2.2. This approach effectively reduces the memory and communication costs. Still, a static and stringent punishment has been taken into account for trust value computation. Recommendation-based trust model with an effective defense scheme for mobile ad hoc networks has been proposed without any central authority and complex system [47]. In this scheme, only highly trustworthy nodes have been considered for the legitimate recommendations which leads to high energy consumption, and is not well suited in WSNs applications.

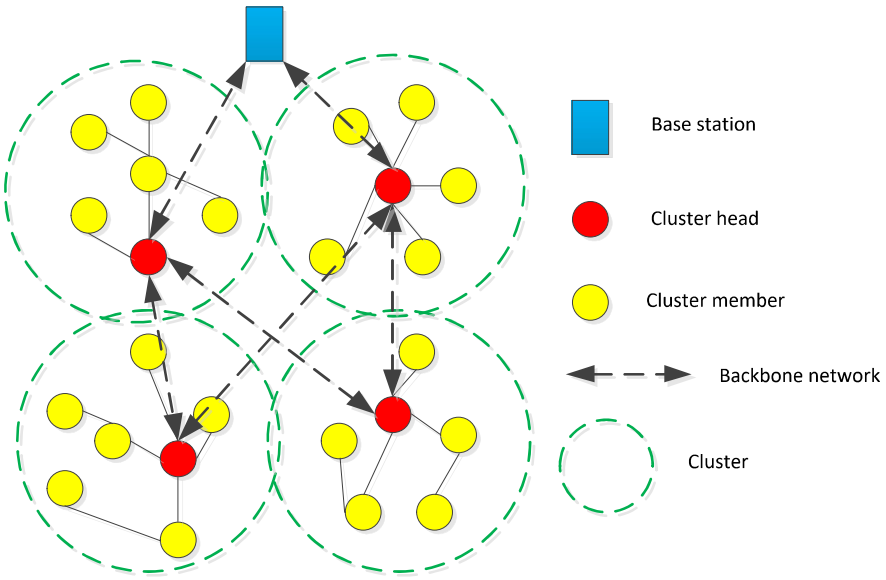



**Figure. 2.2** Roles and identities of nodes in clustered WSN network

An adaptive and dual data-communication trust approach for clustered WSNs has been suggested to reduce the malicious activity in the network [48]. Based on the error tolerance in terms of sensed data and packet loss, adaptive trust function for peer-to-peer cooperation has been formulated. However, this approach does not take into account the dynamicity of the clusters and limits the usage in WSNs applications. Game theory provides various ways to

model the strategic behavior among different entities [49], [50]. It is also useful for the cooperative behavioral analysis in WSNs. Nash Equilibrium base approach has been utilized to incorporate the energy efficient evaluation of the nodes for even utilization of the energy in the network [51]. However, it does not take into account the security and the past interactions of the nodes as well. A security and privacy protection technique using the co-operative and efficient equilibrium in the system has been suggested [49]. Still, this technique fails to mitigate the overheads caused by security and privacy mechanism. An energy-aware trust derivation scheme has been proposed to maintain the trust in WSNs using optimal number of direct and indirect recommendations while satisfying the security parameters [52]. However, the trust request in this scheme increases the overhead of the network. An energy efficient and reducing trust computation overhead, a model has been proposed [53]. In the proposed trust model, weighted trust list is maintain which guide in the process of data fusion. Furthermore, these schemes consider only co-operative behavior of the nodes, not non-cooperative behavior of the nodes while modeling the trust derivation process.

## 2.2. Post Quantum models in IoT

For security in sensor networks, Jao et al. [54] proposed a cryptosystem based on supersingular isogenies for encryption and key exchange which is much faster in contrast to the ordinary isogenies based schemes. This work was further extended by Plut et al. [55] and gave a public key exchange scheme which includes zero-knowledge proof of identity. This model achieves approximately 0.06 s per key exchange runtime operation as presented in test scenario. Costela et al. [56] proposed more efficient algorithms for computing isogenies. This algorithm have claimed to run 2.9 times faster than the scheme by Plut et al. Earlier, the isogeny based cryptographic functions were available only for key exchange protocol or public key encryption scheme. Thereafter, Galbarith et al. [57] proposed the first signature scheme based on supersingular isogeny problems. This scheme is resistant to chosen message attacks in the random oracle model. To achieve a small signature size a time–space trade-off is used which deteriorates the performance of the scheme. Hence, to improve the performance, a signature scheme based on isogeny-based zero- knowledge proof have been suggested which further reduces signature size with small

key sizes [58,59]. However, this scheme suffers from poor performance compared to the other postquantum schemes.

Elliptic Curve Cryptosystem (ECC) based models have been very prominent in IoT. Considering the efficiency of ECC, Malasri et al. [60] gave an authentication scheme for medical sensor networks. As a result, this model could maintain confidentiality and message integrity. In this key management scheme, every step computes the message authentication code, which depletes the resources and delays the packets' processing at the receiver end. Further, Oliveira et al. [61] gave a secure scheme for sensor networks based on IBC and proved it to be practical for resource-constrained nodes. In this scheme, senders broadcast their identities with no security measure and it allows adversaries to broadcast several fake identities and helps them to launch denial-of-service (DoS) attacks. This attack reduces the power of low computation devices. Tan et al. [62] proposed an identity- based cryptography scheme for the security of body sensor networks. This approach uses a hash function for public key generation and stores the key on the sensor's flash memory. Further, this model uses the public key for the computation of elliptic curve encryption/decryption using the Elliptic Curve Digital Signature Algorithm (ECDSA). For public key computation, this scheme requires more storage, energy and computation time. Sankaran et al. [63] gave an IDKEYMAN which uses IBC for wireless body area networks parties to exchange symmetric keys. The pairwise symmetric keys support the minimization of energy consumption.

In addition, this approach provides security from replay attacks by using ephemeral values. This technique does not provide protection against other attacks like selective forwarding, Sybil, etc. Li et al. [64] proposed a biometric-based scheme where physiology signals like electrocardiogram are used to create keys and transmits them in a safe mode. This biometric-based scheme improves the network security and increases the lifetime of the model by using fuzzy commitment and an arbitrated-based approach. However, this approach is limited to a wireless body area network only. Ma et al. [65] proposed a practical access control technique based on IBC for the Internet of Things (IoT). This signcryption scheme provides a reduction in energy and less computation cost with large area applicability [66].

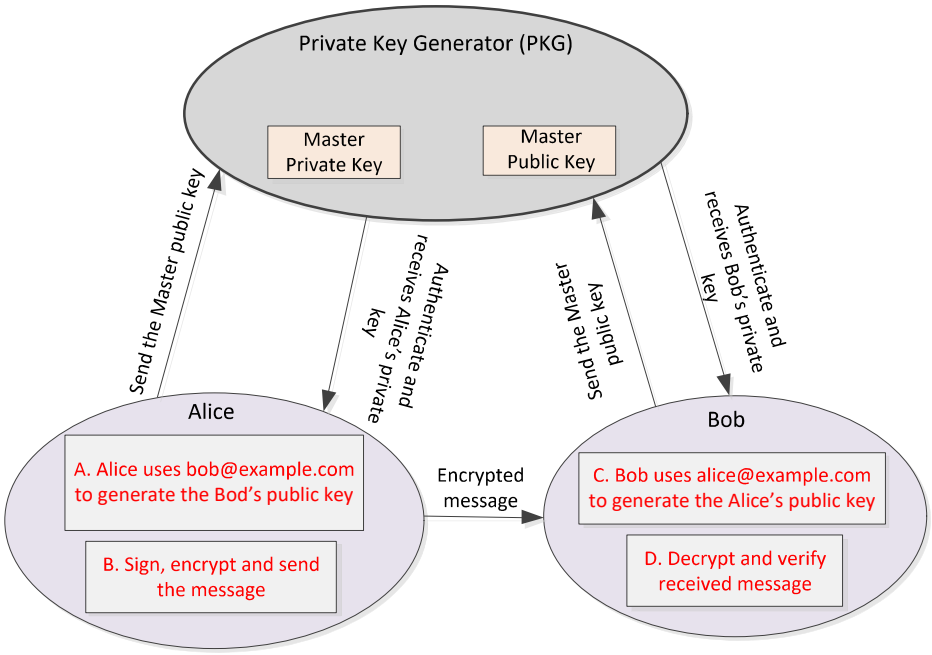



**Figure 2.3.** Flow chart of Identity based encryption.

Public key cryptographic algorithms depend on the hardness of integer factorization and discrete log problems. However, these algorithms will be vulnerable to attacks from quantum computers. Considerable research has been conducted for postquantum cryptography. Among various postquantum techniques, the lattice-based signatures [67] scheme is prominent and based on the hardness of NTRU (Nth degree Truncated polynomial Ring Units) problems with no algebraic structure. The limitation of these techniques is that they have large public and private keys and are not feasible for many practical applications. Another candidate for postquantum cryptography is multivariate-based signatures [68]. These signatures are based on the multivariate quadratic polynomial problem. These models have a smaller signature but large key sizes and are difficult to scale to higher security levels [69]. Furthermore, hash-based techniques have small key sizes but are inefficient in terms of speed. Hence, none of the abovementioned techniques are feasible for the IoE environment [70]. Because of the small key size, isogeny-based cryptography is a suitable candidate for the IoE environment. An isogeny-based cryptosystem depends on the difficulty of computing isogeny between two given curves of the same order.

The first isogeny-based cryptosystem for public key encryption and the key exchange was a traditional model without considering quantum computing. However, Childs et al. [71] proposed a postquantum algorithm that computes ordinary isogenies in subex- ponential time. Since the algorithm relies on the commutative property of endomorphism rings, it does not apply to the supersingular singular case [72]. Feo et al. [73] gave a signature model using class group actions for the 128-bit security level. This model uses only a 1 KB signature size and maintains adequate security in the random oracle model. Parrilla et al. [74] have suggested a unified coprocessor framework in order to run the ECC on IoT devices. The group key support strategy is also incorporated for reducing the communication overhead in key distribution. Similarly, to deal with malfunctioning of the IoT enabled systems, Hussein et al. [75] investigated a secure protocol to maintain the secrecy rate in IoT environments and to reduce the energy consumption at IoT nodes. However, both these ECC frameworks are vulnerable against quantum attacks as edge centric faster and efficient security enabler nodes have not been considered to support the security operations of resources constrained IoT nodes. Quantum centric security analyses have been also missing in the analytical investigation of these approaches.

## 2.3. Security models for healthcare system

In recent years, electronic healthcare systems have received huge attention from the researchers leveraging the technologies of cloud computing and IoT [76] and a fremwork is shown in Fig 2.4. Zhang et al. [77] designed a 3-layered architecture for the cyber-physical healthcare system. As the data is collected at the data collection layer with the help of various data nodes and adapters. Through adapter, availability is maintained by formatting the data. Second layer is data management layer, which consists of distributed file storage (DFS) and distributed parallel computing. Efficient data storage provided by DFS enhances the data storage. Finally, at application layer users can view the analyzed data results. It is a user-centric application which provides various rich and professional healthcare services. To deal with the diversity of objects in IoT, Xu et al. [78] presented a model for ubiquitous medical emergency services. They proposed a resource-based accessing method to store, integrate and interoperate flexible IoT data for emergency medical services. To improve the accessibility, a

ubiquitous data accessing method based on RESTful architecture is used. Further, implementation has shown the benefits for doctors and patients as well.

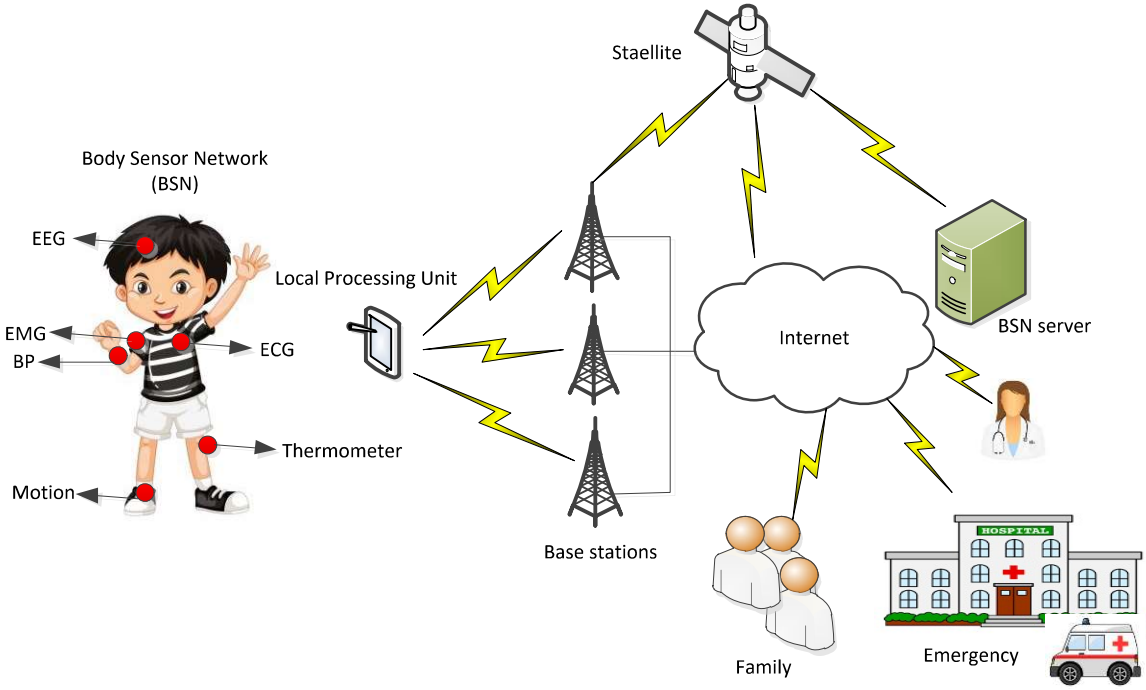



**Figure 2.4.** A framework of healthcare system.

Muhammed et al. [79] gave a ubiquitous healthcare framework (UbeHealth) to resolve the issues of bandwidth, latency and reliability among the users. UbeHealth system incorporates three main components Deep learning, big data and HPC. These components are used by the four layer which are Mobile layer, Cloudlet layer, Network layer, and cloud layer and is shown in Fig 2.5. Further, cluster method used to classify the data originating from the same source. Mehmood et al. [80] proposed a transport sharing for the healthcare system in a smart city. This model leverages big data to improve the transport sharing capacity and efficiencies in meeting the demand for city services. The transport sharing capacity is improved by using the Markov models which is integrated with future city transport sharing and big data. Mohammed et al [81] proposed a smart hospital emergency system (SHES) to provide communication between patients and emergency service providers via mobile phone requests. SHES primarily handles the emergency calls in real-time response system. SHES is an mobile app which handles the emergency and accident requests. Hence, users can request for

ambulance an doctors can response to query raised by user or if required can send the ambulance. It also provides video communication which enhances the two way communication between patients and doctors, to provide first aid instruction remotely.

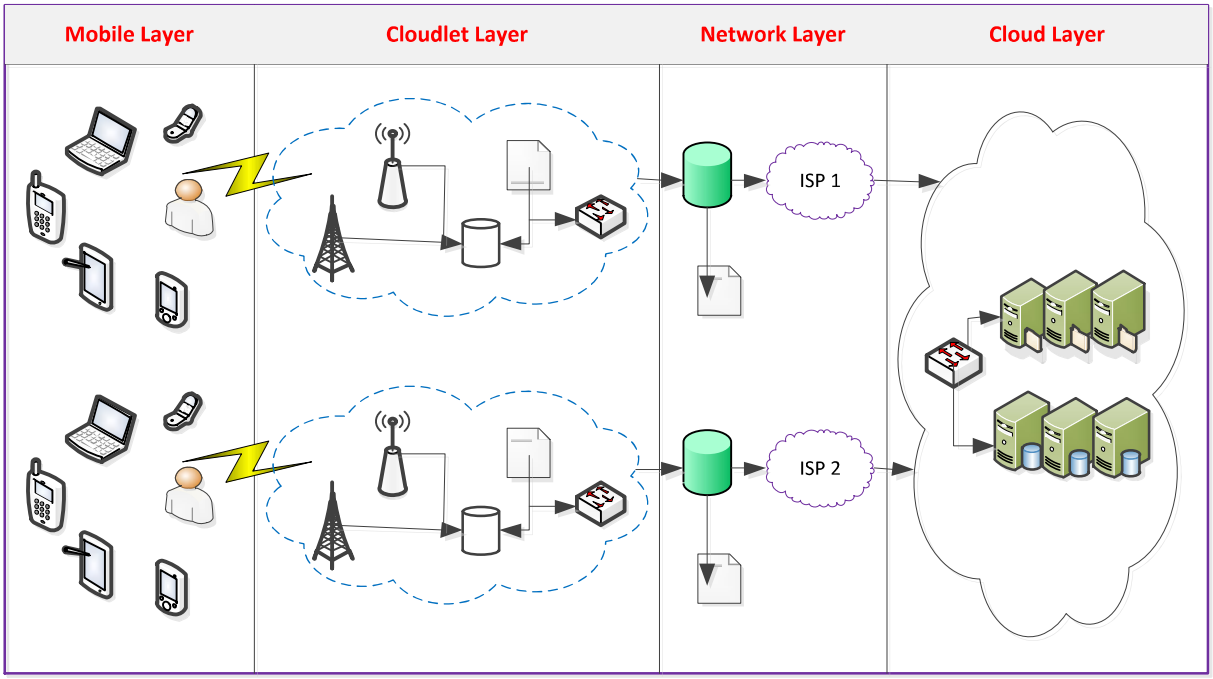



**Figure 2.5** Architectural overview of UbeHealth.

Miao et al. [82] proposed a verifiable conjunctive keyword search to share the data among multi-owner. They shared a single copy of the health records among the group of users by using group signatures. This model is secured against keyword guessing attack. However, all the healthcare systems lack secure communication, access control and do not provide privacy of the patients.

To provide fine-grained access control, Guo et al. [83] explored Ciphertext-policy attribute-based encryption (CP-ABE) schemes in the semi-trusted cloud environment. In CP-ABE scheme, users' secret keys depend on the set of attributes and stored in cloud in encrypted form. However, sharing of electronic health records is also done in encrypted form. In this framework, data return to users depends on the given privilege.

***Attribute Based Encryption***

ABE is a powerful and promising mechanism, where a trusted authority generates public and secret key pair for a user, based on attributes which can be used as an identity of the user [84,85]. In this scheme, messages are encrypted with respect to the set of attributes, and decryption is done only when the receiver has a matching key for the same set of attributes as shown in Fig 2.6. The ABE scheme consists of five fundamental algorithms: System Setup, Key generation, Encryption, Trapdoor, and Decryption.

1. System setup

   ***Setup****(λ,* ℕ*)* → *(pp, MSK, MPK)*: Trusted authority (TA) runs the S$etup$ algorithm. The algorithm takes the implicit security parameters (λ) and an attribute universe ℕ as inputs. It generates public parameters *(pp)*, master secret key (*MSK*) and master public key (*MPK*) as outputs.

2. Key Generation

   ***KeyGen****(MSK, id, s)* → *(sk, pk)*: The KeyGen algorithm takes the *MSK*, identity of user *id* and user's attribute set *s* as inputs. It generates the user's secret key *sk* and public key *pk* as outputs.

3. *Data Encryption*

   ***Encryption****(p,* ℕ, *A*, pk, sk, M*)* →*(C, I):* Encryption algorithm runs by owner of the data. This algorithm takes inputs public parameters, attribute universe ℕ, access structure *A*, public key *pk*, secret key *sk*, and message *M*. It outputs cipher-text *C* and data index *I*. Only the user with the valid access structure would be able to decrypt the message *M*.

4. *Trapdoor*

   ***Trapdoor****(MPK, sk, w)* →*P*: This algorithm takes TA's master public key, secret key *sk* of receiver and keywords *w* as inputs and outputs the trapdoor *P*.

5. *Data Decryption*

   ***Decryption****(A, C, sk)* →*(k, M):* Before sending the encrypted file to the requester, cloud server test the access structure *A* of the trapdoor using its secret key. If the access structure does not match with pre-defined structure, cloud server terminates the algorithm,

otherwise, sends the encrypted file $C$ to receiver. The receiver first decrypts the symmetric key $k$ and then retrieves the message $M$.

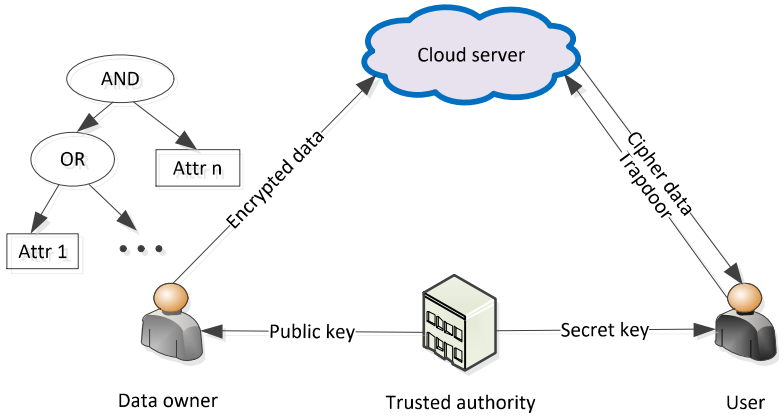



**Figure 2.6.** Attribute based encryption.

To maintain the patient's confidentiality, Zhao et al. [86] enhanced the attribute-based encryption and constructed a structure for fine-grained attribute revocation into m-healthcare cloud computing systems. To accomplish the confidentiality of electronic health record, a universal set of attributes is selected and a set of $s$ attributes is selected from universal set to encrypt the medical data. It also provides revocation list for every attribute which supports attribute/user revocation and electronic health records achieve flexible access control. However, ciphertexts sizes are larger and this structure gives lower efficiency. Miao et al. [87] leveraged the fog computing, searchable encryption and CP-ABE to devise a fine-grained access control mechanism, and improved the conjunctive keyword results. Fog computing helps in partial computational and storage overhead, and reliefs the end users. Further, to avoid the irrelevant search results and illegal accesses conjunctive keyword search and attribute update are incorporated. This scheme is secure against Chosen-Keyword Attack (CKA) and Chosen Plain-text Attack (CPA). To support large attribute set, Zhang et al. [88] proposed a fast decryption method with linear public parameters and achieve full security in static assumptions. In the proposed scheme, only encryptor knows the values of attributes and do not send with the ciphertext. Only the access matrix and the defined function are sent to the

decyrptor along with the ciphertext. Hidden Ciphertext Policy Attribute-Based Encryption supports fast decryption. The reduction in speed is due to the reduction of bilinear pairing evaluations to a constant in decryption phase.

It might be noted that all the above schemes provide fine-grained access control but do not provide privacy preservation and efficient computational cost. Attribute based encryption (ABE) provides fine grained access control but leak the privacy of access policy which can also conatin sensitive information. Further, users' devices have limited bandwidth and limited computing power which does not allow the efficient keyword search on encrypted data. Wang et al. [89] employed an efficient hidden policy ABE for efficient keyword searches on encrypted data with constant computational and storage overhead. Hao et al [85] gave an attribute-hiding policy for cloud-based IoT to hide the attribute information in order to preserve the privacy policy. Although, privacy preserving policy is used but resisting dictionary attack is still feasible. A fuzzy attribute positioning mechanism based on garbled bloom filter is used to prevent unauthorized recipients. In this model, authorized recipients can successfully decrypt the data if the validation of the results occurs happens and for unauthorized recipients no valuable attribute privacy can be compromised. It helps in fine grained access control, and protect the data confidentiality and policy privacy. Chen et al. [90] removed the problem of key delegation abuse by using a directed graph and Cipher-Policy hierarchical attribute-based encryption. In order to prevent higher level domain authority to forge a user attribute private key for unauthorized users, a level key parameter is incorporated into the user attribute private key. It also reduces the amount of workload from the root authority and achieves scalability of the system. In case of key leak, the identity of the key holder can verifiably track. The existing ABE schemes are inflexible and efficiency is restricted for resource-constrained devices.

To achieve immutability and non-traceability of eMHR, Wang et al [91] gave a combined attribute-based/ identity-based encryption and signature scheme which uses different functions of attribute based encryption, identity based encryption and identity based signature in one cryptosystem for healthcare system. It removes the overhead of introducing different cryptographic systems for different security requirements and incorporates the fine grained access control of the medical data. In addition, blockchain ensures the immutability of the

medical records and traceability of the user. Niu et al. [92] explored the permissioned blockchains and ABE to provide secure search in the healthcare system. This model solves the problem of limited blockchain storage space by storing keywords and ciphertext separately on permissioned blockchain and hospital cloud storage servers. Sometimes multiple keywords generate arbitrary connection and to find the connection polynomial equations are used. It not only supports multi-keywords search but also improves the integrity of retrieved data. This work ensures the patients' privacy and is resistant to the chosen keyword attack under random oracle model. Guo et al. [93] gave an attribute-based signature scheme with multiple authorities and enhanced the distributed data storage in the blockchain. One of the challenge for multiple authority is collusion attack. To deal with this attack, two authorities shared a pseudorandom function seed secretly. In addition, private key of each patient encapsulates the private key of authority. This structure helps in preventing $N-1$ corrupted collusion attacks. This model provides the perfect privacy for the signer and is unforgeable in suffering a selective predicate attack under assumption of the computation bilinear Diffie-hellman. But the cost of this protocol increases linearly with the number of attributes and patients. Further, Guo et al. [84] incorporated ABE for flexible and efficient medical on demand services in telemedicine. They also used blockchain for integrity to avoid the misguidance accident from inaccurate eMHR distributed by a malicious user. Zhang et al [94] proposed a data-sharing architecture with attribute-based signature. The access policies are set on the encrypted key where encrypted keys are encrypted by attributes. This model provides fine-grained access control and user-controlled data sharing. They used smart contracts to send the data sharing requests and enhanced the scalability of network. Also, this model incorporates the Byzantine Fault tolerance mechanism, rather than Proof of Work. Further, Nguyen et al. [95] presented a comprehensive data offloading and data sharing prototype based on blockchain for mobile cloud e-health applications. Blockchain also provides user access control mechanism and decentralized storage interplanetary file system helps in protecting health database. It manages data access from network entities and effectively restrict illegal access to EHRs resources. Moreover, to improve the security of EHRs sharing, smart contracts are used to develop a trustworthy access control mechanism. Smart contracts are implemented on an Ethereum blockchain platform on Amazon cloud in order to verify the user identification, authentication,

access control capability of smart contract and system integrity. Further, Sulatana et al. [96] also used smart contracts to provide efficient access control and authentication mechanism. In this model, multiple smart contracts such as access control contract (ACC), Register contract (Rc) and Judge contract (JC) are developed. These smart contracts mitigate misbehavior activity and maintain trust in the network. Notably, all existing healthcare model's computation, communication and storage costs increase linearly with the number of attributes and patients, and hence cannot be deployed on resource-constrained devices. Further, maintaining privacy and accuracy of eMHR in emergency conditions is a difficult task.

## 2.4 Research Challenges

As IoT in its infancy stage, based on review, various research challenges have been observed and are explained in further section.

### 2.4.1 Scalability

The explosive growth in the work of IoT need scalability to handle it. By adding additional resources scalability can be achieved but it remains a challenge for IoT developers. If such problems does not get resolved in early stages, it grows into problems that risk increased maintenance times and latency issues [25].

### 2.4.2 Privacy

As most of the devices in IoT are battery and storage constraint devices. As IoT devices have less processing and storage power this raises issues of security and privacy. Authentication, Identification and device heterogeneity are the pivotal issues in managing security and privacy in IoT. For example, most of the devices in IoT environment communicates in plain text. It can lead to 'Man-in the-Middle' attack. Anyone who is capable of inspecting the network traffic can easily obtain the sensitive information such as login credentials [26,27].

### 2.4.3 Energy consumption

In IoT environment, devices such as cameras, smart watches and speakers are always on watching, sensing and listening mode, whether user using it or not. The power consumption is minimal for one device, but over the period of time cost add up. If you forget to turn off your light, you can switch it off by swipe a button. But if your device is smart doesn't mean

it is doing better job. As we know, IoT devices continuously talk with internet which consumes huge amount of energy [22,23].

### 2.4.4 Internal attacks

Cryptographic techniques based on public key schemes require high computational capabilities and even higher energy consumption. Such techniques can be applied for external threats but it is difficult to prevent internal attacks. Such internal attacks drain the energy of the system and increases the complexity and often makes the system prone to internal attacks.

### 2.4.5 Public keys and digital certificates

IoT network is composed of large number of devices. To maintain security and privacy based on public key infrastructure huge amount of public-private keys are required. However, most of the IoT devices have low storage capacity which cannot hold such amount of data at such small platform. It raises concerns of maintaining public keys and digital certificates, and in this aspect new infrastructure is needed where IoT network can be remain secure and efficient.

## 2.5. Summary

In this chapter, various security and energy efficient methods and algorithms have been discussed that solve different problems such as security, privacy, trust and confidentiality. Firstly, several trust evaluation schemes based on cluster and non-cluster approach for IoT are reviewed to maintain equilibrium among security, privacy and energy. Considering the efficiency of quantum computers, various post-quantum models for IoT are presented which could provide security in such era with their limitations. Further, Electronic healthcare system is an important aspect of day-to-day life in such pandemic environment. Hence, number of security issues are discussed for the implementation of electronic health care system such as confidentiality of electronic health records, privacy of patients and scalability. Finally, various security and privacy research challenges are presented.

# Chapter 3

## Trust Evaluation for Light Weight Security in Green IoT

---

In sensor-enabled Internet of Things (IoT), nodes are deployed in an open and remote environment, therefore, are vulnerable to a variety of attacks. Recently, trust based schemes have played a pivotal role in addressing nodes' misbehavior attacks in IoT. However, the existing trust based schemes apply network wide dissemination of the control packets that consume excessive energy in the quest of trust evaluation, which ultimately weakens the network lifetime. In this context, this chapter presents an energy efficient trust evaluation (EETE) scheme that makes use of hierarchical trust evaluation model to alleviate the malicious effects of illegitimate sensor nodes and restricts network wide dissemination of trust requests to reduce the energy consumption in clustered-sensor enabled IoT. The proposed EETE scheme incorporates three dilemma game models to reduce additional needless transmissions while balancing the trust throughout the network. Specially, 1) a cluster formation game that promotes the nodes to be cluster head or cluster member to avoid the extraneous cluster. 2) An optimal cluster formation dilemma game to affirm the minimum number of trust recommendations for maintaining the balance of the trust in a cluster. 3) An activity based trust dilemma game to compute the Nash equilibrium that represents the best strategy for a cluster head to launch its anomaly detection technique which helps in mitigation of malicious activity. Simulation results show that the proposed EETE scheme outperforms the current trust evaluation schemes in terms of detection rate, energy efficiency and trust evaluation time for clustered-sensor enabled IoT.

This chapter presents the research work carried out to perform the trust evaluation for Internet of Things (IoT) devices using game theory approaches. Three different game approaches are used for network optimization. *In Section 3.1*, a brief introduction of IoT underlying the security issues of the network is presented. *In Section 3.2*, provides the basic

structural design of the network and a trust model to explain the belief computation of the nodes in the network. *In Section 3.3,* presents the proposed EETE scheme in detailed form. The simulation and performance evaluation of the proposed EETE scheme is presented in S*ection 3.4.*

## 3.1. Introduction

IoT refers to the networked interconnection of everyday objects, which are uniquely identifiable and have ubiquitous intelligence in an internet-like structure [97] [98]. IoT devices simplifies and bring convenience to day-to-day life of peoples. With a lot of efforts and research, IoT ponders various applications in numerous areas, such as medical care, agriculture, automotive etc. [99]. In spite of the advancement in IoT, a number of issues are still unsolved. . The most important challenge of a network deployed in IoT environment is security which hinders development and the applications of IoT, especially for a WSN-based IoT [100].

The existing security techniques for secure communication cannot be applied directly in WSN-based-IoT because of the following reasons. Firstly, energy of the sensor devices is constrained to make sensor network economically feasible [101], [102]. Secondly, unlike previous networks, sensor nodes are often deployed in remote areas, which increases the risk of physical attack [43]. Thirdly, sensor devices in IoT have close interaction with the people and the surroundings, which augments the security problems [103]. Finally, IoT is a heterogeneous network, which consists of diverse kinds of sensor nodes for various types of applications [104]. Such heterogeneity may lead to non-cooperative behaviour of the sensor nodes with each other. To illustrate, a node thinks that its battery energy is the most valuable resource and decides not to forward others' data packets to save energy. This deteriorates the performance of the network and causes some serious attacks [105]. Cryptographic based system is one of the most practical systems to counter the security issues in communication networks. However, these cryptographic techniques are not suitable for WSN-based-IoT since cryptographic techniques based on public key schemes require high computational capabilities and even higher energy consumption. Such techniques are not applicable to maintain the

security in low-cost sensor nodes, which generally have the sparse energy and low computational power. Still, requirement of fixed infrastructure or central administration in cryptography causes poor scalability and often makes this system prone to internal attacks [36].

Because of the less computation complexity and high resistance to the internal attacks, trust evaluation is an efficient alternative to resolve the pre-mentioned issues in the public key infrastructure (PKI) [106], [107]. Therefore, trust plays a pivotal role in securing communication for sensors enabled IoTs. However, the wrong information communicated from malicious nodes may misguide the network. Further, in the existing clustered WSNs trust management system, cluster-heads play the key role in the aggregation of collected trust values and forward it to the desired cluster [108]. However, the network may contain numerous illegitimate nodes. These nodes provide certain recommendations that may result in inaccurate evaluation of trust values during the trust aggregation performed by the cluster-heads. Similarly, a base station also suffers from the same problem while calculation of the cluster-head trust value.

Trust computation has been the key focus area for the most of the recent trust models for IoT [52], [53]. Since, a number of recommendations received in trust computation, decide the accuracy of the trust model, and the process of deriving trust that elaborates the broadcasting of the recommendations, is quite significant. The nodes with low bandwidth and limited battery power do not incorporate with the performance of trust derivation model. Further, non-cooperative behavior of the nodes unbalances energy consumption among nodes and compromises the security of the network. It not only leads to bad-mouthing attack but also deteriorates the limited resources of the network. Recently, few methods have been proposed to optimize the number of trust recommendations based on weighting [109], matrix theory [106], Bayesian statistics [33], Beta distribution [110] and game theory [111]. However, applications of these methods consume more energy, increase the complexity of the network, and make the network vulnerable to various attacks [38], [112], [34]. Hence, designing a more attestable energy efficient trust derivation scheme that mitigates the effects

of the non-cooperative behavior of the nodes has become a prominent requirement in sensor enabled IoT networks.

In this context, this chapter proposes an energy efficient trust evaluation (EETE) scheme for lightweight security that addresses the limitations of the current trust evaluation schemes based on energy usage due to unnecessary transmissions involved during trust calculation process. The design of the proposed EETE aims to maintain trustworthiness and energy efficiency of the network. To achieve the aim, the EETE scheme includes three dilemma games to reduce additional needless transmissions. The objective to propose three dilemma games is to create clusters with optimal number of replies to maintain the trust of the individual clusters and to mitigate malicious activity in the network. The main contributions of the proposed scheme are summarized as:

1) Firstly, a system model for the trust computation is presented focusing on intra-trust and inter-trust evaluation of the nodes.
2) Secondly, an energy efficient EETE algorithm is proposed using three dilemma games for cluster formation and detection of malicious activities in the network.
3) Thirdly, three dilemma games for cluster formation, cluster size optimization, and computing the Nash equilibrium to detect illegitimate nodes, are developed.
4) Finally, the proposed EETE scheme is tested for comparative analysis of the performance with state-of-the-art schemes focusing on trust evaluation performance and security related parameters under IoT.

## 3.2. SYSTEM MODEL

In this section, we present a network model to provide the basic structural design of the network, a security model to give security aspects of the nodes and a trust model to explain the belief computation of the nodes in the network. Symbols used in this chapter are given in the Table 3.1.

### 3.2.1 *Network Model*

We consider $n$ number of sensor nodes, deployed randomly in a network field. All these nodes are equipped with limited power batteries and have equal short radio range. A base station with unlimited source of energy as a central administrative authority is also deployed in the network field. It is also considered that the nodes of the network form clusters. A cluster consists of cluster members and a cluster head. For end-to-end communication between any two nodes, multi-hop transmission is used which rely on intermediate nodes.

**Table 3.1.** Symbol description

| Symbol | Description | Symbol | Description |
|---|---|---|---|
| $E_h$ | High energy nodes | $G_{i,j}$ | Gain of player i for player j observation |
| $E_L$ | Low energy nodes | $P_w(a)$ | Positive behavior weightage |
| α, β | Weight factors | $N_w(a)$ | Negative behavior weightage |
| $CH$ | Cluster head | $S$ | Strategy set |
| $CM$ | Cluster member | $E_{th}$ | Energy threshold |
| $T_h$, | High trust value | $\Delta E$ | Residual energy |
| $T_L$ | Low trust value | $U_i$ | Utility of $i^{th}$ player |
| $k$ | Minimum number of nodes in a cluster | $p_i$ | Probability of CH to choose a strategy |
| $\theta, \varphi$ | Weight factors | $q_i$ | Probability of CM to choose a strategy |

### 3.2.2 *Trust Model*

Sensor-enabled IoT is generally vulnerable to various attacks due to its deployment in open and remote environment. We consider that the nodes may act maliciously. These malicious nodes launch two types of attacks in the network: 1) Internal attacks like bad mouthing attacks, packet forwarding/modification attacks, collusion attacks and on-off attacks and 2) External attacks such as denial of service (DoS), black-hole attack and wormhole attack [113]. The internal attacks are more difficult to capture as compared to the external attacks.

Trust model in communication networks commonly drives and evaluates trust for decision making on future actions of the nodes which is based on past observations of the node's behavior. The base station acts as a highly trusted party with more advanced hardware. The cluster heads are responsible for the trust evaluation in their clusters and for communication with the base station. Trust model consists of mathematical formulation of Intra-cluster trust evaluation, Inter-cluster trust evaluation to balance the trust level and to mitigate the malicious activates in the network.

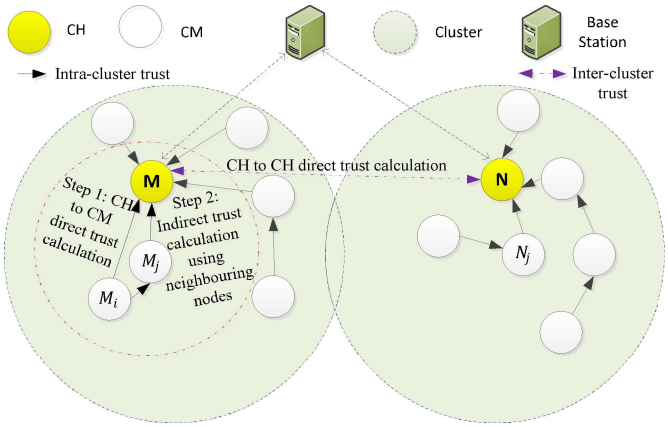



**Figure. 3.1.** Roles and identities of nodes in cluster-based sensor enabled IoT.

### *3.2.2.1 Intra-Cluster Trust Evaluation*

Centralized trust evaluation is performed using intra-cluster communication where each cluster member maintains the trust values of the neighboring nodes. We consider that trust is a continuous value scale [0, 1] where the value 0 means malicious, the value 0.5 represents suspicious, and the value 1 represents complete trust. Direct trust of a node is the belief received from the node using direct communication.

In Fig. 3.1 the cluster head $M$ receives the direct trust from the node $M_i$. Indirect trust of a node is the belief received from its neighbours. The node $M$ computes indirect trust with the help of the neighbours ($M_j$ ,$M_l$) of the node $M_i$ in promiscuous mode. Both direct and indirect trusts resist to prevent attacks such as bad mouthing. All the trust computations are

performed at each cluster head of all the clusters. Each cluster member retains trust of all its neighbours and forwards trust information to its cluster head on the demand basis. The trust of the node $M_i$ in the cluster $M$ can be computed as

$$Trust\ (M, M_i)^t = \alpha_1 . DT(M, M_i)^t + \beta_1 \frac{\sum_{j \in nbr_i, j \neq i} IT(M_j, M_i)^t}{|nbr_i| - 1}, \quad (3.1)$$

where, $\alpha_1 + \beta_1 = 1$, $\alpha_1 > 0$, $\beta_1 > 0$. The $\alpha_1$ and $\beta_1$ are the weight factors which are associated with the access control policies. If $\alpha_1 \geq \beta_1$, it means the trust of the node $i$ using direct communication is more than the trust computed using its neighbour's information. Similarly, if $\alpha_1 < \beta_1$ it represents the higher dependency on the indirect trust than direct. As in Eq. (1), $Trust\ (M, M_i)^t$ represents the trust value of node $M_i$ in the cluster $M$ at round $t$. It is calculated using the trust value denoting $DT(M, M_i)^t$ obtained from the direct communication with the cluster head, and indirect trust $IT(M_j, M_i)^t)$ obtained from its neighbour $(nbr_i)$. Higher value of $Trust\ (M, M_i)^t$ represents that $M_i$ is more trustworthy as compared to the nodes with lower values. The direct trust is expressed as

$$DT(M, M_i)^{\mathrm{t}} = P_w(i) . DT(M, M_i)^{\mathrm{t}-1} - N_w(i) . DT(M, M_i)^{\mathrm{t}-1}, \quad (3.2)$$

where, $P_w(i)$ represents the information of the positive and well-behaved activity of the node $i$ and $N_w(i)$ represents the information of the malicious and misbehaved activity, where $P_w(a) \neq N_w(a) = \Delta E / E_{max}$. $E_{max}$ is the maximum energy that a node can attain and $\Delta E$ is the residual energy of the node after communication. If a node participates in the network activity, the value of weight factor of the node decreases, otherwise increases, which helps to detect selfish nodes. Therefore, if $\Delta E / E_{max} < E_{th}$, it is considered as $P_w(a)$ otherwise $N_w(a)$, where $E_{th}$ is the threshold energy ratio $\in [0, 1]$. We formulate the indirect trust of the node $i$ accumulating the values of the neighbours nodes $(nbr_i)$ and is given as

$$IT(M_j, M_i)^{\mathrm{t}} = P_w(a) \sum_{j \in nbr_i, j \neq i} DT\left(M_j, M_i\right)^{\mathrm{t}-1} - N_w(a) \sum_{j \in nbr_i, j \neq i} DT(M_j, M_i)^{\mathrm{t}-1} \quad (3.3)$$

#### *3.2.2.2 Inter-Cluster Trust Evaluation*

The inter-cluster communication helps to achieve distributed trust evaluation with the help of the cluster heads and the base station. The trust value of nodes in different clusters depends on the trust relationship between two clusters $(M, N)$ (see Fig. 3.1). The inter-cluster trust between the node $M_i$ of the cluster $M$ and the node $N_j$ of the cluster $N$ at round $t$ can be evaluated using the mapping function.

$$T(M_i, N_j)^{\mathrm{t}} = T(M, N)^{\mathrm{t}} \times T(N, N_j)^{\mathrm{t}} \tag{3.4}$$

where, $T(M, N)^{\mathrm{t}}$ and $T(N, N_j)^{\mathrm{t}}$ represent the inter-cluster trust of the cluster $N$ to the cluster $M$ at round t and trust of node $N_j$ in its own cluster $N$ respectively. $T(M, N)^{\mathrm{t}}$ is calculated with the help of direct and indirect trust. Indirect trust is calculated with the help of neighboring cluster $P$. If the target cluster $N$ has no past interaction (P.I) with $M$ in the network then the trust value of $N$ is received from the base station. The inter-cluster trust from the cluster heads $N$ to $M$ is calculated as

$$T(M, N)^{\mathrm{t}} = \begin{cases} BT_N^t \quad , \quad \text{if P.I} = \varphi \\ \alpha_2 . T(M, N)^{\mathrm{t}-1} + \beta_2 . \frac{\sum_{p \exists CN_N, P \notin M, \ P \notin N} IT(P,N)^{\mathrm{t}}}{|C_i| - 2} + BT_N^t \ , \\ otherwise \end{cases} \tag{3.5}$$

where $\alpha_2 + \beta_2 = 1$, $\alpha_2 > 0$, $\beta_2 > 0$. $\alpha_2$ and $\beta_2$ are the weight factors which are associated with the access control policies.

**Algorithm 3.1: EETE**

**Input:** n, ND, k
**Process**:
1: *Initially, Store the value of ND degree in descending order using BFS in* $UnCO_{set}$.
2: ***for*** $n_i$ *nodes in* $UnCO_{set}$
3: ***if*** $ND_i > k$ *using Eq.* 3.22 ***then***
4: $n_i \, \varepsilon$ *cluster head*
5: ***else***

6: $n_i \; \varepsilon \; cluster \; member$
7: **end if**
8: **for** $n_i \; \varepsilon \; cluster \; head \; send \; REQ_M \; to \; cluster \; member \; in \; 3 \; hops$
9: **if** $n_i^{CM} \; receive \; REQ_M \; > 2$ **then**
10: **if** $cluster \; member_M \; < \; k$ **then**
11: $add \; n_i \; into \; member_M$
12: **else**
13: $add \; n_i \; into \; member_M \; with \; least \; number \; of cluster \; member_M.$
14: **end if**
15: **end if**
16: **if** $member_M < k$ **then**
17: $\forall \; member_M \; join \; the \; other \; nearby \; cluster \; head$
18: **end if**
19: $\forall \; cluster \; member, cluster \; head \; checks \; for \; malicious \; activity \; using \; Eq. (3.35)$
20: **if** $Trust_{sys} \; > \; Trust_{th}$ **then**
21: $\forall \; M \; checks \; if \; E_j > \; E_{th}$ **then**
22: **if** $trust_j > \; trust_{th}$ **then**
23: $j \; will \; decide \; to \; be \; CH \; or \; CM \; using \; Eq. (3.14) \; and \; Eq. (3.18)$
24: **else**
25: $add \; node \; j \; into \; s_i$
26: **end if**
27: **end if**
28: **if** $(s) \neq \emptyset$ **then**
29: $\forall \; s_i$ **if** $aging \; time \; t(s_i) = \Delta t$ **then**
30: $f = f + 1$
31: **if** $f > \; f_{th}$ **then**
32: $remove \; the \; s_i \; from \; the \; network$
33: **else**
34: $add \; cluster \; member$
35: **end if**
36: **end if**
37: **end if**

## 3.3 ENERGY EFFICIENT TRUST EVALUATION SCHEME

In this section, we propose an Energy Efficient Trust Evaluation Scheme for IoT based network in detail. It consists of Dilemma games to maintain satisfactory trust level and to mitigate the malicious activates in the network. The stepwise working of the algorithm 3.1: cluster based trust evaluation in as follows:

Step 1. Initially, store the values of node degree (ND) in uncovered set ($UnCO_{set}$) in descending order using breadth first search algorithm (BFS). The nodes with value greater than $k$ will be selected as cluster head otherwise as cluster member. Cluster head sends the request to cluster member within the 3 hops limit. Cluster member after receiving the request chooses the cluster head with the least number of members. If any cluster head fails to maintain the minimum number of cluster members (calculated using (22)) then the cluster head joins the nearest cluster.

Step 2. Based on the activity, payoff is given to each node in the network using activity based dilemma game, described in the following section 3.3.1.3 using (3.35). Trust of the system $Trust_{sys}$ should always be greater than threshold trust ($Trust_{th}$). If there is any node that has energy more than threshold ($E_{th}$) and trust value lower than $Trust_{th}$ , it is added to the suspended list ($s$).

Step 3. After completing one round, based on the residual energy and individual interest, each node decides whether it wants to become cluster head or cluster member and accordingly payoffs are given using eq. (3.14) and eq. (3.15).

Step 4. If any node $s_i$ is in the list ($s$) for less than $\Delta t$ time $f_{th}$, the node is added into the network to perform better in future. If it continuously behaves maliciously, it removes permanently from the network to maintain the trust of the network.

After completing each round, energy and trust are calculated. Further, we present three dilemma game models for cluster formation with the help of remaining energy and calculated trust.

### 3.3.1 *Dilemma Games for Trust Evaluation*

In this section, first, we present three dilemma game models for cluster formation, optimum cluster members in a cluster to maintain satisfactory trust and capture the malicious activity of the nodes, which use in the EETE algorithm. We also present three lemmas to find the solutions for the proposed games as evolutionary stable strategy and mixed Nash equilibrium.

#### *3.3.1.1 Cluster Formation Dilemma Game*

In a network area with $n$ nodes, the cluster formation game can be represented by a three-tuple $G\ (E, S, U)$, where $E, S$, and $U$ represent the node set, strategy set, and utility set respectively. $E$ is divided into two subset of the nodes based on the remaining energy i.e., $E_h$ and $E_L$ where $E_h$ is the set of nodes having energy more than or equal to the $E_{thres}$ and $E_L$ consists of the nodes with energy lower than $E_{thres}$ . So $E = E_h \cup E_L$ and $E_h \cap E_L = \emptyset$. A player has two strategies to choose either cluster head or cluster member, and are denoted as $CH$ and $CM$. So, strategy set $S = \{CH, CM\}$. $U$ of a player consists of two parts: the reward/penalty and the communication cost. The utility function $U_i$ of every player is define as

$$U_i = r_i - p_i, \tag{3.6}$$

where, $r_i$ and $p_i$ are the reward and penalty respectively of the player $i$ based on the action performed by the player. The nodes with more energy are encouraged to become the cluster head and others are encouraged to become cluster member. Cluster formation dilemma game's payoff matrix is shown in the Table 3.2. The players earn payoff in the following ways:

**Table 3.2**. Trust payoff of Cluster formation dilemma game

| $E_h$ \ $E_L$ | To be CH $(s_1{}')$ | To be CM $(s_2{}')$ |
|---|---|---|
| To be CH $(s_1)$ | $(U_{1,1},\ U_{1,1}{}')$ | $(U_{1,2},\ U_{1,2}{}')$ |
| To be CM $(s_2)$ | $(U_{2,1},\ U_{2,1}{}')$ | $(U_{2,2},\ U_{2,2}{}')$ |

1) The trust payoffs of $E_h$ and $E_L$ players decrease when both players become $CH$ with no $CM$ that forms a illicit cluster. This action is undesirable in the network. Therefore, double penalty is imposed on both of the players and payoffs of both players can be expressed as

$$\begin{cases} U_{1,1} = \theta T_h - 2\varphi C_h \\ U_{1,1}{}' = \theta T_L - 2\varphi C_L \end{cases} \tag{3.7}$$

where, $T_h$ and $T_L \in [0,1]$ are the trust values of high and low energy nodes respectively and are obtained using Eq. (1). $C_h$ $and$ $C_L \in [0,1]$ are the communication costs for $E_h$ $and$ $E_L$ respectively. $\theta, \varphi \in [0,1]$ are the weight factors.

2) When $E_h$ player chooses to become $CH$ and $E_L$ chooses to become $CM$ then the trust payoffs of both the players increases and only mandatory penalty is imposed. As it is the best strategy to choose for both players and there payoffs are

$$\begin{cases} U_{1,2} = 2\theta T_h - \varphi C_h \\ U_{1,2}{}' = 2\theta T_L - \varphi C_L \end{cases} \tag{3.8}$$

3) When $E_h$ players choose to become $CM$ and $E_L$ players choose to become $CH$. It unbalance trust of a cluster because of selection of $E_h$ player's strategy. So, $E_h$ trust payoffs decreases but the $E_L$ player helps in formation of cluster. Therefore, $E_L$ payoff increases and the payoffs can be given by

$$\begin{cases} U_{2,1} = T_h - \varphi C_h \\ U_{2,1}{}' = \theta T_L - \varphi C_L \end{cases} \tag{3.9}$$

4) When $E_h$ and $E_L$ both choose to become $CM$ there will be no $CH$. It will lead to illicit cluster, which only decreases the trust payoffs of both players and the payoffs can be given by

$$\begin{cases} U_{2,2} = \theta T_h - 2\varphi C_h \\ U_{2,2}{}' = -\varphi C_L \end{cases} \tag{3.10}$$

Although the players are unaware of the other's strategies, the rate of a certain behavior tends to be stable when the evolutionary game theory is adopted. The change of rate is named replicator dynamics and the state is known to be the evolutionary stable strategies (ESS). When the players meet the ESS condition, they get into the steady state.

Lemma 1. The ESS of the cluster formation dilemma game is existent and it is $CH$ for class $E_h$ and $CM$ for class $E_L$

Proof 1. Let's assume that rate of selecting the $s_1$ strategy is $x$, hence that of selecting $s_2$ is $(1-x)$. Similarly, the rate of selecting $s_1'$ and $s_2'$ strategy is $y$ and $(1-y)$ respectively. Therefore, the $E_h's$ expected utility strategy $U_{E_h-C}$ and $U_{E_h-CM}$ are expressed as

$$U_{E_h-CH} = y(\theta T_h - 2\varphi C_h) + (1-\mathrm{y})(2\theta T_h - \varphi C_h)$$

$$= 2\theta T_h - y\theta T_h - y\varphi_h - \varphi C_h, \quad (3.11)$$

$$U_{E_h-CM} = y(T_h - \varphi C_h) + (1-y)(\theta T_h - 2\varphi C_h)$$

$$= yT_h - y\varphi C_h + \theta T_h - 2\varphi C_h - y\theta T_h, \quad (3.12)$$

The average revenue of $U_{E_h}$ can be denoted as

$$\overline{U_{E_h}} = x(2\theta T_h - y\theta T_h - y\varphi C_h - \varphi C_h) + (1-x)(yT_h - y\varphi C_h + \theta T_h - 2\varphi C_h - y\theta T_h)$$

$$= x\theta T_h - 2xy\varphi C_h + x\varphi C_h - yT_h + y\varphi C_h + \theta T_h - 2\varphi C_h - y\theta T_h - xy_h, \quad (3.13)$$

Now, we analyse the replication dynamics of the ESS, the replicator dynamics equation is

$$\frac{dx}{dt} = x(U_{E_h-CH} - \overline{U_{E_h}}) = x(2\theta T_h - y\theta_h - y\varphi_h - \varphi C_h - x\theta T_h + 2xy\varphi C_h - x\varphi_h + yT_h - y\varphi C_h - \theta T_h + 2\varphi C_h + y\theta T_h + xyT_h)$$

$$= x(1-x)(\theta T_h + \varphi C_h - y(T_h - \varphi C_h)) \quad (3.14)$$

Similarly, we obtain the expression for $E_L$

$$U_{E_L-CH} = x(\theta T_L - 2\varphi C_L) + (1-x)(\theta T_L - \varphi C_L) = \theta T_L - x\varphi C_L - \varphi C_L \quad (3.15)$$

$$U_{E_L-CM} = x(2\theta T_L - \varphi C_L) + (1-x)(-\varphi C_L) = 2x\theta T_L - \varphi C_L \quad (3.16)$$

$$\overline{U_{E_L}} = y(\theta T_L - x\varphi C_L - \varphi C_L) + (1-y)(2x\theta T_L - \varphi C_L)$$

$$= y\theta T_L - 2xy\theta T_L - xy\varphi C_L + xy\varphi C_L + 2x\theta_L - \varphi C_L \quad (3.17)$$

$$\frac{dy}{dt} = y(\theta T_L - x\varphi C_L - \varphi C_L - y\theta_L + 2xy\theta T_L + xy\varphi C_L - xy\varphi C_L - 2x\theta_L + \varphi C_L$$

$$= y(1-y)(\theta T_L - x(\varphi C_L + \theta T_L)) \quad (3.18)$$

From the Eq. (3.14) it can be obtained that when $x^*$ = 1, the player $E_h$ achives the stable state, and remains unaffected from the strategy of $E_L$ when $y < (\theta T_h + \varphi C_h)/(T_h - \varphi C_h)$. For $y^*$=0 is the stable state for $E_L$ when $x > \theta T_L/(\varphi C_L + \theta T_L)$. The ESS condition can be achieved if both $E_h$ and $E_L$ satisfy the above two inequalities at the same time. The above inequalities of $x$ and $y$ help in cluster formation phase. It means that all the $E_h$ nodes tend to become $CH$ and $E_L$ tends to become $CM$ with probability 1. These two inequalities can be used to determine the energy efficiency and trust level of the cluster formation game.

### *3.3.1.2 Optimal Cluster Formation Dilemma Game*

A cluster must contain optimal number of nodes to maintain the trust of the cluster in the network. Here, we introduce a game theoretic approach to deal with the potential selfishness in the process. The optimal cluster formation dilemma game depends on the number of replies obtained from the members. Cluster head and Cluster member have two types of strategies *Reply* or *No Reply*. *Reply* means on receiving a trust request, receiver sends the trust reply to the evaluating node. *No Reply* means receiver disregards the trust request.

We define a utility $U_k$ under the condition that the evaluating node have atleast $k$ replies. In optimal cluster formation dilemma game, there are two cases: 1) when the request replies are less than $k$ and 2) when the request replies are greater than $k$. The payoffs matrix of the game is given in Table 3.3. If cluster head (CH) does not receive $k$ replies, other nodes prefer to keep silence in order to save their energy. In this game, all the nodes are independent of each other and choose their own strategy.

**Table 3.3.** Payoff Matrix for optimal cluster formation dilemma game (k >1)

| $CH$ | $number\ of\ CM$ | |
|---|---|---|
| | $\gamma\ nodes\ reply$ $(0 < \gamma < k-1)$ | $\delta\ nodes\ reply$ $(\delta \geq k)$ |
| $No\ Reply$ | $0, -\gamma C$ | $T\ , \delta T - \delta C$ |
| $Reply$ | $T - C, T - \gamma C$ | $T - C, \alpha\delta T - \delta C$ |

Utility for the CH corresponds to No Reply = $\{0, T\}$, where 0 represents the number of replies is less than $k$ and no loss of energy. Trust gain $T$ remains same as in the previous round. When CH replies, it charges only communication cost $C \in [0,1]$ to send the trust request/reply. We make a reasonable assumption that the gain is more than the communication cost. The payoffs for the cluster members (CM) strategies based on the number of nodes replying to the CH are defined as

1) When $\gamma$ nodes replies, the trust payoff decrease in both the cases as CM replies < $k$ and $\gamma \in [0,1]$ represents the weight factor. The utility for $\gamma$ nodes is

$$U_1' = T - 2\gamma C \tag{3.19}$$

2) When $\delta$ nodes reply, the trust payoff increases as CM replies $> k$ and $\alpha \in [0,1]$ is the reward given to the CMs for balancing the trust of the network. Utility for the CMs when replies $\geq k$ is

$$U_2' = \delta T(1+\alpha) - 2\delta C \tag{3.20}$$

**Lemma 2**. For non-cooperative trust game, a mixed strategy Nash Equilibrium exists if the probability of atleast $k$ number of nodes in a cluster to maintain the trust is $p$.

**Proof 2.** We suppose that the probability for an arbitrary node reply is $p$, or remaining silent is $(1-p)$. Then atleast $k$ nodes reply the trust request with a probability of $1 - (1-p)^k$. Therefore, as a result, the expected payoff using mixed strategy, Nash equilibrium can be computed as

$U_k$ = Trust × Probability of atleast $k$ nodes reply

$$= T\,(1 - q^k) = T(1 - (1-p)^{k-1}) \tag{3.21}$$

At the Nash equilibrium, $U_k$ equals to the $k-1$ nodes payoff, therefore, they maintain the minimum trust level in the individual node. Thus,

$$\text{T}\,(1 - (1-p)^{k-1}) = kT(1+\alpha) - 2kC\,,$$

By solving the above expression, we can compute the probability $p$ of a player choose to become the part of a cluster

$$p = 1 - w^{\frac{1}{k-1}} \tag{3.22}$$

where, w = $1 - k(1-\alpha) + 2\,kC/T$. The probability $p$ can never be zero to maintain the equilibrium. Therefore, $k > 1$ or $1 - \alpha(1 - k) + 2\,kC/T > 1$. By calculating the expression we can say that if we have $\alpha < 2\,C/T - 1$, we can maintain the $k$, and $\alpha$ depends on the $C$ and $T$.

#### *3.3.1.3 Activity Based Trust Dilemma Game*

In this section, we present a dynamic game model to compute the Nash equilibrium that represents the best strategy of CH to launch its anomaly detection technique. In a dynamic game, players have the chance to change their strategies according to the observations of the past choices.

The CH based on its interaction with the players can distinguish them into three categories: *Trust*, S*uspicious*, or *Malicious*. Trust node is the node that is trustworthy and works according to the requirement of the network throughout the lifetime. Suspicious nodes are those nodes which change their patterns and not able to transmit the packet due to link failure or unreliable communication channel. Malicious nodes are those nodes that perform lethal attacks continuously that hinder the operation of the network. Denial of services are one of the kinds of attack.

The CH is the watchdog of the cluster and members are the attackers who are either *Normal* or *Illegitimate*. Table 3.4 illustrates the payoff matrix of the trust. Since the aim of this trust model is to find an optimal steady state solution in which a consensus between CH and CM is needed to stabilize the network. We call the consensus as a Saddle-point equilibrium of the game. According to the strategies of the players, the payoff is defined as:

**Table 3.4.** Different payoff at different outcomes

| | **Player's Behaviour** | | |
|---|---|---|---|
| **Strategy** | **Trust** | **Suspicious** | **Malicious** |
| Normal | $G_{i,j}(N,T)$, $G'_{i,j}(N,T)$ | $G_{i,j}(N,S)$, $G'_{i,j}(N,S)$ | $G_{i,j}(N,M)$, $G'_{i,j}(N,M)$ |

| | | | |
|---|---|---|---|
| Illegitimate | $G_{i,j}(I,T)$, $G'_{i,j}(I,T)$ | $G_{i,j}(I,S)$, $G'_{i,j}(I,S)$ | $G_{i,j}(I,M)$, $G'_{i,j}(I,M)$ |

1) If any player behave *Normal* and the CH observes it as a trustworthy player, it increases the trust of both the players. $G_{i,j}(N,T)$, and $G'_{i,j}(N,T)$ are the gain of the player $i$ and the CH $j$ . If player $i$ behaves normally, and node $j$ observes it as trustworthy. The payoff of the both the parties can be expressed as

$$\begin{cases} G_{i,j}(N,T) = \alpha_i T_{H_i}^t \\ G'_{i,j}(N,T) = \alpha_i T_{H_i}^t - C_i^t \end{cases} \quad (3.23)$$

Where, $\alpha_i \in [0,1]$ is the weight factor for the node $i$. $T_{H_i}^t \in [0,1]$ represents the trust gain for high trust value for $i^{th}$ player at time $t$. $C_i^t \in [0,1]$ is the communication cost to assign the value of *Trust*, *Suspicious* or *Malicious* to a CM by the CH.

2) If any player behave normally and the CH observes it as *Suspicious*, the payoff of both the players are given as

$$\begin{cases} G_{i,j}(N,S) = \beta_i T_{S_i}^t \\ G'_{i,j}(N,S) = \beta_i T_{S_i}^t - C_i^t \end{cases} \quad (3.24)$$

Where, $\beta_i \in [0,1]$ is the weight factor for the node $i$ . $T_{S_i}^t \in [0,1]$ represents the *Suspicious* gain for $i^{th}$ player at time $t$.

3) If a player behaves normally but the CH observes it as *Malicious* player, the payoff of both the players are given as

$$\begin{cases} G_{i,j}(N,M) = \alpha_i T_{M_i}^t \\ G'_{i,j}(N,M) = -(\gamma_i T_{M_i}^t + C_i^t) \end{cases} \quad (3.25)$$

Where, $\gamma_i \in [0,1]$ is the weight factor, and $\alpha_i + \beta_i + \gamma_i$=1. $T_{M_i}^t \in [0,1]$ is the *Malicious* gain for $i^{th}$ player at time $t$.

4) When a player behaves *Illegitimately* and the CH observe it as *Trustworthy*. The trust payoff of the CH decreases and players payoff increases and given by

$$\begin{cases} G_{i,j}(I,N) = \gamma_i T_{M_i}^t \\ G'_{i,j}(I,N) = -(\gamma_i T_{M_i}^t + C_i^t) \end{cases} \quad (3.26)$$

5) If a player behaves *Illegitimately* and the CH observe it as *Suspicious*, the trust payoffs of both players decrease and are respectively shown in Eq. (27).

$$\begin{cases} G_{i,j}(I,N) = -\beta_i T_{M_i}^t \\ G'_{i,j}(I,N) = -(\beta_i T_{S_i}^t + C_i^t) \end{cases} \quad (3.27)$$

6) When the CH observes that a node behaves *Maliciously* while the node performing *Illegitimately*, it increases the trust payoff of the CH and decreases the payoff of the player for performing false activity and are respectively given by

$$\begin{cases} G_{i,j}(I,N) = -\beta_i T_{M_i}^t \\ G'_{i,j}(I,N) = -(\beta_i T_{S_i}^t + C_i^t) \end{cases} \quad (3.28)$$

Finally, game theoretic analysis of the trust-based interaction between the attacker and the CH derives the optimal policy based on min-max theorem to guarantee the optimal utility of the network. According to the min-max theory, we calculate the maximum loss of the network, which can be caused by the attackers and then select the minimum depletion of the network in the maximum loss. For the CH, maximum loss in *Normal* strategy is $G'_{i,j}(N,M)$ and for the *Illegitimate* behaviour $G'_{i,j}(I,T)$ is the maximum. From the above observation, we can say that in an insecure environment, the gain of the attacker is equal to the loss of the network. Therefore, for an attacker priority utility based on the payoff of the network is $G_{i,j}(N,T) > G_{i,j}(I,T) > G_{i,j}(N,M) > G_{i,j}(N,S) > G_{i,j}(I,S) > G_{i,j}(I,M)$ whereas for the CH payoff priority are $G'_{i,j}(N,T) \cong G'_{i,j}(I,M) > G'_{i,j}(N,S) > G'_{i,j}(I,S) > G'_{i,j}(N,M) > G'_{i,j}(I,T)$.

It is desired that the CH and CM negotiate their independent strategies to reach the steady state solution that is a Saddle point. Let $p_i$ be the probability for the CM to choose a strategy from *Normal* or *Illegitimate* and $q_i$ be the probability to adopt the strategy for *Trust*, *Suspicious* or *Malicious*, where $\sum_{i=1}^{2} p_i = 1$ and $\sum_{j=1}^{3} q_j = 1$. The utility functions of the

players $CM_i$ and $CH_j$ are denoted by $U_{CM_i}$ and $U_{CH_j}$ respectively that depend on the adopted strategies and are given by

$$U_{CM_1}(\textit{Strategy}= \textit{Normal}) = \alpha_i T_{Hi}^t . q_1 + \alpha_i T_{M_i}^t . q_2 + \beta_i T_{S_i}^t . q_3$$
$$= G_{1,1} . q_1 + G_{1,2} . q_2 + G_{1,3} . q_3, \quad (3.29)$$

$$U_{CM_2}(\text{Strategy}= \textit{Illegitimate}) = \gamma_i T_{M_i}^t . q_1 + \left(-\beta_i T_{M_i}^t\right) . q_2 + \left(-\gamma_i T_{M_i}^t\right) . q_3$$
$$= G_{2,1} . q_1 + G_{2,2} . q_2 + G_{2,3} . q_3, \quad (3.30)$$

$$U_{CH_1}(Strategy = \textit{Trust}) = \left(\alpha_i T_{H_i}^t - C_i^t\right) . p_1 - \left(\gamma_i T_{M_i}^t C_i^t\right) . p_2$$
$$= G'_{1,1} . p_1 + G'_{1,2} . p_2 , \quad (3.31)$$

$$U_{CH_2}(Strategy = \textit{Suspicious}) = \left(\beta_i T_{S_i}^t - C_i^t\right) . p_1 - \left(\beta_i T_{S_i}^t + C_i^t\right) . p_2 = G'_{2,1} . p_1 + G'_{2,2} . p_2 , \quad (3.32)$$

$$U_{CH_3}(Strategy = \textit{Malicious}) = -\left(\gamma_i T_{M_i}^t + C_i^t\right) . p_1 + \left(\alpha_i T_{M_i}^t - C_i^t\right) p_2$$
$$= G'_{3,1} . p_1 + G'_{3,2} . p_2 \quad (3.33)$$

***Lemma 3***. $CM_i$ is a *Illegitimate* node when $p_2 > p^*$and $CH_j$ target it as a *Malicious* node when $q_3 > q^*$; where $(p^*, q^*)$ is defined as first saddle-trust equilibrium point to maintain

***Proof 3***. The CM and CH both adopt strategies $U_{CM_2}$(Strategy= *Illegitimate*) $>$ $U_{CM_1}$(Strategy= *Normal*) and $U_{CH_3}(Strategy = \textit{Malicious}) > U_{CH_1}(Strategy = \textit{Trust}) = U_{CH_2}(Strategy = \textit{Suspicious})$, i.e.,

$$\begin{cases} \gamma_i T_{M_i}^t . q_1 + \left(-\beta_i T_{M_i}^t\right) . q_2 + \left(-\gamma_i T_{M_i}^t\right) . q_3 \\ \quad > \alpha_i T_{Hi}^t . q_1 + \alpha_i T_{M_i}^t . q_2 + \beta_i T_{S_i}^t . q_3, \\ -\left(\gamma_i T_{M_i}^t + C_i^t\right) . p_1 + \left(\alpha_i T_{M_i}^t - C_i^t\right) p_2 \\ > \left(\alpha_i T_{H_i}^t - C_i^t\right) . p_1 - \left(\gamma_i T_{M_i}^t + C_i^t\right) . p_2 \\ \quad + \left(\beta_i T_{S_i}^t - C_i^t\right) . p_1 - \left(\beta_i T_{S_i}^t + C_i^t\right) . p_2 . \end{cases} \quad (3.34)$$

It is observed that $q_1 + q_2 + q_3 = 1$. We suppose *Trust* and *Suspicious* nodes are equally detectable Therefore, $q_1 = q_2 = \frac{1-q_3}{2}$ and $p_1 = 1 - p_2$. Hence, we obtain the following equalities

$$\begin{cases} q_3 > q^* = \frac{G_{1,1}+G_{1,2}-G_{2,1}+G_{2,2}}{Z_1} \\ p_2 > p^* = \frac{2G'_{1,1}-G'_{3,1}}{Z'_1} \end{cases} \quad (3.35)$$

Where, $Z_1 = G_{1,1} + G_{1,2} - G_{2,1} + G_{2,2} + 2G_{1,3} + 2G_{2,3}$ and $Z'_1 = 2G'_{1,1} - 2G'_{1,2} + G'_{3,1} + G'_{3,2}$. Therefore, the IoT device is rank as a *Malicious* node when the saddle-trust equilibrium point is reached which is equal to $(p^*, q^*) = (\frac{2G'_{1,1}-G'_{3,1}}{Z'_1}, \frac{G_{1,1}+G_{1,2}-G_{2,1}+G_{2,2}}{Z_1})$ ; $q^*$ is a trust threshold of an illegitimate node.

## 3.4 SIMULATION RESULTS AND PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed Energy Efficient Trust Evaluation (EETE) scheme in sensor-enabled IoT environment. We use the NS-3 simulator to compute the trust of the nodes in the network in the presence of malicious activity and computed detection rate, energy efficiency, and time spent on trust calculations. We compare the EETE scheme with state of the art TDDG [52], HIDS [114], CWSN [115] and LHIDS [116] to show the effectiveness of each other in various environment. The simulation runs until maximum iteration (50) reached or converged.

### 3.4.1 Simulation Environment

In this section, we define the metrics considered in the simulation such as network area $500 \times 500m^2$, where 300 nodes are randomly deployed. The Log Distance and Constant Speed Propagation Loss model has been employed in the simulation to calculate the propagation delay between the sender and receiver for transmission of trust request and trust replies. We use the Simple Device Energy Model of ns3 which uses the basic radio energy model for the initial distribution of energy and also keeps on track of the usage of the energy in the network. The length of data packet is 1024 bits. Table 3.5 shows the list of parameters used to configure the simulation scenario.

### 3.4.2 Simulation Metrics

a) *Detection rate ($D_r$)*: It is defined as the ratio to the numbers of correctly attackers are identified ($A_i$) out of total number of attackers ($A_t$).

$$D_r = \frac{A_i}{A_t} \times 100$$

b) *Average energy consumption ($EC_{avg}$)*: It is defined as the ratio of the total energy consumed by the active nodes to the total number of participating node in the network.

$$EC_{avg} = \frac{\sum_{i=2}^{k} E_i}{k}$$

where, $E_i$ is the energy of the $i^{th}$ member node of the cluster, $k$ ($k = 10$ ) is the maximum number of nodes in a clusters.

c) *Trust evaluation time*: It is a time span from receiving the request to calculate the direct and indirect trust of the nodes and sending the acknowledgement to the source node.

d) *Detection time*: It is first response time to the detection of malicious node in the network.

e) *Saddle point*: It is defined as an optimized steady state solution in which a consensus between cluster head and cluster member to stabilise the stability in the network in the presence of illegitimate nodes.

**Table 3.5.** Simulation parameters

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| Network area | $500 \times 500m^2$ | Communication range | $100\ m$ |
| Number of nodes | 300 | $\alpha_1, \alpha_2$ | 0.5 |
| Cycle time | $0.3\ sec$ | $P_w(a)$ | 0.01 |
| Node sensing range | $25\ m$ | $N_w(a)$ | $-0.15$ |
| Initial energy | $10\ J$ | $E_{th}$ | $3\ J$ |
| Packet size | 1024 bits | Number of attackers | 10 - 40% |
| Initial energy | $10\ J$ | Hop limit | 3 |
| Maximum iteration | 50 | Initial trust value | 0.5 |

### 3.4.3 Result Analysis

This section presents the comparative analysis of state of the art algorithms with respect to simulation metrics.

#### 3.4.3.1 Malicious node and Detection rate

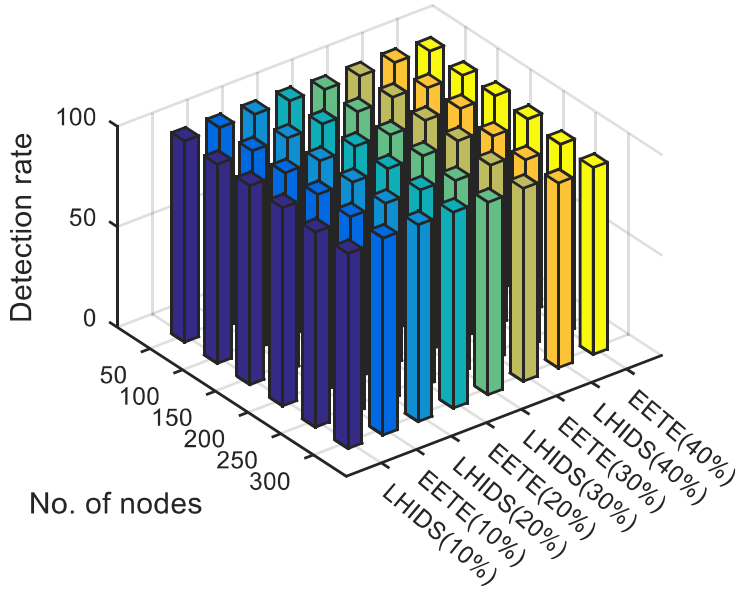



**Figure. 3.2.** Number of nodes vs detection rate (10-40%)

Fig.3.2 shows the variation of detection rate of malicious node (MN -10% to 40%) towards increasing number of nodes. When the number of MN is 10 %, the detection rate for LHIDS varies between 100% (nodes=50) to 98 % (nodes=300) and when the MN is 20%, the detection rate falls to 96% as shown in Fig.3.2. Whereas, the detection rate of the EETE never falls below 97% when the MN is 20%. The detection rate of LHIDS, starting from 99% to 96% when the MN is 30%, after that as number of MN increases to 40%, there is drastic change in detection rate and it falls below 93%. This behavior shows that poor performance towards increasing number of malicious nodes. Whereas, for the proposed EETE, the detection rates are 94 % and 97% when MN are 30% and 40% respectively. This is due to the optimal settings of $(p^*, q^*)$ using the activity based trust dilemma game and uses Nash equilibrium startegy, which classifies the nodes in three categories: *Trust, Suspicious*, and

*Malicious* according to their behavior in the network. The EETE removes malicious nodes from the network performing illegitimately for longer duration of time, which helps in reducing the malicious activity in the network. The results clearly explain that the EETE outperforms in the presence of malicious nodes.

### 3.4.3.2 Average Energy Consumption ($EC_{avg}$) and Trust Evaluation Time

In Fig. 3.3, the average energy consumption is comparatively analyzed with the EETE considering number of one hop and state of the art models: flooding, flooding with 2 hops and TDDG. It is observed that for 20 number of participating nodes, the maximum energy consumption for flooding without hop and with 2 hops, are 10.6 J and 6.5 J respectively. It clearly shows that flooding with 2 hops consumes less energy than flooding without hops. It is noticed that EETE consumes energy 0.40 J, when only 2 nodes have participated. For 20 number of participating nodes, energy consumption is about 1.84 J. the EETE gives the best result comparative to state of the art models. The reason for the better performance is that in EETE, all the cluster heads manage the trust computation overhead and the cluster member only receives and transmits the packets. Therefore, the overhead of the trust calculation is reduced and it helps in better energy consumption.

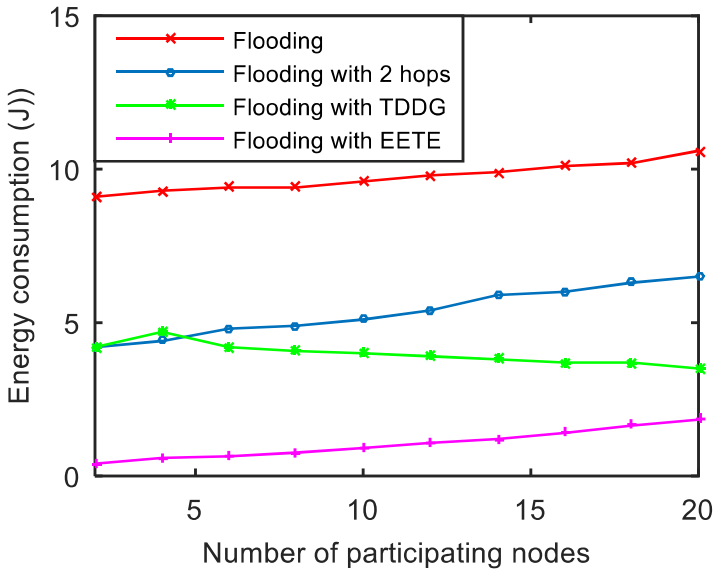



**Figure.3.3.** Number of participating node vs Energy consumption (J) with hop limit 1

Fig. 3.4 shows the corresponding time spent on evaluation of trust, as the number of nodes increases. Initially, for 2 participating nodes, the time spent on trust evaluation is 130 ms for flooding and increases up to 242 ms for 20 nodes. In case of flooding with 2 hops, the spent time on trust evaluation is 30 ms and 130 ms for 2 and 20 number of nodes respectively. Flooding with TDDG and with EETE follows the steady state curve. TDDG consumes 14 ms and 17 ms for the trust evaluation of 2 nodes and 20 nodes respectvely. Whereas duration of evaluating trust for 2 to 20 nodes are 4 ms and 10 ms respectively. That means EETE is unaffected as the number of participating nodes increases. This is because of the reduction in comunication overhead due to the consideration of optimal number of recommendations (k) for the trust evaluation of the nodes.

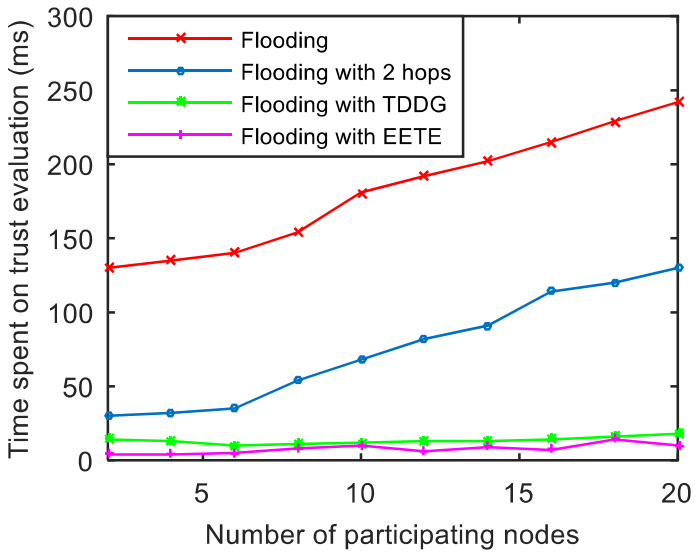



**Figure. 3.4.** Number of participating node vs Time spent on trust evaluation with hop limit 1

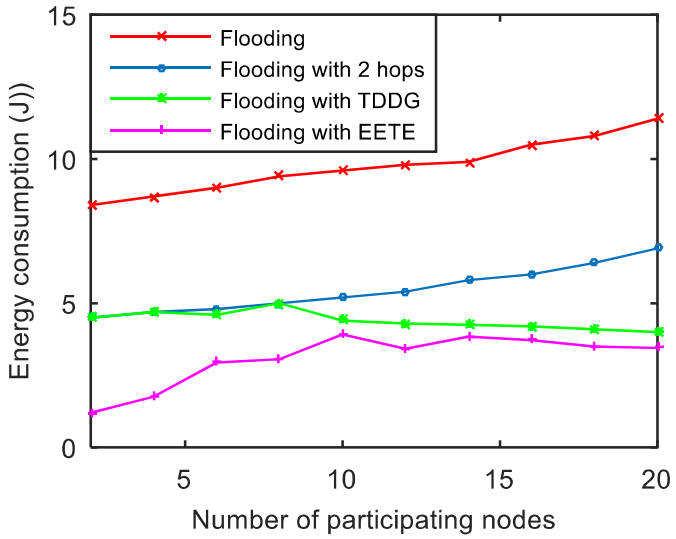



**Figure. 3.5.** Number of participating node vs energy consumption (J) with hop limit 3

Fig. 3.5 illustrate the comparative analysis of average energy consumption with EETE with 3 hops and the existing models: flooding, flooding with 2 hops, and TDDG. Flooding without hops consumes 11.4 J when number of nodes is 20, which is the highest energy consumption among the state of the art models. Initially for 2 to 6 nodes, flooding with 2 hops shows almost the similar result with TDDG but when the number of nodes increases from 6 to 20, energy consumption reaches to 6.9 J for flooding with 2 hops and TDDG follow the steady state curve. In case of EETE, energy consumption is 1.2 J and 3.5 J for 2 and 20 nodes respectively. EETE follows the steady state curve. It is clear that EETE is more energy effieient as compare with the state of the art models.

Fig.3.6 shows that maximum trust evaluation time of flooding is 259ms for 20 number of participating nodes. Whereas, EETE takes trust evaluation time 8 ms for 2 nodes and 23 ms for 20 nodes. Such performance is achieved because of the dilemma game has been employed for cluster formation. These dilemma games calculates the optimal size of the cluster and uses the past trust values which helps in reduction of extraneous trust calculation. Further, it reduces energy consumption and time spent on trust evaluation at every node of the network.

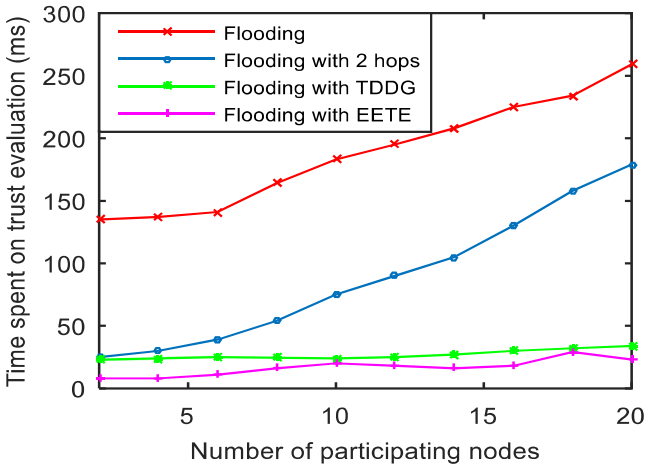



**Figure. 3.6.** Number of participating nodes vs Time spent on trust evaluation (ms) with hop limit 3.

### 3.4.3.3 Detection time and Probability

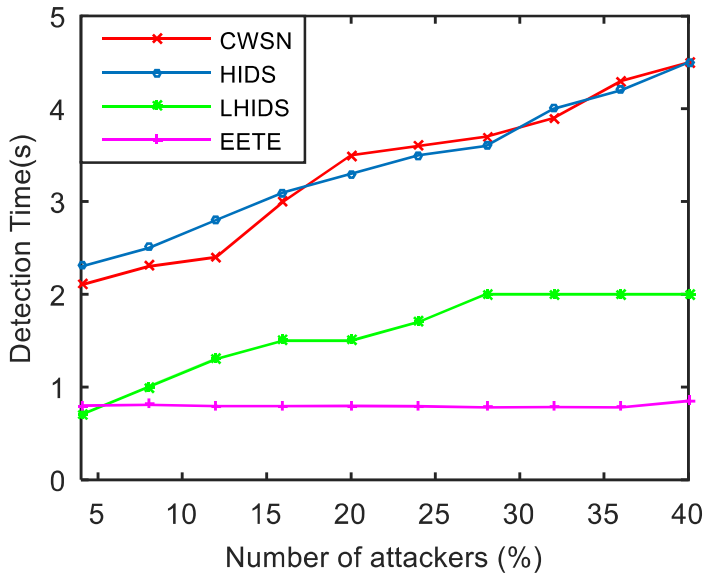



**Figure. 3.7.** Number of attackers (%) vs detection time

Fig 3.7 illustrates the comparative analysis of detection time of malicious node for the proposed EETE and the state of the art models: CWSN, HIDS, and LHIDS. It is clear from the result that CWSN and HIDS detect the first malicious node at 4.5s after deploying 40

number of nodes. The detection time of LHIDS increases from 0.7s to 2s as number of nodes increases 4 to 28, thereafter detection time is steady. The EETE responses for first malicious node at 0.7s similar to LHIDS and remain in steady state upto 40 number of nodes. The detection efficiency of EETE is 60% more than LHIDS and 200% more than other two models. The acquired result is obtained due to the utilization of activity based trust dillema game to capture the malicious nodes quickly. Whenever EETE achieves the equilibrium point $(p^*, q^*)$, the nodes get classified into *Normal* or *Illegitimate*. Further, past interaction helps in detection of the malicious activity due to which EETE performs better than the state of the art model.

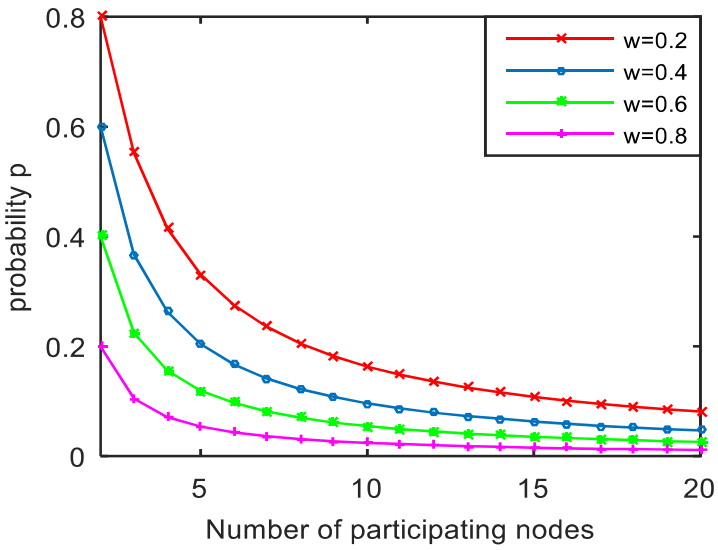



**Figure 3.8.** Number of participating nodes vs Probability

Fig. 3.8 shows the probability of a node to reply after receiving a trust request from the cluster heads for the proposed EETE scheme. In initial phase, when the participating nodes are limited to 2 and weight factor is 0.2, the probability of a node to reply is 0.8. As number of nodes increases up to 20 the probability reduces to 0.081. When the weight factor is 0.8 and number of nodes increses from 15 to 20, the probability of a node to reply a trust request almost reaches to 0. In such scenario, all the nodes assume that other neighbouring nodes are participating in the trust evaluation process and replying to the concern node but in fact, probability of reply is almost zero, therefore no one reply the trust request. It creates a

malicious environment for the illegitimate nodes.To remedy this situation, we choose the optimum value of participating nodes from 5 to 10 and weight factor from 0.2 to 0.6.This is due to the fact that the weight factor proportional to the communication cost and trust values of the nodes. Such as, if a node have the high trust value, the probability to reply is also high.

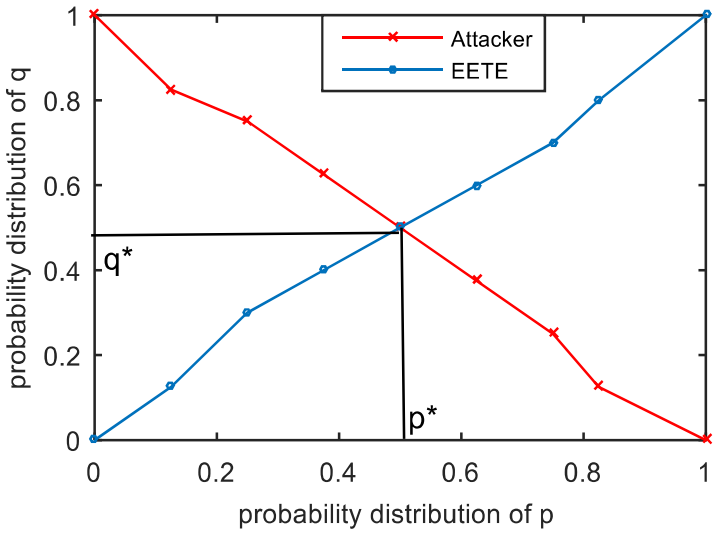



**Figure 3.9.** Probability distribution of p and q

### 3.4.3.4 Optimality analysis of the Activity based dilemma Game

As shown in th Fig. 3.9, x-axis represents the probability distribution of trust of a node from illegitimate node to normal node that determines by CH. Whereas, y-axis represents the probability distribution of a node to become a normal node from illegitimate node or probability of an attacker. Initially, the probability of attacker is 100% towards a victim node that means it behaves as illegitimate node. At that time, probability of a trust determined by cluster head is 0% towards victim node. As the probability of attack on a node decreases up to 50% that means node behaves as either malicious or suspicious, then probability of trust increases by 50% that means cluster head assumes victim node as normal node or malicious node. After that if the probability of attack on a node decreases, the probability of trust increases proportionally. However, it consumes excessive energy to detect whether it is malicious or normal. Therefore, there is a trade-off between detection rate and energy

consumption. So, we stabilised the proposed EETE scheme by using Nash-equilibrium strategy called as Saddle-trust equilibrium where neither the attacker gains too much on the network nor the cluster head losses too much control over the network. The $p^*(0.5)$ represents the probability to gain control over the network by the attacker and $q^*$ $(0.5)$ represents the probability to detect the malicious activity by the cluster head which is shown as Saddle-trust equilibrium point in Fig. 3.9.

## 3.5 SUMMARY

In this chapter, we present a novel light weight trust evaluation (EETE) scheme using game theory to improve the security of clustered-sensor enabled IoT in presence of several illegitimate and malicious nodes. We considered two important factors: trustworthiness and energy efficiency in EETE that are the most indispensable for the existence of the sensor enabled IoT in insecure environment. The EETE provides secure and energy efficient communication among the nodes by employing the evolutionary game theory in cluster formation, and non-cooperative game theory to detect the malicious nodes in the network. The game models also reduce needless transmissions that are required to detect the malicious nodes. Two important inequalities using evolutionary stable strategies have been derived to analyse the energy efficiency and trust of the network in the cluster formation phase. We derived a steady state solution as a Saddle-point equilibrium of the game in which a consensus between cluster head and cluster member is needed to stabilise the network. The simulation results of the EETE scheme are better than that of the current trust evaluation schemes in terms of detection rate and time of malicious nodes, energy efficiency and trust evaluation time. In future works, our goal, is to improve scheme for detection of different kinds of external attacks like denial of service (DoS), black-hole attack and wormhole attack.

# Chapter 4

# A Lightweight Post-Quantum Signature for Green Computing in IoE

---

Post-Quantum Cryptography for elevating security against attacks by quantum computers in Internet of Everything (IoE) is still in its infancy. Most post-quantum based cryptosystems have longer keys and signature sizes and require more computations that span several orders of magnitude energy consumption and computation time, hence sizes of the keys and signature are considered as another aspect of security by green design. To address these issues, the security solutions should migrate to the advance and potent methods for protection against quantum attacks and offer energy efficient and faster crypto-computations. In this context, a novel security framework Lightweight Post-quantum ID-based Signature (LPQS) for secure communication in IoE environment is presented. The proposed LPQS framework incorporates super-singular isogeny curve to make it quantum-resistant. The execution of LPQS is detailed including initialization, registration, signature and validation phases. The unforgeability of LPQS under an adaptively chosen message attack is proved. Security analysis and experimental validation of LPQS are performed to assess its lightweight performance. It is evident that the size of keys and signature of LPQS is smaller than that of existing signature-based post-quantum security techniques for IoE. It is robust in the post-quantum environment and efficient in terms of energy and computations.

The rest of the chapter is organized as follows. *Section 4.1* presents the introduction of IoE and various security breaches. *Section 4.2* briefly introduces supersingular isogeny curve and its problems. *Section 4.3* and *Section 4.4* presents the details of the proposed security framework LPQS. In *Section 4.5*, a security analysis is carried out. *Sections 4.6* discusses about experiment, and analysis of results followed by conclusions presented in *Section 4.7.*

## 4.1 INTRODUCTION

Internet of Everything (IoE) is an interconnection of smart devices, business processes and data structure without any human intervene [117]. It expands applications from digital sensor tools to smart and self-configuring intelligent nodes in distributed hardware to enrich the lives of people [118]. In such smart networks, information security is of paramount importance as all the decisions and actions depend on the accuracy and credibility of the received data [119]. The public-key infrastructure (PKI) plays a critical role in information security. In PKI, however, both sender and receiver authenticate each other with the help of certificates obtained from certificate authority. This process can be time-consuming and complex.

Identity-based cryptography (IBC) schemes remove these barriers and use public strings such as email address or domain name for data encryption and signature verification, instead of digital certificates [120]. Security of IBC depends on solving some mathematical problems such as integer factorization and discrete logarithms. Major recent signature schemes depend on these two mathematical problems which are infeasible to solve on any classical computer. However, these problems can easily be solved by quantum computers in polynomial time. For instance, Shor's quantum algorithm can solve the integer factorization in polynomial-time [121]. Moreover, it can not only forge a signature but also recover private keys. Thus, such system poses serious threats to the modern cryptography. To effectively block these threads, many cryptographers are developing new quantum-resistant algorithms that are unbreakable in the era of quantum computers. Several Post-Quantum cryptography (PQC) classes have been proposed which are currently believed to be quantum resistant namely: lattice-based [122-124], hash-based [125], code-based PQC [126] and isogeny-based [127].

Over the past few years, isogeny-based cryptography has been gaining a lot of momentum owing to its small key sizes. Various isogeny-based cryptosystems have been published for public-key encryption and key exchange protocols [128,129] but later have been broken by a sub-exponential quantum attack. Recently, a key exchange scheme based on supersingular isogeny Diffie-Hellman (SIDH) has been proposed, for which there is no known sub-exponential quantum attack [54] and is much faster than ordinary isogeny. SIDH uses supersingular elliptic curves for key exchange and public key encryption [55,56]. Isogeny-based cryptosystems have also been used for digital signature such as strong designated

verifier signature [57] and undeniable signature [58-59]. However, feasibility of these schemes on resource-constrained devices is not known. Compressed digital signature scheme reduces the public and private key sizes to 336 byte and 48 byte respectively for 128-bit quantum security level. Unfortunately, these primary signature schemes are slower than other quantum signature techniques due to their larger signature sizes.

The prime issues in security by green computing for IoE applications are related to the key size, signature and the encryption computation of the post-quantum based cryptosystems, which must be kept compact to reduce energy consumption and computation time [59]. Most post-quantum based cryptosystems require higher order of magnitude longer keys to provide current level of protection, which are substantial enough to impact energy requirement and computation time [60]. The use of isogeny curve based post-quantum cryptography is considered to be the most practicable solution to energy required for the shortest key's computation. To efficiently exploit resistant capability of post-quantum cryptography, we use super-singular isogeny curve and ID-based signature for post-quantum cryptography that requires much shorter keys to maintain the same level of protection and provides user friendly access of the system. In addition to this, it can also reduce the overall energy and time needed for the crypto operations than post-quantum based cryptosystems is therefore appropriate replacement in sensors, handheld devices, and IoE applications.

In this context, a lightweight post-quantum ID-based signature (LPQS) scheme using a supersingular isogeny curve for secure data transmission in the IoE environment is presented. The design of the LPQS scheme aims to provide a signature scheme for the post-quantum cryptography and to reduce the complexity of the system with fewer system resources consumption. The LPQS scheme uses the identity of the client for the initialization of the process. Further, this scheme uses two isogeny curves for verification to provide double-fold secure encryption. The main contributions of the scheme are summarised as:

1) Firstly, a system model for post quantum security is presented considering its applicability in IoE environments.
2) Secondly, the four phases of the execution of the proposed framework LPQS is detailed including initialization, registration, signature and validation.

3) Thirdly, unforgeability of LPQS under an adaptively chosen message attack is proved and security analysis is performed to show its resistance against various cyber-attacks.
4) Finally, performance analysis and experimental validation of the proposed framework are performed to assess its lightweight performance in realistic IoE environments.

## 4.2 PRELIMINARIES

In this section, we briefly introduce supersingular isogeny curve that has been used to design the proposed signature scheme and its problems to prove its resistance against cyber-attacks.

We consider two elliptic curves $E_A, E_B$ over a finite field $F_q$ also used in [130, 131]. An isogeny φ: $E_A \rightarrow E_B$ is a non-constant morphism that preserves the group structure [132]. The degree of an isogeny φ is equal to the degree of φ as a morphism. An isogeny of degree ℓ is called a ℓ-isogeny [133,134]. If φ is separable, then deg φ= #ker φ. If isogeny is separable between two curves, we say that they are isogenous [135]. Tate's theorem [136, 137] is that two curves $E_A, E_B$ over $F_q$ are isogenous if and only if $\#E_A(F_q) = \#E_B(F_q)$. An isogeny can be identified by its kernel in such a way that for every finite subgroup G of $E_A$, there is a unique $E_B$ and a separable isogeny φ: $E_A \rightarrow E_B$ with kernel G such that φ: $E_B \cong E_A/G$. To obtain subgroup G we can use Vélu's formulae [59]. For every prime ℓ not dividing p, the torsion group E[ℓ] contains exactly ℓ+1isogenies of degree ℓ since the group of ℓ-torsion points form a subgroup E[ℓ].

Isogenies with the same domain and range are called as endomorphisms. The set of endomorphisms of an elliptic curve is represented by $END(E)$ and is maximal order either to a quaternion algebra or to an imaginary quadratic field. The curve is supersingular for the first case, otherwise, the curve is ordinary.

In the case of a supersingular elliptic curve, there is always a curve in the isomorphism class defined over $F_{p^2}$, thus its j-invariant is over $F_{p^2}$. One can construct a so-called isogeny graph for any prime $\ell \neq p$, where an edge and vertex are associated with an l-isogeny and j-invariant respectively. Isogeny graphs with degree ℓ +1 are regular; they are undirected since any isogeny from $j_1$to $j_2$ corresponding to a dual isogeny from $j_2$ to $j_1$. Next, we present a few hard problems related to supersingular elliptic curves over $F_{p^2}$[15].

Problem 1 (Computational Supersingular isogeny ($CSSI_A$) problem): Suppose $\Phi_A: E_0 \to E_A$ to be an isogeny with kernel $(P_A + [\alpha]Q_A)$ where α chose at random from $z/l_A^{e_A}z$ and not divisible by $l_A$. Find a generator $G_A$ of $(P_A + [\alpha]Q_A)$ where $\{ E_A, \Phi_A(P_C), \Phi_A(Q_C)\}$ is given.

Problem 2 (Computational Supersingular isogeny ($CSSI_C$) problem): Suppose $\Phi_C: E_0 \to E_C$ to be an isogeny with kernel $(P_C + [\beta]Q_C)$ where $\beta$ chose at random from $z/l_C^{e_C}z$ and not divisible by $l_C$. Find a generator $G_C$ of $(P_C + [\beta]Q_C)$ where $\{ E_C, \Phi_C(P_A), \Phi_C(Q_A)\}$ is given.

Problem 3 (Supersingular Isogeny Diffie- Hellman (SIDH) problem): let $\Phi_A: E_0 \to E_A$ to be an isogeny with kernel $< P_A + [\alpha]Q_A >$, and $\Phi_C: E_0 \to E_C$ to be an isogeny with kernel $< P_C + [\beta]Q_C >$, where α, β are chosen at random from $z/l_A^{e_A}z$ and $z/l_C^{e_C}z$, respectively. $\{E_A, \Phi_A(P_C), \Phi_A(Q_C), E_C, \Phi_C(P_A), \Phi_C(Q_A)\}$ be given, find j-invariant of $E_0/ <P_A + [\alpha]Q_A, P_C + [\beta]Q_C) >$.

Problem 4 (Supersingular Isogeny Auxiliary Point Computation ($SIAPC_A$)): Suppose $\Phi_A: E_0 \to E_A$ to be an isogeny with kernel $(P_A + [\alpha]Q_A)$ where α chose at random from $z/l_A^{e_A}z$ and is not divisible by $l_A$. The Supersingular Isogeny Auxiliary point computation problem is to find the auxiliary point $\Phi_A(P_C)$ and $\Phi_A(Q_C)$, where $\{E, E_A, P_A, Q_A, P_C, Q_C\}$ are given.

Problem 5 (Supersingular Isogeny Auxiliary Point Computation ($SIAPC_C$)): Suppose $\Phi_C: E_0 \to E_C$ to be an isogeny with kernel $(P_C + [\beta]Q_C)$ where $\beta$ chose at random from $z/l_C^{e_C}z$ and is not divisible by $l_C$. The Supersingular Isogeny Auxiliary point computation problem is to find the auxiliary point $\Phi_C(P_A)$ and $\Phi_C(Q_A)$, where $\{E, E_A, P_A, Q_A, P_C, Q_C\}$ are given.

A signature scheme consists of three polynomial-time algorithms: Key generation, Registration, and Validation. We prove the security of the scheme using the existential unforgeable under an adaptively chosen message attacks (EU-ACMA) [72]. A forger and a challenger play a game where forger uses public key and signing oracle model. Forger issues signature queries to sign oracle to generate a signature $\sigma_i$ of message $m_i$ and oracle sends $\sigma_i$ to the forger. The successful attack is considered when the forger produces valid signature and message pair different from those generated from the query oracle.

Definition 1: A digital signature scheme is existentially unforgeable under an adaptively chosen message attacks (EU-ACMA) if, any adversary Ã cannot produce a valid message-signature pair in polynomial time with access to the signing oracle.

Setup: Suppose we have a function KeyGen to output key pair (pk, sk), and challenger give the pk to the adversary Ã.

Queries: The adversary Ã issues signature queries to sign oracle Ś to generate valid signature $\sigma_1, \ldots, \sigma_i$ corresponding to messages $M_1, \ldots, M_i$

Output: Finally, adversary Ã generates a valid message signature pair $(M^*, \sigma^*)$ and wins the game if $M^* \notin M_i$.

The signature scheme is secure if probability to distinguish between simulated signature and real signature is negligible for adversary Ã with access to signing oracle $(Sign_{sk}(.))$ i.e.,

$$\Pr\begin{bmatrix} (pk, sk) \leftarrow keyGen(1^n) \\ (M_i, \sigma_i) \leftarrow \tilde{A}^{Sign_{sk}(.)}(\text{pk}) \\ Verify_{PK}(M, \sigma) = 1 \; and \; M^* \notin M_i \end{bmatrix} \leq negl\,(\lambda)$$

### 4.3 LIGHTWEIGHT POST-QUANTUM SIGNATURE SCHEME FOR IOE

In this section, the proposed Lightweight Post-quantum ID-based Signature (LPQS) framework is presented focusing on system model for post quantum security and the execution of lightweight post-quantum signature consisting of initialization, registration, signing and validation algorithms.

#### 4.3.1 System Model

We consider an IoE environment in which several heterogeneous smart nodes such as an individual human, an organization, sensors, vehicles, smart watches, smart phones are deployed as shown in Fig. 4.1. We classify these smart nodes in two main categories: service provider, and client. In the IoE environment, a client can be an organization, individual human or any device that wants to access services such as health reports collection, banking, e-commerce. The client encrypts the data with its signature and send it to the service provider. The service provider allows authentic clients to access the service. A service provider provides an organization with three servers: the key generation server, database server, and validation server. For individual clients, the key generation server generates the global parameters and public-private keys. The database server maintains the data and the validation server helps in authenticating the clients. service provider generates appropriate rights using a tag machine

and performs key generation, encryption/decryption using the supersingular isogeny curves. It issues the rights to clients based on the service such as a client can view only his/her data for a particular period.

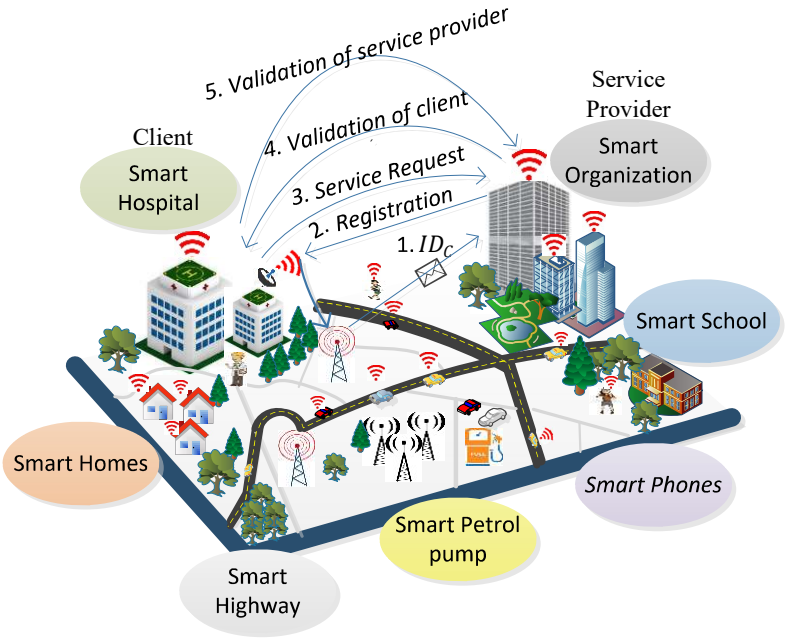



**Figure 4.1.** A system model for the LPQS framework

To ensure secure data transmission between a service provider and clients, and to reduce the complexity of the system with less consumption of the system resources, we present a LPQS scheme for secure data transmission for an IoE environment. The scheme uses supersingular isogeny curves for the post-quantum cryptography signature. The proposed scheme consists of four phases: Initialization, Registration, Signature, and Validation. In the first phase, service provider initializes all the parameters for global access. The second phase, service provider calculates the basis points for the clients using the id of an individual client. A client performs the signature on the data with the help of a service provider in the signature phase. In the validation phase, clients and service providers validate each other using the two isogeny curves.

## 4.4 Lightweight Post Quantum Signature

### 4.4.1. Initialization

Firstly, in the initialization phase, the service provider initializes the system by setting all the global parameters as a set $\{\mathrm{p}, \mathrm{E}, P_A, Q_A, I_A(2), I_B(3), n, m\}$, where the description and use of every parameter is given in Table 4.1. Isogeny-based cryptosystem uses supersingular elliptic curves over characteristics $p$, where $p$ is a prime of form $2^n.3^m.f \pm 1$. Here, $n, m$ are positive integers such that $2^n \simeq 3^m$ and f is a small cofactor to ensure $p$ is a prime. This special form of $p$ allows us to efficiently compute isogenies, as given in the next sections.

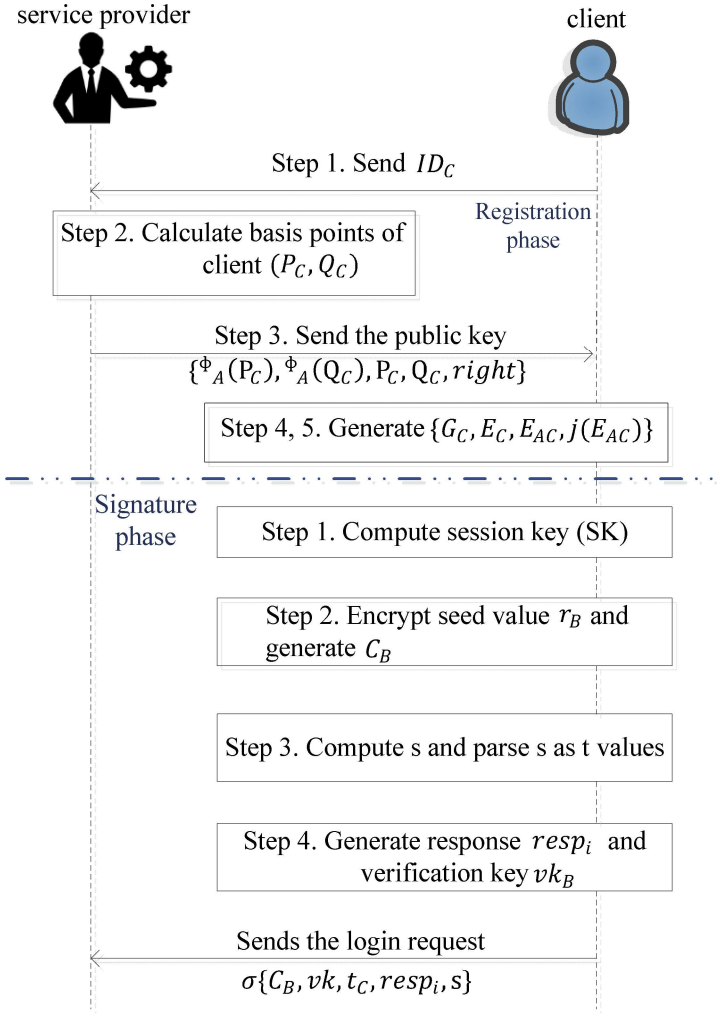



**Figure 4.2.** Flow diagram of registration and signature.

The global parameters generated by service provider include $\{\mathrm{p}, \mathrm{E}, P_A, Q_A, I_A(2), I_B(3), n, m\}$ over the curve $E$ of finite field $F_{p^2}$ of characteristics $p$ with $p^2$ element. service provider selects a random integer α, such that $0 \leq \alpha \leq 2^n$. The random number α is kept secret as service provider's secret key. service provider uses an ephemeral secret key, which changes in every session to support non-traceability. Fix points $P_A, Q_A \epsilon E[2^n]$ such that group $< P_A, Q_A >$ generated by $P_A$ and $Q_A$ in the whole group $E[2^n]$. The elliptic curve points $(P_A, Q_A)$ are the global parameters of the supersingular isogeny-based cryptosystem. $GT_A = P_A + [\alpha]Q_A$, where $< GT_A >$ is the generator of a kernel of service provider which creates a secret subgroup of E $[2^n]$. $E_A = E/< GT_A >$ is the elliptic curve that is the image curve under the isogeny $\{^{\Phi}{}_A\}$.

**Table 4.1** Nomenclature

| Symbol | Description |
|---|---|
| $p$ | Prime number |
| $E$ | Elliptic curve over finite field F |
| $P_A, Q_A$ | Elliptic curve basis points |
| $^{\Phi}{}_A{}^{\Phi}{}_C$ | Isogeny for superingular curve $E_A, E_C$ |
| $n, m$ | Positive integers such that $2^n, 3^m$ |
| $GT_A$ | Generator of a kernel of service provider |
| $f$ | Small cofactor to ensure $p$ as a prime |
| $r_B$ | Seed value |
| $ID_C$ | Identity of client |
| $\|\|$ | Concatenation operator |
| $\oplus$ | Xor operator |

### *4.4.2. Registration*

In this phase service provider performs the registration with the help of client (C) to provide access to the facility/services of the service provider in the IoE environment as shown in Fig 4.2 and the steps are:

Step 1. client sends its identity $ID_C$ generated randomly to service provider through a public channel.

Step 2. After receiving the $ID_C$, service provider calculates basis points of client i.e., $Q_C$ and $P_C$ using the $ID_C$ and $right$, which are assign by service provider and is shown below:

$Q_C = H(ID_C \,||\, f)$ , and $P_C = H(right \,||\, ID_C) \oplus p$

where, $H$ is fixed hash function, and rights are the authority assign to client. The notation $\oplus$ is xor function, and $||$ is a concatenation operation.

Step 3. service provider generates the public key of client $\{\Phi_A(P_C), \Phi_A(Q_C), P_C, Q_C, right\}$ and send it to $client$.

Step 4. Upon receiving $\{\Phi_A(P_C), \Phi_A(Q_C), P_C, Q_C, right\}$, client selects a random number as a secret key from $0 \leq \beta \leq 3^m$. The generator for the kernel of client is $G_C = P_C + [\beta]Q_C$, where $P_C$ and $Q_C$ are the basis for $E_C$ and $E_C = E/< G_C >$;

Step 5. client computes the image curve $E_{AC}$ and also computes shared secret value $j(E_{AC})$, where $j(E_{AC})$ is the j-invariant of the image curve $E_{AC}$.

### *4.4.3. Signature*

The client does as follows to sign message $m$ and is shown in Fig 4.2.

Step 1. client calculates the $session\ key\ (sk) = H(t_C, j(E_{AC}), ID_C, U, V)$, where $U = \Phi_C(P_A), V = \Phi_C(Q_A)$ and $t_C$ is timestamp.

Step 2. Further, encrypt the seed value $r_B$, $C_B = Enc_{ID_C}(r_B \oplus sk)$, for 1≤B≤t,

Step 3. Compute $s = H(m, C_1, .., C_t)$. Parse $s$ as t values $CH_B \in \{0,1\}^C$.

Step 4. If $CH_i = 1$ then response $resp_i = (G_C, \Phi_A(G_C))$ else $resp_i = (\Phi_C(G_A))$. $\Phi_A(G_C)$ is only calculated at service provider and verification key $(vk_B) = h(t_C, j(E_{AC}), ID_C, r_B, CH_B, s)$ for $1 \leq B \leq t$. client sends the login request $\sigma\{C_B, vk, t_C, resp_i, s\}$ to service provider.

### *4.4.4. Validation*

In this phase, service provider and client validate each other and is shown in Fig 4.3.

Step 1. service provider checks the validity of $t_C$ of received signature $\sigma$ and if it is valid

then proceed further, otherwise rejects the request. After checking the $t_C$ validity calculates the image of client with the help of its basis as, ${}^{\Phi}{}_A(P_C) = {}^{\Phi}{}_C(P_A) = U'$, ${}^{\Phi}{}_A(Q_C) = {}^{\Phi}{}_C(Q_A) = V'$ and also compute $sk' = H(t_C, j(E_{CA}), ID_C, U', V')$, $r'_B = Dec_{ID_C}(C_B \oplus sk)$,

for i=1 to t do parse s as t values and check if $CH_i = 1$, then parse $resp_i$. Check if $resp_i$ have order $3^m$ and if $G_C$ generates $E_C$ and ${}^{\Phi}{}_A(G_C)$ generates $E_{CA}$.

If $CH_i = 0$, then check if $resp_i$ have order $2^n$ and generates $E_{AC}$ and $vk' = h(t_C, j(E_{CA}), r'_B, ID_C, CH_{B,}\text{s})$. If $vk'$is equal to $vk$ then *client C* is authenticated.

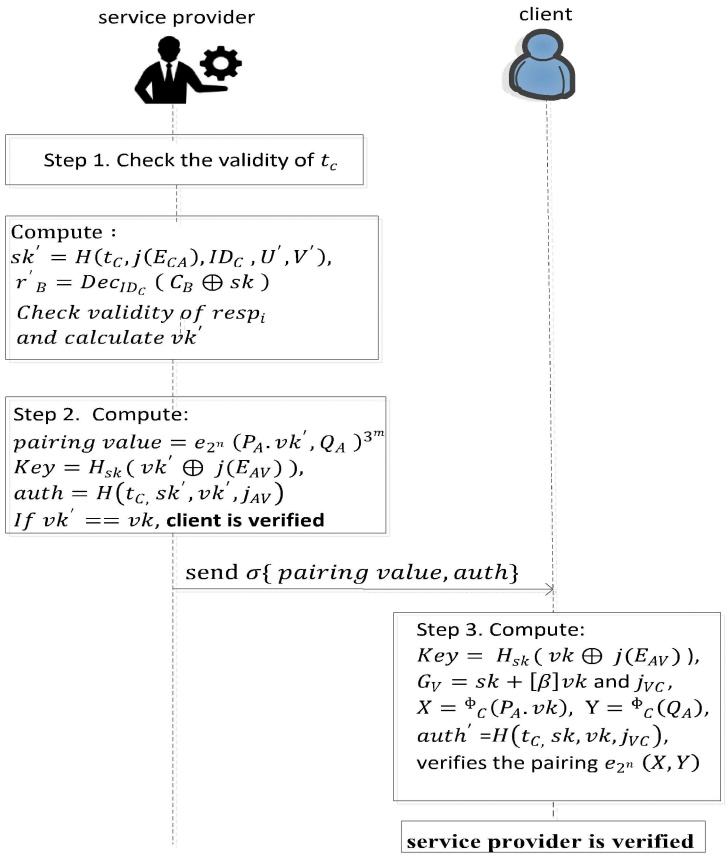



**Figure 4.3.** Work flow of client and service provider validation

Step 2. service provider computes $pairing\ value = e_{2^n}(P_A.vk',\ Q_A)^{3^m}$ and develop the keys using $sk$ and $vk$. Compute the value of ${}^{\Phi}{}_A(sk')$, ${}^{\Phi}{}_A(pk')$, $E_V$ and $j_{AV}$ (as shown in Fig.4.3).

$$Key = H_{sk}(\, vk' \oplus j(E_{AV})\,),$$
$$au\ h = H(t_{C,}\, sk', vk', j_{AV})$$

and send $\sigma\{\, pairing\ value, auth\}$ to client.

Step 3. After receiving the signature, client verify the authenticity of service provider and computes, $Key = H_{sk}(\, vk \oplus j(E_{AV})\,)$ and $G_V = sk + [\beta]vk$ and $j_{VC}$ as shown in Fig 4.4. Further, calculate $X = \Phi_C(P_A.vk)$, $Y = \Phi_C(Q_A)$, $auth' = H(t_{C,}\, sk, vk, j_{VC})$ and also verifies the pairing $e_{2^n}(X, Y)$. Now service provider is also verified.

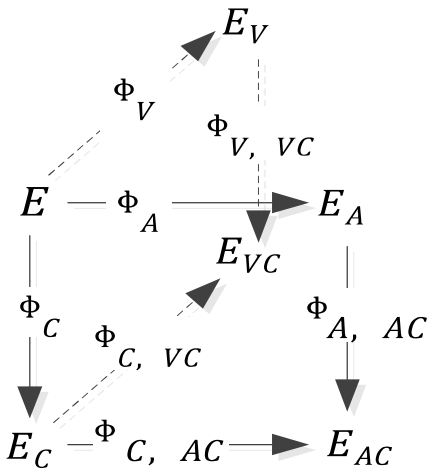



**Figure 4.4.** Isogeny path with its corresponding kernel

## 4.5. SECURITY ANALYSIS

### 4.5.1. Mathematical Security Analysis

***Theorem 1.*** The digital signature LPQS is EU-ACMA in the quantum random oracle model with

$$\mathfrak{E}\,(1/2^n))\,(1-(q_q/2^k-4q_h-q_s))\left(1-\ q_q/2^{|F_{P^2}|}\right) \leq \Pr[C]$$

*Proof*. Suppose an adversary A exists in the system who can produce valid LPQS signatures. It takes system parameters $\{\, \mathrm{p}, \mathrm{E}, P_A, Q_A\,, I_A(2), I_B(3), n, m, P_c, Q_c\}$, public keys $(E_A, \Phi_A(P_C), \Phi_A(Q_C))$ and a verifier $(E_B, \Phi_C(P_A), \Phi_C(Q_A))$. Adversary make queries q to the oracle of client C with queries of a signing oracle (Ş), and a verifying oracle (v), and a hashing oracle ($\mathscr{H}$).

The adversary A aims at producing $\sigma\{C_B, vk, t_C, resp_i, \mathrm{s}\}$ for $M^* \notin M_i$. To generate a regular LPQS signature, he first calculates basis point U, V. Then he computes $sk$ and encrypts the seed value. Let $CH_0, CH_1$ represents the possible outcome of the challenge $ch = 0,1$, respectively with the cardinality of $c$. If $ch = 0$, then $resp = ({}^{\Phi}{}_c(G_A))$ otherwise $resp = (G_C, {}^{\Phi}{}_A(G_C))$. The verifier will accept signature if the $resp$ contains the right order.

We now calculate the success probability of adversary A. The probability of Secret value of signing oracle $(0 \leq \alpha \leq 2^n)$ is guessed successfully is $1/2^n$. The probability adversary A can produce a valid signature by inquiring $q_q$ queries to signing oracle are $\left(1 - \left(q_q/2^k - 4q_h - q_s\right)\right)$ where $q_h, q_s$ denotes the total number of queries for a hashing and signing oracle and $k$ is the output length of the hash function $h$. The $4q_h$ queries are required to calculate $sk', vk', key$, and $auth$. Another probability that A solves the SSCDH problem is atleast $\left(1 - q_q/2^{|F_{P^2}|}\right)$. Therefore, the successful simulation of A happens with a probability of

$$\mathcal{E}\,(1/2^n))\,(1 - (q_q/2^k - 4q_h - q_s))\left(1 - q_q/2^{|F_{P^2}|}\right) \leq \Pr[C]$$

Where $1/2^n < \frac{1}{4}$, $q_q/2^{|F_{P^2}|} < \frac{1}{3}$, so $\frac{\mathcal{E}}{2}\left(1 - \left(q_q/2^k - 4q_h - q_s\right)\right) \leq \Pr[C]$.

This contradicts with the hardness of the SIDH problem (problem 3). Thus, there is no adversary A that could forge signature under an adaptively chosen message attacks.

### *4.5.2. Security Analysis*

In this subsection, we present theoretical analysis of the LPQS scheme to prove its resistance against various cyber-attacks and is described as:

1) *Mutual Authentication*: client and service provider share the message $\{C_B, vk, t_C\}$ and $\{pairing\ value, auth\}$ respectively. $vk$ depends on the $j(E_{AC})$ which is a SIDH problem (Problem 3) and it is hard to find the value of $j(E_{AC})$ . Furthermore, $C_B$ is also difficult to obtain by adversary as it contains $sk$. Similarly, $auth$ can't be calculate because of SIDH hardness. Therefore, our scheme provides mutual authentication.

2) *Anonymity:* In the proposed scheme, client's identity is hidden in the message $\{C_B, vk, t_C\}$, where $vk = h(t_C, j(E_{AC}), ID_C, r_B), C_B = Enc_{ID_C}(r_B \oplus sk)$, $sk = H(t_C, j(E_{AC}), ID_C, U, V)$. To find the value of client's identity, the adversary has to calculate the $j(E_{AC})$ which is a SIDH problem (Problem 3). Therefore, our scheme is secure to maintain the anonymity of the client.

3) *Non-traceability*: Suppose the adversary store the value of $\{C_B, vk, t_C\}$ and the $\{ pairing\ value, auth \}$ exchange between client and service provider. As α and β are the ephemeral keys and changing in each session separately. Even if the adversary guess the private key but not possible to find the auxiliary point $\{^{\Phi}{}_{\mathrm{c}}(\mathrm{P_A}), {}^{\Phi}{}_{\mathrm{C}}(\mathrm{Q_A}), {}^{\Phi}{}_{\mathrm{A}}(\mathrm{P_C}), {}^{\Phi}{}_{\mathrm{A}}(\mathrm{Q_C})\}$ as given in *Problem (4),(5)*.

4) *No verification table*: In the proposed scheme, no verification table has been maintained for the mutual authentication between client and service provider.

5) *Session key agreement*: client and service provider both generate the session key, $key =$ h $(sk, vk, j(E_{AC}))$, where $sk = H(t_C, j(E_{AC}), ID_C, U, V)$, $vk = h(t_C, j(E_{AC}), ID_C, r_B), U = {}^{\Phi}{}_{\mathrm{A}}(\mathrm{P_C})$, $V = {}^{\Phi}{}_{\mathrm{A}}(\mathrm{Q_C})$. For an adversary it is not possible to create a valid login session because of the Problem (4), and (5). So, our scheme could provide the session key agreement.

*6) Perfect Forward Secrecy:* Perfect forward secrecy is provided by $j(E_{AC})$ and is explained in theorem 1.

7) *Attack Resistance:* We present that our scheme is resistant to impersonation attack, replay attack, modification attack, stolen verifier attack and the man in the middle attack.

   *a) Impersonation attack:* According to theorem 1, we can claim that any adversary without any secret key cannot generate a generator as describe in problem (1), (2) and without the generator no auxiliary point can be calculated as describe in problem (4) and (5). So, only a valid client and service provider can create a login message or response $\{C_B, vk, t_C\}$, $\{ pairing\ value, auth\}$. Then the client and the service provider can check the validity of each other by checking the $\{ pairing\ value, auth\}$, and $\{C_B, vk, t_C\}$ and can find out if any adversary is present in the system.

*b) Replay attack:* In the LPQS scheme, client access the service by generating the message $\{C_B, vk, t_C\}$. After getting the message service provider checks the freshness of $t_C$, before executing the other steps. If in any case adversary generate $t_C$ and capture the packet $\{C_B, vk, t_C\}$, adversary wouldn't be able to calculate the key without knowing the private key of client i.e., β. Also, adversary cannot use the same login message in another session as clients and service provider uses the different key {α, β} in each session. So, the client and service provider could find the replay attack by checking the $\{pairing\ value, auth\}$ and $\{C_B, vk, t_C\}$.

*c) Modification attack:* service provider can detect the modification attack by checking the validity of signature $\{C_B, vk, t_C\}$. Similarly, clients check the validity of $\{pairing\ values, auth\}$.

*d) Stolen verifier table attack*: no table is maintained in our scheme by the client or the service provider. So, no such attack is possible.

*e) Man-in-middle attack*: Due to the mutual authentication, no man-in–the middle attack is possible.

8) Due to the usage of supersingular isogeny curves, we can effectively compress the keys and signature size. The infinite field Fp2 elements used to transmit the points ΦA(PC), ΦA(QC) are rather large compared to the size of the integer coefficients. However, we have used compressed curves which can be represented by one field element. The key basis calculated by the nodes need not be published as a public parameter, as long as all nodes are able to generate the same basis independently by a predefined algorithm. It also supports perfect forward-secrecy, nontraceability and anonymity as detailed in Section 4.2. In summary, to efficiently exploit the resistant capability of postquantum cryptography, we have used a supersingular isogeny curve and an ID-based signature for postquantum cryptography that requires much shorter keys to maintain the same level of protection and provides user friendly access to the security system.

In Table 4.2, we compare various security features of the proposed LPQS with non-quantum cryptography models ASMS [60], TinyTate [61], BSNS [62], and IDKEYMAN [63]. It is clearly seen that the proposed LPQS has all the eleven listed security features

T1 to T11 but the non-quantum cryptography models are deficient in terms of security features.

**TABLE 4.2.** COMPARISON OF SECURITY FEATURES WITH NON-QUANTUM CRYPTOGRAPHY SCHEMES

| Security parameters | ASMS | TinyTate | BSNS | IDKEYMAN | LPQS |
|---|---|---|---|---|---|
| T1 | √ | √ | X | √ | √ |
| T2 | X | √ | √ | √ | √ |
| T3 | √ | √ | √ | √ | √ |
| T4 | √ | √ | X | √ | √ |
| T5 | √ | X | X | √ | √ |
| T6 | √ | X | √ | X | √ |
| T7 | √ | X | √ | √ | √ |
| T8 | √ | √ | √ | √ | √ |
| T9 | X | X | X | √ | √ |
| T10 | √ | √ | √ | √ | √ |
| T11 | √ | √ | √ | √ | √ |

T1: Mutual authentication, T2: Anonymity, T3: Non-traceability, T4: No verification table, T5: Session key agreement, T6: Perfect forward secrecy, T7: Impersonation attack, T8: Replay attack, T9: Modification attack, T10: Stolen verifier table attack, T11: Man-in-middle attack, √: Yes, X: No

### 4.6. COMPUTATION COST ANALYSIS

In this section, numerical analysis and simulation results are demonstrated to analyze the performance of the proposed LPQS framework focusing on cost computation in the terms of time, CPU cycles and energy of non-quantum and post-quantum techniques.

The computation cost of the LPQS scheme is given in detail for public key, private key and signature. In this computation, we have neglected the lightweight operations like exclusive-OR and string concatenation. As we know primes $p$ have the form of $2^n.3^m.f \pm 1$, such that $2^n \simeq 3^m$. We compute the cost in terms of λ bits for λ bits of a quantum computer. We assume $p$ has 6λ bits length. All values are calculated for 128-bit security. Our scheme

uses Montgomery curves $E: By^2 = x^3 + Ax^2 + x$, where A–coefficient is sufficed for isogeny computation. The isomorphism classes of Montgomery form have the same Kummer line. So, both can be represented by one field element, requiring 12 λ-bits. We compare LPQS in the terms of the sizes of public and private keys, and signature with variants of lattice, multivariate and isogeny, and is shown in Table 4.3.

**TABLE 4.3**. VARIOUS POST-QUANTUM SIGNATURES SCHEME COMPARISON IN BYTES WITH VARIOUS PARAMETERS SIZES FOR 128-BIT QUANTUM SECURITY

| Scheme | Public key size | Private key size | Signature size |
|---|---|---|---|
| Lattice-based1[122] | 11,653 | 6,769 | 2,444 |
| Lattice-based [73] | 7,168 | 2,048 | 5,120 |
| Multivariate-based [68] | 417,408 | 14,208 | 48 |
| Multivariate-based [69] | 81,800 | 8,900 | 337 |
| Multivariate-based [70] | 136,100 | 101,300 | 79 |
| Hash-based [125] | 1,000 | 1,000 | 41,000 |
| Isogeny-based [127] | 768 | 48 | 141,312 |
| LPQS | 336 | 96 | 79,872 |

4.6.1. Public keys

In LPQS, public keys contain $\{^{\Phi}{}_A(P_C), ^{\Phi}{}_A(Q_C), P_C, Q_C, right\}$, where $P_C$ $and$ $Q_C$, are the points on the elliptic curve E of order $3^m$ calculated by service provider using exclusive-or and concatenation operation. So, its cost is negligible and $right$ needs no operation. Further, torsion basis $(^{\Phi}{}_A(P_C), ^{\Phi}{}_A(Q_C))$ requires three 3 λ-bits coefficients and 12 λ-bits for the curve. Thus, the public key requires 21 λ- bits. For 128-bit quantum, it needs 336 bytes (21×128=2688 bits). Other post-quantum techniques such as lattice based [6-122] and multivariate [28] needs 11,653 bytes and 417,408 bytes, respectively.

*4.6.2. Private keys*

Private keys contain the two generators $GT_{A,}, G_{Av,}$ are described in the section IV. The private key $GT_A$ ( $GT_A = P_A + [\alpha]Q_A$) can be represented as a single coefficient α with respect to the basis point $P_A$ , $Q_A$ and it requires 3 λ- bits. So, for two generators we need 6 λ- bits and for 128-bit security level we need 96 bytes (6×128=768 bits).

*4.6.3. Signature*

Signature of client includes $\{C_B, vk, t_C\}$, where $C_B$ is an encrypted representation of random seed value $r_B$ and $(sk = H(t_C, j(E_{AC}), ID_C, U, V))$. We discussed in the previous section computation cost of $U, V$ is 6 λ- bits and the hash function is 3 λ- bits. The J-invariant $(j(E_{AC}))$ requires 6 λ- bits to store the value in the 128-bit computer. Further, $vk$ $(vk = h(t_C, j(E_{AC}), ID_C, r_B))$ takes 3 λ- bits for the hash function. So the total cost will be 18 λ- bits.

service provider's signature includes the $\{pairing\ value, auth\}$ where mapping cost is negligible and auth = $H_{key}(t_{C,}\ sk', vk', j_{AV})$. The hash function requires 3λ- bits and similarly $sk', vk'$ needs 15 and 3λ-bits, respectively and Key= $H_{sk}(\ vk' \oplus\ j(E_{AV})\ )$ requires 3 λ-bits. Thus, the total signature cost of the client and service provider is 39 λ-bits. Thus, on average, our scheme requires 21λ-bits (336 bytes) for a public key, 6 λ- bits (96 bytes) for private key and 39 $\lambda^2$-bits (39×128×128=79,872 bits) which is equal to 624 bytes for a signature to achieve 128-bit of quantum security. Comparatively, signature size is larger than public and private key because for signature, we use two torsion groups $(E_A, E_C)$ to increase the hardness of isogeny problem but it requires more storage space.

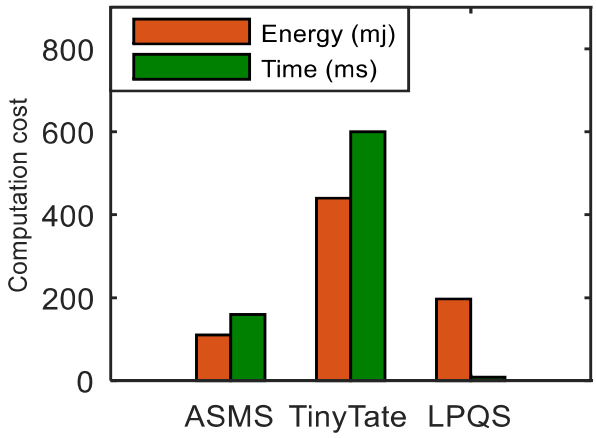



**Figure 4.5.** Computation cost of non-qunatum techniques for energy (in millijoules) and time (in milliseconds) consumption.

## 4.7. Software Implementations and performances

In this section, we evaluate the performance of the ID-based LPQS scheme for secure data transmission in the IoE environment. The C implementation done in [130] is further extended to include the signature scheme introduced in this chapter. For the comparison analysis, we compute the energy consumption, computation time, and CPU cycles taken by the key generation, signing, and verification. We use the C language on the Microsoft Visual Studio 2013 platform on Intel(R) Core(TM) i7-8700 CPU @3.20 GHZ with x64-based processor, running Windows 10 to implement the proposed scheme. Intel Power Gadget 3.7.0 is used to measure the execution time and energy consumption of LPQS. Our scheme uses Montgomery curves $E: By^2 = x^3 + Ax^2 + x$, where A–coefficient is sufficed for isogeny computation. The comparative analysis is performed with state of the art non-quantum and post-quantum techniques.

### 4.7.1. Non-quantum Schemes

In this subsection, we compare energy and time of LPQS with predicate non-quantum signature schemes ASMS [60] and TinyTate [61] for 128-bit non-quantum security level. Non-quantum security 128-bit is approximately equals to 85-bit security level.

ASMS and TinyTate use the elliptic curve $y^2 = x^3 + x$. We have consider one ID and one byte of data transmission using AES-128. In terms of energy, ASMS and TinyTate take 110 mJ and 440 mJ, respectively, to perform key generation, signature and verification. While LPQS needs 196.85 mJ to perform the same task which is 123% more efficient than TinyTate. Total time consumption of LPQS is 8.057 ms. ASMS and TinyTate take 2410 ms and 600 ms, respectively and is shown in Fig. 4.5. So, LPQS is approximately 300 and 74 times faster than ASMS and TinyTate, respectively. The reason for less computation time is the use of isogeny curve. It takes less time to perform addition, subtraction and multiplication and hence overall time reduces effectively. It is notice that 128-bit non-quantum security can be achieve at 85-bit quantum security level with reasonable tradeoff between energy and time.

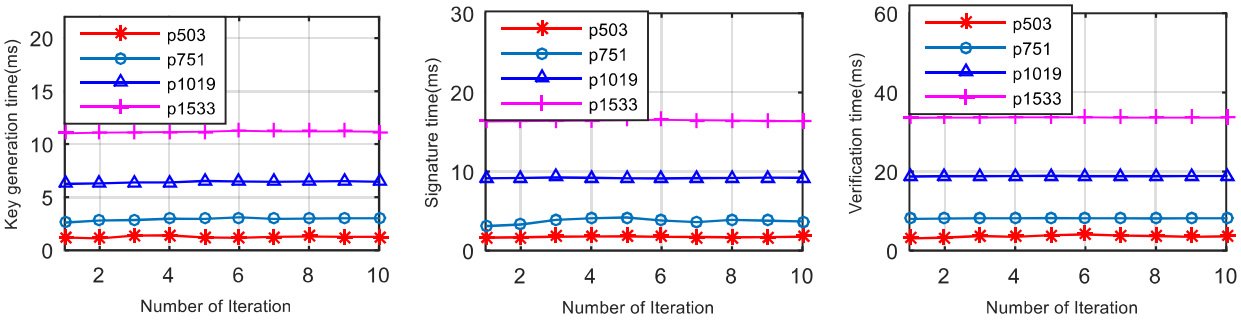
### 4.7.2. Post-Quantum Schemes

In this section, we evaluate the performance of the LPQS scheme with state-of-the-art schemes. The performance of LPQS scheme is evaluated in terms of time for key generation, signature and verification which are iterated for 10 times for prime $p503$, $p751$, $p1019$, and

$p1533$. Comparative analysis of energy with non-isogeny signature schemes SPHINCS [125] and Rainbow [70] are presented. Total number of clock cycles is also analysed and compared with isogeny based schemes Efficient Algorithms for Super-singular Isogeny (EASI) [56], Microsoft's Supersingular Isogeny Diffie-Hellman (MSIDH) [130], Efficient Post-Quantum Undeniable signature (EPQU) [133], and Key Compression for Isogeny-Based cryptosystems (KCIB) [134]. In LPQS, we use supersingular elliptic curves with prime $p = 2^n.3^m.f \pm 1$. For prime $p503$, n is 250, m is 159, f is 1 and it provides 83 bit quantum security which is approximately equals to 125-bit non-quantum security and other prime values are shown in Table 4.4.

**Table 4.4**. PUBLIC PARAMETERS WITH COMPARATIVE NON-QUANTUM AND QUANTUM SECURITY (BITS).

| $p = 2^n.3^m.f \pm 1$ | Non-Quantum security (bit) | Quantum security (bit) |
|---|---|---|
| $p503 = 2^{250}3^{159} - 1$ | 125 | 83 |
| $p751 = 2^{372}3^{239} - 1$ | 186 | 124 |
| $p1019 = 2^{508}3^{319}.35 - 1$ | 253 | 168 |
| $p1533 = 2^{776}3^{477} - 1$ | 378 | 252 |




(a) Key generation time (b) Signature time (c) Verification time

**Figure 4.6.** Various computation time of different phase vs number of iteration with different p values.

**TABLE 4.5**. COMPUTATION TIME OF DIFFERENT PHASES FOR DIFFERENT PRIME VALUES

| Key Generation time with number of iteration | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| p | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| P503 | 1.20 | 1.11 | 1.39 | 1.40 | 1.20 | 1.18 | 1.27 | 1.29 | 1.27 | 1.27 |
| P751 | 2.60 | 2.81 | 2.85 | 2.97 | 2.96 | 3.10 | 2.95 | 2.99 | 3.02 | 3.01 |
| P1019 | 6.25 | 6.30 | 6.39 | 6.40 | 6.53 | 6.49 | 6.45 | 6.49 | 6.51 | 6.45 |
| P1533 | 11.02 | 11.07 | 11.12 | 11.13 | 11.17 | 11.25 | 11.20 | 11.21 | 11.19 | 11.17 |
| Signature time with number of iteration | | | | | | | | | | |
| P503 | 1.65 | 1.69 | 1.77 | 1.79 | 1.81 | 1.75 | 1.73 | 1.69 | 1.71 | 1.76 |
| P751 | 3.10 | 3.30 | 3.90 | 4.10 | 4.20 | 3.80 | 3.60 | 3.90 | 3.80 | 3.70 |
| P1019 | 9.14 | 9.20 | 9.25 | 9.21 | 9.15 | 9.13 | 9.17 | 9.19 | 9.22 | 9.21 |
| P1533 | 16.35 | 16.39 | 16.41 | 16.44 | 16.51 | 16.52 | 16.49 | 16.44 | 16.39 | 16.38 |
| Verification time with number of iteration | | | | | | | | | | |
| P503 | 3.10 | 3.30 | 3.70 | 3.50 | 3.90 | 4.10 | 3.80 | 3.70 | 3.50 | 3.60 |
| P751 | 8.05 | 8.11 | 8.17 | 8.21 | 8.23 | 8.20 | 8.19 | 8.16 | 8.17 | 8.20 |
| P1019 | 18.76 | 18.81 | 18.83 | 18.86 | 18.89 | 18.84 | 18.81 | 18.83 | 18.85 | 18.86 |
| P1533 | 33.58 | 33.62 | 33.65 | 33.69 | 33.70 | 33.68 | 33.64 | 33.63 | 33.63 | 33.64 |

Computation time of key generation for different p values is shown in Fig. 4.6(a) and Table 4.5. All results are run for 10 iteration. For $p503$, $p751$, $p1019$, and $p1533$ key generation's average running time are 1.25 ms, 2.96 ms, 6.45 ms and 11.17 ms, respectively. Further, average running time of signature generation for $p503$, $p751$, $p1019$, and $p1533$ are 1.75 ms, 3.9 ms, 9.20 ms and 16.44 ms, respectively. Signature time is more than key generation time because we use two isogeny curves (i.e., ${}^{\Phi}{}_{A}, {}^{\Phi}{}_{C}$) and only one isogeny is used for key generation (i.e., ${}^{\Phi}{}_{A}$). In Fig. 4.6(c), computation time of verification is shown and it is clear that average running time for $p503$, $p751$, $p1019$ and $p1533$ is 3.45 ms, 8.17 ms, 18.84 ms and 33.66 ms, respectively. Verification needs 3 times more computation time than key generation and 2 times more computation time than signature phase. Thus, most of the computation time is spent on verification because signature size is larger than public and

private keys and in addition, two isogeny operations and one pairing operation are also performed.

**TABLE 4.6.** MESSAGE SIZE VS ENERGY CONSUMPTION (MJ) FOR DIFFERENT P VALUES.

| Message Size (bytes) | 1 | 2 | 5 | 10 | 20 |
|---|---|---|---|---|---|
| P503 | 196.854 | 442.921 | 848.440 | 1791.371 | 3574.868 |
| P751 | 467.154 | 1051.096 | 2013.433 | 4251.101 | 8483.516 |
| P1019 | 1070.640 | 2408.940 | 4614.458 | 9742.824 | 19442.822 |
| P1533 | 1912.624 | 4303.404 | 8243.409 | 17404.878 | 34733.251 |

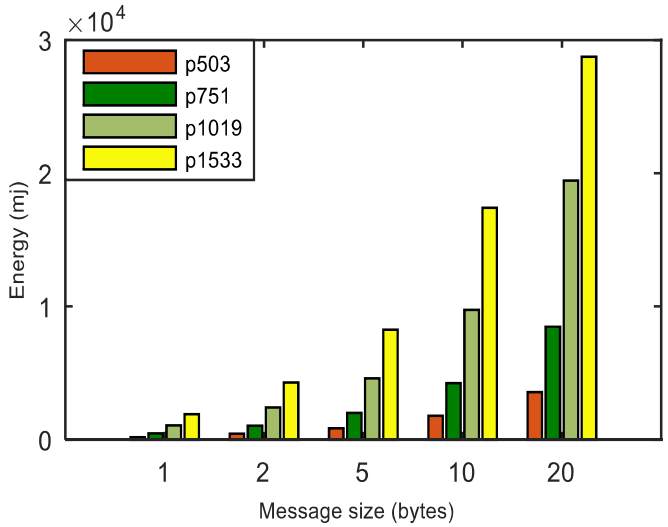



**Figure 4.7.** Comparison for energy (in millijoules) with message sizes (in bytes) for various p sizes.

In Fig. 4.7, energy consumption of the LPQS is shown for different message sizes. Message size impact the energy consumption and is clear from Fig. 4.7 and Table 4.6. For 5 bytes message, maximum and minimum energy consumption are 848.440 mJ and 8243.409 mJ. Energy consumption is increasing exponentially with the increase of the message size and security level. Hence, for security level 256-bit and 20 bytes message size, energy consumption is 34733.251mJ. Total time taken to complete the process for $p1019$ is 43.82 ms, 49.64 ms, 93.00 ms, 103.00 ms and 131.21 ms for 1, 2, 5, 10 and 20 bytes of message, respectively. It is clear from Fig. 4.8 and Table 4.7 that the total time is increasing linearly with increase in the size of messages.

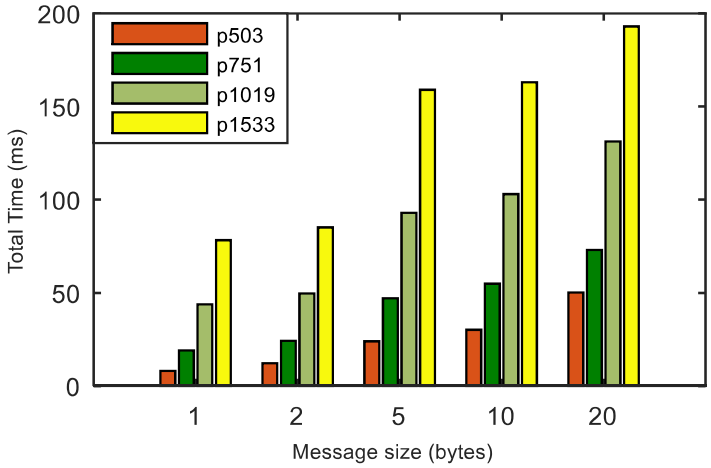
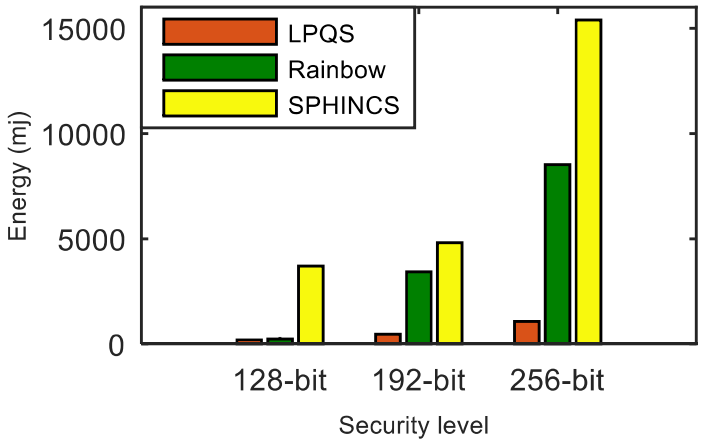



**Figure 4.8.** Total time to perfrom the operations (in milliseconds) vs. different message sizes (in bytes) for various p sizes.

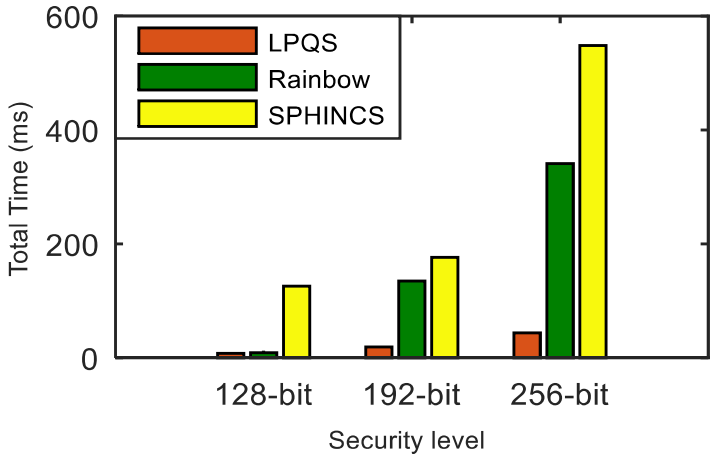
**TABLE 4.7.** MESSAGE SIZE VS TIME (MS) FOR DIFFERENT P VALUES

| Message Size (bytes) | 1 | 2 | 5 | 10 | 20 |
|---|---|---|---|---|---|
| P503 | 8.05 | 12.16 | 24.0 | 30.14 | 50.14 |
| P751 | 19.12 | 24.19 | 47.10 | 54.90 | 73.01 |
| P1019 | 43.82 | 49.64 | 93.00 | 103.00 | 131.21 |
| P1533 | 78.29 | 85.12 | 159.00 | 163.00 | 192.98 |

We have compared energy consumption and time computation of LPQS with non-isogeny signature scheme for 128-bit, 192-bit and 256-bit security level. In this comparison, we are considering message size as one byte for one ID. For 128-bit security level, Rainbow and SPHINCS need energy of 234.76 mJ and 3706.66 mJ, respectively. LPQS consumes 196.854 mJ which is approximately 1.1 times and 19 times more efficient than Rainbow and SPHINCS, respectively and is shown in Fig. 4.9(a) and Table 4.8. For 256-bit security level, LPQS needs 1070.64 mJ while Rainbow and SPHINCS takes 8518.95 mJ and 15394.60 mJ, respectively. Further time taken by Rainbow and SPHINCS for 128-bit security are 9.12 ms and 125.9 ms, respectively. For the same security level LPQS needs 8.057 ms which is approximately 15 times faster than SPHINCS.




(a) Energy consumption (mJ)




(b) Total computation time (ms)

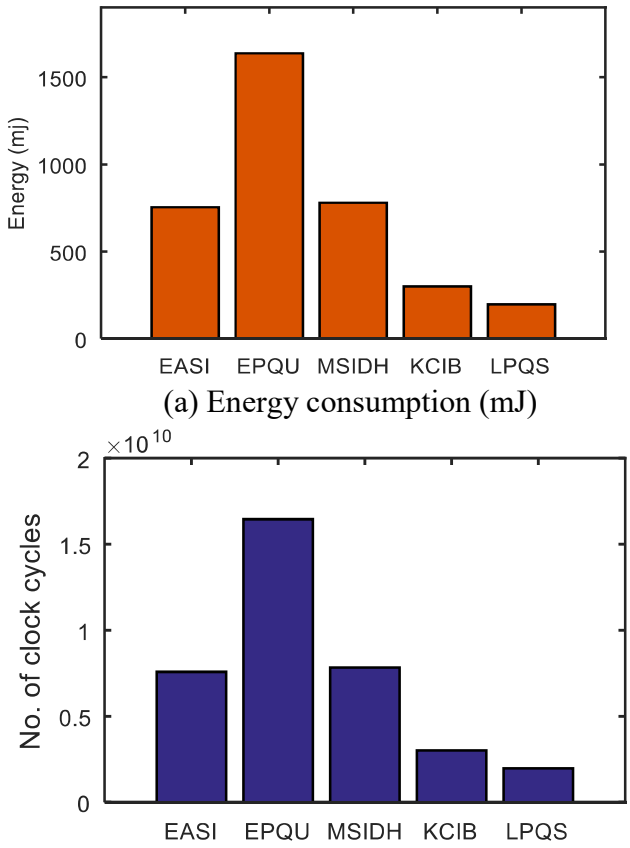
**Figure 4.9.** (a) Energy consumption, (b) computation time comparison of LPQS with non-isogeny based post-quantum signature schemes for 128-bit, 192-bit and 256- bit security level.

**TABLE 4.8.** COMPARISON OF TOTAL ENERGY (MJ) WITH POST-QUANTUM TECHNIQUES AT DIFFERENT SECURITY LEVEL.

| Security level→ | Energy (mJ) | | | Total time (ms) | | |
|---|---|---|---|---|---|---|
| | 128-bit | 192-bit | 256-bit | 128-bit | 192-bit | 256-bit |
| Rainbow | 234.76 | 3421.63 | 8518.95 | 9.12 | 134.93 | 340.86 |
| SPHINCS | 3706.66 | 4812.19 | 15394.60 | 125.90 | 176.57 | 548.30 |
| LPQS | 196.58 | 467.15 | 1070.64 | 8.057 | 19.12 | 43.82 |

For 256-bit security level, Rainbow and SPHINCS take 340.86 ms and 548.30 ms. But LPQS needs 43.821 ms for 256-bit security level and is shown in Fig. 4.9(b). These values may be different for different processor. But LPQS has smaller public and private key sizes (as shown in Table 4.3), and it consumes less energy and time, and is clear from Fig. 4.9.

As shown in Fig. 4.10, EASI takes 754.102 mJ of energy and 7,580 million CPU cycles for SIDH key exchange while EPQU needs energy of 1637.039 mJ and 16,455 million cycles for an undeniable signature. MSIDH and EASI consume 7,836 and 3,009 million cycles, respectively for the complete process. While LPQS takes 1,976 million cycles and needs 196.854 mJ of energy for the signature, which is least among state-of-the-art schemes. The reason for the less energy and fewer CPU cycles consumption is the usage of two isogeny curves instead of one, which takes the previously computed values for the second verification.




(a) Energy consumption (mJ)

(b) Number of clock cycles

**Figure 4.10.** (a) Energy consumption; (b) clock cycle comparison with isogeny based postquantum schemes.

The energy consumption of the embedded devices implemented in Raspberry Pi for different numbers of nodes is shown in Fig. 4.11a. In this environment, the numbers of clients are increasing from 2 to 10. For two clients the energy consumption is 233.109 mJ and for six clients 497.805 mJ for p503. Further, the energy consumption for p1019 with eight clients is 2612.706 mJ. As we know, the keys are computed once and used for a long period of time. For the signature, the clients need only one pairing and hash operation, which takes less energy for computation. Fig. 4.11b shows the number of clock cycles consumed for a number of nodes ranging from 2 to 10. For p751, the number of clock cycles taken are 1391 and 1640 million cycles for 8 and 10 nodes, respectively. The LPQS consumes fewer CPU cycles because it uses previously computed isogeny values for the next computation.

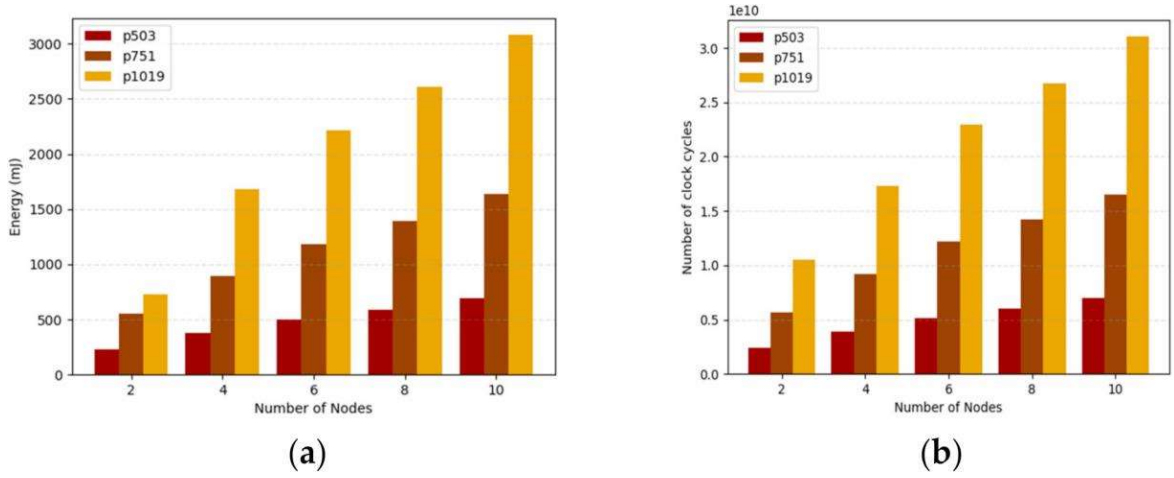



**Figure 4.11.** (**a**) Energy consumption, (**b**) number of clock cycles in million cycles with number of nodes.

## 4.8. SUMMARY

In this chapter, we presented a lightweight postquantum ID-based signature scheme using the supersingular elliptic curve isogeny for the IoE environments. We use the ID for the calculation of the basis for clients and two isogenies for the verification of service provider and clients. Compressed curves are used to reduce the size of keys and validation of signature depends on the commutative property of curves. In comparison with the nonquantum schemes, LPQS outperforms state-of-the-art techniques in terms of time, CPU cycle and energy. Further, Montgomery curves reduced the public and private

keys, and signature sizes. We performed a thorough analysis of postquantum schemes on X86-64 system and Raspberry Pi enabled embedded nodes. The results have clearly shown that the LPQS is feasible for embedded devices. Finally, in comparison with the state-of-the-art techniques, the LPQS scheme is more efficient and secure. In the future, we will extend our scheme to investigate how to represent the elliptic curves efficiently and use the three-party id-based signature scheme based on the supersingular isogeny curve for future networks such data or content focused networking [138] and vehicular communication [139].

# Chapter 5

# Secure IoT Centric Blockchain Framework for Next Generation eHealth Services

The Internet of Things (IoT) plays a crucial role in shaping the future of the next-generation eHealth (NGeH) system with unsurpassed context-aware, mobile, and personalized services. The growing demand for personalized NGeH services raises privacy, accuracy, and scalability concerns due to the increase in extremely sensitive patient eHealth data. Hence, the technical design of the NGeH system should consider these issues to effectively secure eHealth data from unauthorized breaches, certify accuracy in data sharing, and efficiently manage the increase in eHealth data. This chapter proposes, in this context, a novel, secure fog-enabled blockchain framework (SFBF) for NGeH services in the IoT environment to efficiently monitor patients in real time and to manage and securely access patients' electronic medical health records (eMHRs). Three smart contracts have been designed in SFBF to authorize eHealth services for patients or healthcare providers and emergency medical responders and to control the access to patients' eMHRs. Ciphertext-policy attribute-based keyword search encryption has been used to preserve patients' privacy while sharing their eMHRs among the eHealth-care communities. Firstly, a secure NGeH system architecture is presented that comprises a network model and its security needs. Secondly, smart contracts are developed to support eHealth services. Thirdly, the technical design of SFBF is proposed in detail. Finally, security and simulation analyses are performed to demonstrate the efficiency and feasibility of SFBF.

The rest of the chapter is organized as follows: *Section 5.1* presents various healthcare schemes and their limitations. *Section 5.2* briefly introduces basics of blockchain, smart contract, and attribute-based encryption. *Section 5.3* presents the NGeH system architecture and its security requirements. *Section 5.4* presents the design of the smart contracts in detail. *Section 5.5* presents the proposed integrated design of SFBF. *Section 5.6* presents the performance analysis. Finally, we conclude the chapter in *Section 5.7*.

## 5.1. INTRODUCTION

Next Generation eHealth (NGeH) paradigm is a shift from the conventional healthcare paradigm by adopting the concept of context-aware, mobile, and personalized services, offered by the growing wireless network of Internet-connected heterogeneous devices, known as the Internet of Things (IoT) [76, 140]. The NGeH paradigm offers context-aware, and personalized healthcare services everywhere, at any time, and in the right manner [141]. NGeH systems include smart use cases of context-aware sensor networks to gather information related to a patient's activities and a patient's surrounding environment and a wireless body area network (WBAN) to collect vital information such as blood pressure and cardiac index from a patient's body [142]. An example of NGeH services comprises remote patient monitoring to assess a patient's health condition from a remote location outside the clinic settings and emergency medical response to provide immediate assistance to sustain the patient's life under concrete circumstances [143].

In the NGeH domain, instead of being assessed in the face-to-face medical situation of "in-hospital patients," the wearable and non-wearable bio-sensors deployed in the WBAN that are implanted on a patient's body and its surrounding environment, respectively, collect vital and contextual physiological data (e.g., pulse rate, blood pressure, cardiac activity, environment temperature, etc.) remotely, continuously, and in real time [144]. The physiological data, patient profile and so on together are called the electronic medical health record (eMHR). The bio-sensors acquire and transmit a patient's eMHR to one or more local servers (gateways) that may perform further data normalization, fusion or distributed storage. The patient's eMHRs from all WBANs may eventually be transferred to medical databases (or cloud servers). The eMHRs can either be accessed remotely or queried locally from the WBAN by the several eHealth-care communities (e.g., physician, researchers, and insurance companies) to expedite eHealth services. However, implementation of such eHealth systems raises many serious concerns, such as privacy of a patient's eMHR, the accuracy of the received eHealth data, the organization of data, and response delays [145,146].

Incorporating blockchain has emerged in recent years as a promising solution to the issues that exist in the current eHealth systems [147-149]. Blockchain is an immutable ledger of transactions stored openly and in a distributed manner. Only data miners can add the ledger in the

network after verifying all the transactions. This provides transparency and trustworthiness in the network. However, blockchain-based biomedical and eHealth applications face several potential challenges including, but not limited to, 1) stored eMHRs are sensitive and confidential, and anyone in the network can have access to the information, which can damage a patient's reputation [147], 2) Low response time means that as more users incur more transactions, waiting time increases sharply during peak hours to complete one transaction [148], 3) Sharing the sensitive eMHR to a third party without a patient's permission causes various privacy issues [149].

It is essential to have a robust data encryption and authorization mechanism in an IoT-enabled NGeH system to preserve confidentiality and prevent unauthorized access of sensitive eMHRs. Attribute-based encryption (ABE) gained much popularity to provide fine-grained access control over encrypted eHealth data [84, 85]. Efficient search over encrypted data and secure access control are vital concerns in the healthcare system. Searchable encryption has been extensively explored to retrieve the eMHR of interest from the healthcare system [86]. CipherText-Policy Attribute-Based Keyword Search encryption (CP-ABKS) has attained great interest from both the academic and industrial communities for furnishing the searchable encryption and fine-grained access control [87]. A user can decrypt the ciphertext in CP-ABKS only when his set of attributes matches the access policy and the generated trapdoor matches the indexes simultaneously.

Although CP-ABKS is a solution for access control, communication and computational costs increase linearly with the number of attributes [89]. This increment in cost is not feasible for strict, energy-constrained, WBAN-enabled IoT and may impede its wide range deployment; this demands an alternative solution [142, 144]. Fog computing acquired much popularity as a promising solution and is particularity vital for computationally intensive and delay-sensitive applications, such as healthcare applications [150]. Fog computing contains the placement of small but powerful servers referred to as fog nodes closer to resource-constrained devices (users) in the form of a distributed network and offers an operative solution for offloading the communication and computation costs to fog nodes. Furthermore, smart contracts can potentially meet the future healthcare demands to provide a real-time response in emergencies by enabling anytime, anywhere capture and analysis of patients' data [94, 95]. But these solutions raise the following questions:

1) How to securely offload the data to cloud servers in the presence of fog nodes to maintain the privacy of patients? 2) How to design and deploy smart contracts while balancing the response time and privacy in a flexible healthcare environment? Considering such shortcomings, we need to develop a fast and secure blockchain framework for advanced eHealth services to deal with privacy, scalability and response issues.

A fog-enabled blockchain framework (SFBF) for next-generation eHealth services is presented in this context to offer secure remote health-care monitoring and privacy-preserving access mechanisms for eMHRs. It incorporates fog nodes to deliver the real-time solution in medical emergencies due to its presence in the close proximity of end users. Furthermore, fog nodes perform the encryption and data storage operations with the help of smart contracts that reduce the overhead of end users. Only legitimate users can access the eHealth services due to the use of smart contracts. The Chapter's main contributions are summarized as follows.

1. Firstly, an NGeH system architecture is presented comprising the network model and security requirements for NGeH services in the IoT environment.
2. Secondly, we designed three smart contracts, namely authorization contract (AC), emergency service contract (ESC), and access control contract (ACC), to streamline complex medical workflows and to ensure proper handling of eMHRs.
3. Thirdly, the core design of SFBF for NGeH services is presented focusing primarily on secure remote health-care monitoring and eMHR sharing by integrating an access control mechanism using CP-ABKS and blockchain-based smart contracts.
4. Finally, security and numerical analyses are performed to demonstrate the efficiency and feasibility of the proposed healthcare system.

## 5.2. PRELIMINARIES

This section introduces the background required for the construction of the proposed secure fog-enabled blockchain framework (SFBF) for next-generation eHealth (NGeH) services.

### 5.2.1. Blockchain

Blockchain is a decentralized and distributed ledger consisting of records that store immutable transactions across various networks. The entire process of transaction generation and storage is secure and transparent and, thus, builds trust among the nodes. Each block in blockchain comprises a block header and body, in which the block header contains the hash of the previous block and Merkle root, and the body contains transactions and smart contracts. Blockchain comprises existing technologies such as distributed ledger, consensus protocols and cryptography [148, 149]. Based on the access control requirements, there are three basic types of blockchain: public blockchain, private blockchain and consortium blockchain. SFBF uses consortium and private blockchain. The reason for choice is because consortium blockchain allows only preset nodes to perform the consensus mechanism and verifies the transactions in near real time. Consortium blockchain is implemented at the fog level, so that fog nodes perform transactions openly but privately quickly and securely.

A smart contract is an immutable self-executable code that leverages the blockchain technology. The transaction executes when predefined rules are met and verified. The primary objective is to fulfil general terms of contracts. It performs trusted transactions between two anonymous parties without any central authority or external enforcement mechanism. Users can easily interact with smart contracts via functions or application binary interfaces (ABIs). ABI is an interface between two contracts and is executed by one transaction of another contract, and functions are executed by calling the function's name without sending any transaction or message.

### 5.2.2. Ciphertext-Policy Attribute-Based Keyword Search Encryption

Ciphertext-policy attribute-based keyword search (CP-ABKS) encryption is a powerful and promising mechanism, in which a trusted authority generates a public and secret key pair for a user, based on attributes that can be used as a user's identity [84, 85, 151]. Messages are encrypted in this scheme with regard to the set of attributes, and decryption is performed only when the receiver has a matching key for the same set of attributes. The CP-ABKS scheme comprises six fundamental algorithms: System Setup, Key generation, Encryption, Trapdoor, Test and Decryption.

1. **System setup**

   ***Setup****(λ, ℵ) → (pp, MSK, MPK)*: Trusted authority (TA) runs the S*etup* algorithm. The algorithm takes the implicit security parameters (λ) and an attribute universe ℵ as inputs. It generates public parameters *(pp)*, master secret key (*MSK*) and master public key (*MPK*) as outputs.

2. **Key Generation**

   ***KeyGen****(MSK, id, s) → (sk, pk)*: The KeyGen algorithm takes the *MSK*, identity of user *id* and user's attribute set *s* as inputs. It generates the user's secret key *sk* and public key *pk* as outputs.

3. **Data Encryption**

   ***Encryption****(pp, ℵ, A, pk, sk, M) →(C, I):* Encryption algorithm runs by owner of the data. This algorithm takes as inputs public parameters *pp*, attribute universe ℵ, access structure *A*, public key *pk*, secret key *sk*, and message *M*. It outputs cipher-text *C* and data index *I*. Only the user with the valid access structure would be able to decrypt the message *M*.

4. **Trapdoor**

   ***Trapdoor****(MPK, sk, w) →P*: This algorithm takes TA's master public key, secret key *sk* of receiver and keywords *w* as inputs and outputs the trapdoor *P*.

5. **Test**

   ***Test****(P,I) →0 or 1:* Before sending the encrypted file to the requester, the cloud server tests whether the data index *I* contains the keyword *w* specified by the trapdoor *P*. If the trapdoor does not match with pre-defined structure, cloud server outputs *0* and terminates the algorithm. Otherwise, cloud server outputs *1*.

6. **Data Decryption**

   ***Decryption****(C, sk) →(k, M):* This algorithm takes ciphertext *C* and secret key sk as input and outputs the symmetric key *k* and message *M*.

## 5.3. NGeH System Architecture

This section describes the proposed network model for NGeH services and its associated entities, focusing on their roles and security requirements for NGeH services in the IoT environment.

### 5.3.1. Network Model

The secure fog-enabled blockchain framework (SFBF) Network model comprises three layers, as Fig. 5.1 shows. Data accumulation layer (layer 1) incorporates a number of sensor nodes such as biometric shirt, pulse and spo2, and smartwatches. These sensor nodes continuously capture the various electronic medical health records (eMHR) such as body temperature, oxygen level, heart rate and blood pressure. The collected health records are directly outsourced to the fog layer (layer 2) with the help of a local gateway in order to preprocess the eMHR. The fog layer contains many servers and databases known as a local medical supervisor (LMS) and are deployed in the vicinity of patients. The LMS acts as a cluster head and the patient is a cluster member. LMS monitors the patients remotely and classifies the received patient's data as urgent or normal. For instance, if any emergency occurs, it alerts the hospital and the patient's relatives and also maintain a blockchain. The cloud layer (layer 3) contains a centralized data center known as the cloud storage server that stores the encrypted eMHR coming from the LMS. It allows a number of complex searching tasks and maintains a blockchain. The network model includes six entities whose main roles are explained as follows:

1. *Trusted Authority*: TA is a trusted entity that registers all the entities (users, patients, LMSs), generates private-public key pairs, and manages the attributes using CipherText-Policy Attribute-Based Keyword Search encryption (CP-ABKS). It also issues the smart contracts to the respective party as requested.
2. *Patient*: Patients are equipped with sensors such as biometric shirts, smartwatches, and GPS to monitor their heart rate, oxygen level, and electrocardiogram.
3. *LMS*: Local medical supervisor is a decentralized and localized data centre that monitors a cluster of patients remotely and classifies the data as urgent or normal. It allows a large number of computational tasks, through virtualization technology, to reduce the complex computational

cost for users. It makes an appropriate real-time response in emergencies. Smart contracts help the LMS to make decisions in emergencies.

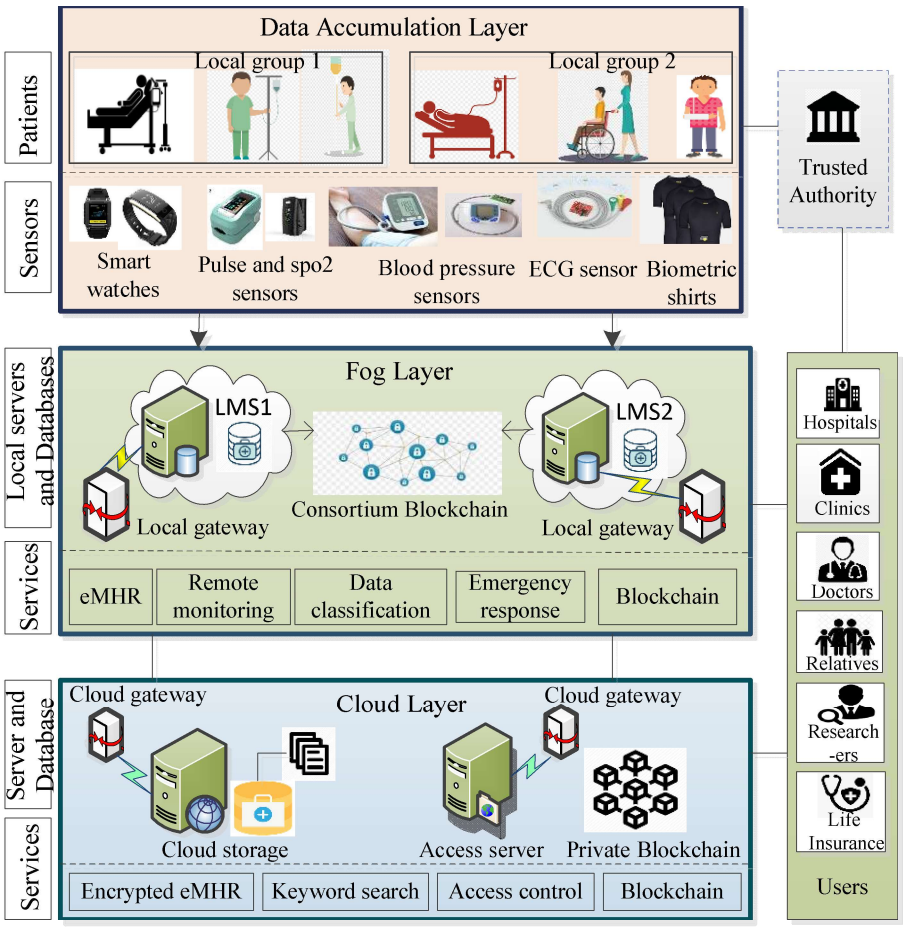



**Figure. 5.1.** Conceptual View of NGeH System Architecture

4. *Users*: Users are patients, doctors, researchers, hospitals, clinics, life insurance providers and patient's relatives who want to access the medical records or remote monitoring.
5. *Cloud Server*: Cloud server stores the encrypted eMHR and provides data access for legitimate users. It also provides the keyword search when a trapdoor is received from a user. It carves away the difficult task of maintaining and tracking eMHR for users. The availability of complete eMHR when requested helps in proper diagnosis and research.
6. *Blockchain Network*: This is a technical infrastructure that provides applications for the ledger and smart contracts. Consensus nodes handle the state of transactions and smart contracts. The

smart contracts primarily help to store eMHR, and LMSs together form a consortium blockchain with the help of consensus nodes. Furthermore, cloud server forms a private blockchain to perform a search query for authentic and valid users.

The user sends a search query to the cloud server to perform the search on the medical dataset. Cloud server first checks the authenticity and validity of the user and query, respectively. Once authentication is done, it searches in its database and if any medical record matches the requested set of attributes, sends the encrypted eMHR to the requester. Upon receiving the file, the user performs a symmetric decryption algorithm with the keys and decrypts the medical record.

### 5.3.2. Security Needs of NGeH Services

We need secure communication to provide eHealth services for advanced detection, precise diagnosis, and to maintain the privacy of the user. Based on the latest research efforts, [89, 95] blockchain can be used as a service if satisfies the following security requirements.

- *Identity Privacy*: Cloud server and other users should not be able to extract the real identity of a patient from eMHR.A adversary should also not be able to know the identity from intercepting messages.
- *Traceability*: As we know, data is stored in encrypted form. If any user misbehaves, then the system should be able to detect who is performing the illicit activities.
- *Message Authentication*: Cloud server should be able to verify the credentials of the message received from the users. Users should also be able to authenticate the medical record received from the cloud server.
- *Authentication of the search result*: Users should be able to detect whether the received data records are relevant to the keywords requested or not.
- *Resistance to cyber-attacks*: A blockchain-based system should generally be able to resist the various cyber attacks, such as replay attack, modification attack and impersonation attack.

**Algorithm 5.1.** Authorization Contract

**Input**: address, name, unique identity, name, value

**Output**: serial no, validity, timestamp, keys, fog server id

```
1.  contract Authorization {
        //parameters
        //address of the user
2.  address place;
        // unique identity provided by government
3.  string unique_identity;
        // name of user
4.  char name;
        // what type of service required
5.  string value;
6.  event register (address place, string unique_identity,
        string fog_server_id, uint256 validity, char name,
        string value, uint256 time, uint256 keys );
7.  event modify (uint256 validity, string unique_identity, address place);
8.  event delete (string unique_identity);
        // constructor to initialize the registration details
9.  func Authorization (address place, string unique_identity, char name,
        string value) public {
        // check for validity of unique_identity and address
9.1.    require (verify_add? (address, unique_identity));
        //initialize the details of the user
9.2.    address location = place;
9.3.    string u_id = unique_identity;
9.4.    char name = name;
        // The type of service user wants, it can be Emergency service or search
9.5.    string type = value;
                //generate the public keys and secret key using ABE and register the user
9.6.    emit register (location, u_id, server_id, date, name, type, now, keys);
9.7.    emit ("register successfully");
        }
        // function to update the information
10. func update (address place, string uniqu _identity, uint256 validity)
        public{
            // check if validity expired
10.1.   require (verify_validity? (unique_identity, validity));
10.2.   if (validity expired)
10.3.   emit delete (u_id);
10.4.   if (location is changed)
```

```
10.5. emit modify (u_id, location, location new);
10.6. emit ("updated successfully");
        }}
11. // end contract
```

## 5.4. SMART CONTRACTS CONSTRUCTION

In this section, we present three smart contracts for the proposed secure fog-enabled blockchain framework (SFBF) to assist in an authorization process for legitimate users, emergency medical response, and accessing of patients' eMHRs.

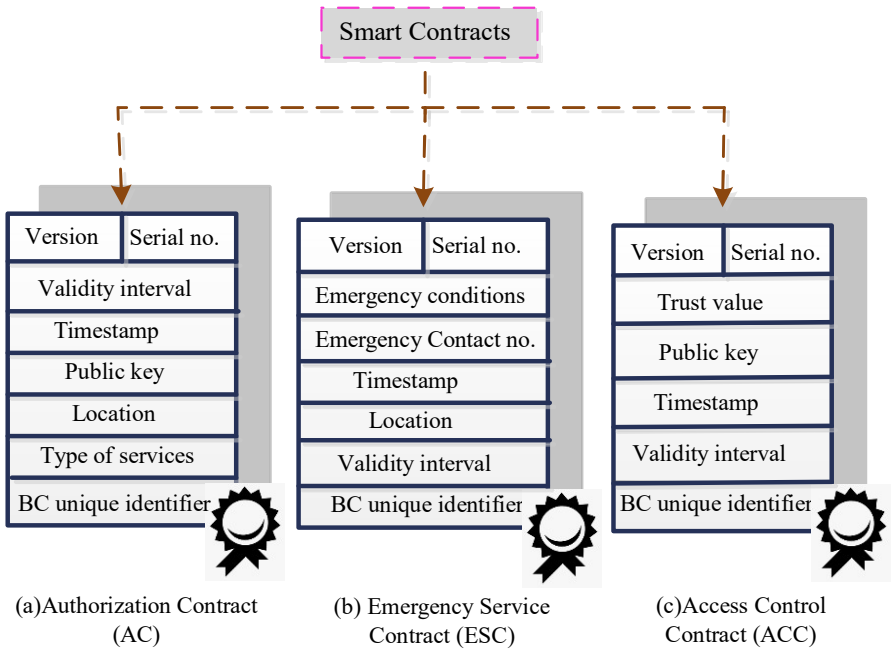



**Figure. 5.2.** Content of AC, ESC and ACC.

### 5.4.1. Authrization Contract (AC)

All the registered users have an authorization contract (AC) with a unique serial number. It decides which type of service will be given to a user per the request. It also maintains an authorization table that stores information about users, such as serial number, validity and location, as Fig. 5.2(a) shows. Algorithm 5.1 demonstrates a smart contract AC to register and update the

user information with the help of functions and ABIs. Function $Authorization()$ first checks the validity of the unique identity provided by a user. If the identity is valid, it calls the event $register()$ to store the user's details and generate an AC with a unique serial number. Function $update()$ ensures that only valid users gain access to the network. For instance, if any contract expires, it automatically deletes the contract by invoking the event $delete()$. Additionally, it fulfils the user's request to update the data by using event $modify()$.

**Algorithm 5.2.** Emergency Service Contract

**Input**: serial no, location, disease, state, encrypted data, contact no

**Output**: version, serial no, emergency contact, validity, encrypted database

```
1.  contract EmergencyService{
                    //function to store the monitored data into database in
                                        encrypted form
2.  func DataEncryption (char disease, uint256 serial no,
                         address location)
    public {
    //check for valid serial no
2.1 require(verify_serial_no? (serial_no));
    // assign the condition of patient as weak, medium, or strong
2.2 string state = weak;
    // interval for data recording depends on condition of patient.
2.3 uint256 interval_of_data_record = 10 mins;
    // call for database storage in local and cloud database using
    public and private keys
2.4 event storage (char disease, uint256 ser    no,
                                        uint256 encrypted_data);
2.5 emit ("Data stored successfully");
3.  func MonitoringandAlertGeneration( char disease, uint256 serial_no,
    uint256 emergenc  contact_no,
    address location) public{
    //call for predefine conditions of illness
3.1 event EmergencyCondition(char Disease, uint256 searial_no);
3.2 if (receivedData ≠ Nor     )
3.3 event CallAmbulance (serial_no, service, location);
3.4 event CallEmergencyContact (serial_no, contact_no, address);
      //after calling for emergency, generate a transaction in
    database
3.5 emit ("Emergency emerged");
    }}
4.  //end contract
```

### 5.4.2. Emergency Service Contract (ESC)

This contract is issued by LMSs to the legitimate patients in their cluster, as algorithm 5.2 shows. ESC contains the address of AC, to link both the contracts. This smart contract stores the patient's information like emergency conditions, contact no etc. , as Fig. 5.2(b) shows. Once data is received from sensor devices, ESC calls the function $DataEncryption()$ to encrypt eMHR and outsources the encrypted eMHR to cloud server. If any emergency emerges, ESC invokes function $MonitoringandAlertGeneration()$ and trigger events $callAmbulance()$ and $callContact()$ to send an alert to the hospital and relative about the severe condition of the patient.

### 5.4.3. Access Control Contract (ACC)

TA issues this contract to the users who want to access the the patients' eMHR. Access control contract (ACC) allows the peer to search for eMHR in the system based on keywords and is given in algorithm 5.3. This smart contract also contains the address of AC to link both the contracts. Users search for eMHR through a number of keywords. Once the request is received, ACC initiates the function $GenerateRequest()$ and calls the event $trapdoor()$ and $request()$, and sends the generated trapdoor and request to the cloud server. Sometimes malicious users try to keep the system busy by sending too frequent service access requests or by canceling the request after generation. ACC maintains the trust value of users to protect the system from such behavior. Fig. 5.2 shows the ACC details.

**Algorithm 5.3.** Search Contract

**Input**: serial no, keywords
**Output**: trapdoor, encrypted eMHR files

```
1.  Contract SearchContract{
    // parameters
2.  string keywords;
3.  func GenerateRequest (serial_no, key, keywords) public {
    // check for validity of serial no
3.1 if (serial_no is valid)
3.2 event trapdoor (uint256 key, string keywords);
3.3 event request (uint256 request_id, uint256 serial_no, uint256
     timeastamp, uint256 session_id, uint256 trapdoor_output);
```

```
3.4 else
3.5 emit ("contract not valid");
    }}
4. //end contract;
```

## 5.5. INTEGRATED DESIGN OF SFBF FOR NGEH SERVICES

This section presents the working of the proposed secure fog-enabled blockchain framework (SFBF) in detail. The SFBF comprises six core modules, namely system setup, smart contracts deployment, patient registration, data generation and encryption, trapdoor generation, and file retrieval.

### 5.5.1. System Setup

Trusted authority (TA) calls the Setup algorithm and generates public parameters $ABEParams = \{G_0, G_1, p, H, g, MPK\}$, where $G_0, G_1$ are two cyclic groups with the same order of prime number $p$ and satisfy a bilinear pairing mapping $e: G_0 \times G_0 \rightarrow G_1$. Let $H$ is a cryptographic hash function defined as $H: \{0,1\}^* \rightarrow G_0$, and $g$ is a random generator of $G_0$. It selects random $a_k$ attribute and compute $A_k = g^{a_k}$ for each $k \in \{1, \ldots, 3n\}$. Finally, TA selects two random numbers $y, \alpha \in Z_p$ and outputs master public key MPK and secret key MSK as $MPK = \{Y,\ A_1, .., A_{3n}, e(g,g)^{\alpha}\}$, where $Y = e(g,g)^{y}$ and $MSK = \{y, \alpha, a_1, \ldots\ldots, a_{3n}\}$ and various parameters of ABE are shown in Table 5.1.

### 5.5.2. Smart Contract Deployment

TA deploys smart contracts into the blockchain. TA has authorized all local medical supervisors (LMSs) in advance to participate in the consensus process, and it forms a consortium blockchain following the practical Byzantine Fault tolerance PBFT [153] consensus mechanism. LMS verifies whether or not the contract is legitimate. The smart contract receives a unique address once it is verified. The transaction will execute accordingly whenever it is invoked.

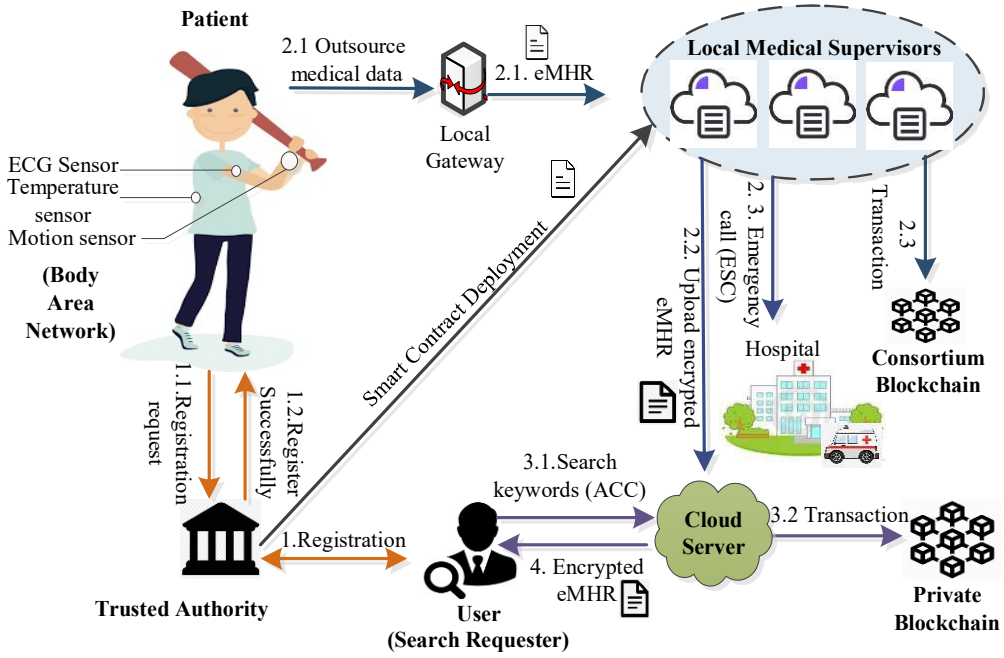



**Figure 5.3.** Flow diagram of SFBF for NGeH services.

### 5.5.3. Patient Registration

Every user in the system registers with TA to receive its secret authentication credential in this phase. All the communication in this phase is completed within a secure channel.

**Table 5.1.** Description of various parameters of ABE

| Parameters | Description |
|---|---|
| N | A universal attribute set {1,2,…. . n} |
| B | User's attribute list |
| I | An attribute set used for an access structure on an encrypted index and I is subset of N. |
| A | Access structure |
| $w$ | Keyword |

1. Initially, user $u$ generates a register request stating the type of service (e.g., monitoring or accessing eMHR) as $register =< register||u||timestamp||type >$ and sends the request to TA, shown in Fig. 5.3 as step1.1.

2. Upon receiving the request, TA selects a random number $x_u \in Z_p$ and KeyGen algorithm computes $Y_u = Y^{x_u}$, where $x_u$ and $Y_u$ are master key and public key, respectively, of the user. TA invokes the event $register()$ to generate secret key $sk$ of the requested user $u$.
3. For every attribute $i \in A$, it selects random $t_i$ from $Z_p$ such that $t = \sum_{i=1}^{n} t_i$. Additionally, TA maintains a legitimate user list UL to identify who is allowed to access the dataset calls. Specifically, $u$ selects random $s \in Z_p$ and TA computes $\widetilde{sk} = g^{y-t}$ and for $i \in B$, $sk_i = g^{t_i/a_i}$, $\overline{Q_u} = Y_u^{-s}$ and stores (u, $\overline{Q_u}$ ) into its dataset.
4. Finally, TA loads secret key $\{x_u, \widetilde{sk}, sk_i\}$ into the user's list, and the user is successfully registered, s shown in Fig. 5.3 as step 1. 2.

### 5.5.4. Data Generation and Encryption

Once a patient is successfully registered, the LMS starts to monitor the electronic medical health record (eMHR) via calling function $Monitoring\ and\ AlertGeneration()$. Before storing and outsourcing eMHR(F), LMS encrypts the eMHR ($E_k(F)$) with a symmetric key $k$ and calls the function $DataEncryption$. LMS encrypts the symmetric key $k$ and generates a secure index for the file by the encryption algorithm.

1. Key encryption: $\tilde{C} = k.e(g,g)^{\alpha s}$
2. Index generation: After encryption of the symmetric key, LMS generates a secure index $Q$ for the eMHR F as follows: $\tilde{Q} = g^s, \hat{Q} = Y^s$. Given an access policy $i \in I$, let $Q_i = A_i^s$ and $Q_i{}' = \alpha.a_i$. Finally, the LMS sends the encrypted file $\{E_k(F), \tilde{C}, \tilde{Q}, \hat{Q}, Q_i\}$ to the cloud server, shown in Fig. 5.3. as step 2. 2.
3. The LMS remotely monitors the patients' health via the calling function $Monitoring_and_alert_generation()$while outsourcing the data. The application binary interface (ABI) automatically calls the nearby hospital and the patient's relatives if the coming eMHR shows irregular behaviour and generates a special transaction $Tx$ as

$$Tx = [Tx_{id} || AC || E_k(F) || T_{stamp}]$$

where $Tx_{id}$ is the hash digest of $Tx$ and $T_{stamp}$ is the timestamp of transaction generation, shown in Fig. 5.3. as step 2. 3.

### 5.5.5. Trapdoor Generation

1. Every legitimate user, such as researcher, hospital or medical insurance, generates a trapdoor for the required keyword via function $GenerateRequest()$. It uses the Trapdoor algorithm and selects a random number $\beta \in Z_p$ for the requesting user $\bar{u}$ and computes $\tilde{P} = \widetilde{sk}^{\beta}$, $\hat{P} = \beta + x_u$, and $P_i = {sk_i}^{\beta}$. Hence, trapdoor $P = \{\tilde{P}, \hat{P}, \{P_i\}_{i \in N}\}$. It also generates $requestmsg = < req_{ID} || P || AC || T_{stamp} >$, where $req_{ID}$ is the identity of request message, shown in Fig. 5.3. as step 3.1.
2. After sending the trapdoor $P$ with $request\ msg$ to the cloud server, a session is created for eMHR search as $Session = < SC || requestmsg || session_{ID} || T_{stamp} >$, and a transaction $TX_x$ is generated corresponding to the request as

$$\mathrm{TX_x} = [\mathrm{Tx_{ID}} || \mathrm{session_{ID}} || \mathrm{T_{stamp}} || \mathrm{AC}]$$

### 5.5.6. *File Retrieval*

The cloud server checks the validity of the authorization contract (AC) once the search request is received. The cloud server starts the search once the user is legitimate, and decryption occurs as follows:

1. The cloud server first checks the UL and inputs the $Q_i$. For every attribute $i \in I$, Test algorithm compute $e(Q_i, P_i) = e\left(g^{a_i s}, g^{t_i \cdot \beta / a_i}\right) = e(g, g)^{s.t_i.\beta} = CT$. The user is allowed to access the dataset search if the equation holds, otherwise the request is cancelled.
2. If the user's attributes satisfy the access structure embedded in the index and the keyword of interest is equal to the stored keyword that is $w' = w$, then the following equation holds $\hat{Q}^{\hat{P}} . \overline{Q_u}? = e\left(\tilde{Q}, \tilde{P}\right) . \prod_{i=1}^{n} e(Q_i, P_i)$
3. After validating the access structure, the cloud server sends the corresponding data $\{E_k(F), \tilde{Q}, {Q_i}', \tilde{C}\}$, shown in Fig. 5.3. as step 4.
4. The requester runs the Decryption algorithm once the data is received and computes k as

$$k = \frac{\tilde{C} . CT}{e(\tilde{Q}, {Q_i}' . \tilde{P})}$$

Finally, the requester decrypts the eMHR $F = D_k(E_k(F))$ and receives the required eMHR F.

*Correctness*:

We now show the correctness of the test algorithm. The cloud server checks whether the secure index $Q$ contains the keywords specified by the trapdoor $P$.

$$\hat{Q}^{\hat{P}}.\overline{Q_u} = Y^{s(\beta+x_u)}.Y_u^{-s} = e(g,g)^{y(s(\beta+x_u))}.e(g,g)^{-y\ u.s}$$

$$= e(g,g)^{y.s.\beta}$$

$$e(\tilde{Q},\tilde{P}).\prod_{i=1}^{n} e(Q_i,P_i) = e(g^s,\widetilde{sk}^{\beta}).\prod_{i=1}^{n} e(A_i^s, {sk_i}^{\beta})$$

$$= e\left(g^s, g^{(y-t)\beta}\right).\prod_{i=1}^{n} e\left(g^{a_i.s}, g^{t_i.\beta/a_i}\right) = e(g,g)^{y.s.\beta}$$

We now show the correctness of the Decryption algorithm. User $u$ can successfully decrypt the symmetric key $k$ using data $(\tilde{Q}, {Q_i}', \tilde{C})$ received from the cloud server.

$$\frac{\tilde{C}.CT}{e(\tilde{Q},{Q_i}'.P_i)} = \frac{k.e(g,g)^{\alpha s}.e(g,g)^{s.t_i.\beta}}{e(g^s, g^{\alpha.a_i}.g^{t_{i.\beta}/a_i})} = \frac{k.e(g,g)^{\alpha s}.e(g,g)^{s.t_i.\beta}}{e(g,g)^{\alpha s}.e(g,g)^{s.t_i.\beta}} = k$$

## 5.6. PERFORMANCE ANALYSIS

This section presents the security analysis, analytical, and simulation-based results for analysing the performance of the proposed secure fog-enabled blockchain framework (SFBF) for next-generation eHealth (NGeH) services in the Abstract: Internet of Things (IoT) environment. The proposed SFBF is compared with the predicate state of the art schemes.

### 5.6.1. Security Analysis

We analyze the security of the proposed SFBF for the healthcare system in this section. We particularly demonstrate that the proposed framework satisfies all the security requirements described in section 5.3.2 and are compared with other eMHR models [77], [79], [96], and [152], as Table 5.2 shows.

**Table 5.2.** Comparative analysis of related solutions and SFBF

| | Techniques used | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| SFBF | Blockchain, CP-ABE, Fog computing | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| [77] | Fog computing, ABE | Yes | No | Yes | Yes | No | No | Yes |
| [79] | Blockchain, ABE | Yes | Yes | Yes | No | No | Yes | Yes |
| [96] | Blockchain, Smart contract | No | No | Yes | No | Yes | Yes | Yes |
| [152] | Blockchain, ECC | Yes | Yes | No | No | Yes | Yes | Yes |

1. Identity privacy, 2. Traceability, 3. Message authentication, 4. Authenticity of search result, 5. Replay attacks, 6. Modification attack, 7. Impersonation attack.

1. *Identity Privacy*: The proposed framework inherits the properties of attribute-based encryption (ABE) and Blockchain. Every eMHR at a local medical supervisor (LMS) or cloud server stores in ciphertext form with encrypted key $k$. An adversary can intercept the communication between the server and user and gain information of $E_k(F), \tilde{C}, \tilde{Q}, \hat{Q}, Q_i$. However, without $sk$ and $\alpha$, the adversary cannot derive $k$. Hence, SFBF meets the requirement of identity privacy.

2. *Traceability*: The trusted authority ($TA$) registers the users using the master secret key $(y, \alpha)$ and assigns a unique secret key $x_u$ to every user in the design of a smart contract framework. Encrypted requests ($requestmsg$) are received at the cloud server when a user requests to access an eMHR. Only the TA knows the owner of *sk* and can identify the real identity of the requester. So, if any user tries to generate malicious requests to disrupt the system, the cloud server sends the malicious activity to the TA, which easily discovers the real identity of the mischievous requester. Therefore, SFBF can achieve the traceability requirement.

3. *Message authentication*: $TA$ checks the authenticity of the received data from users. If the received request is in an authenticated format that is $e(Q_i, P_i) = CT$, only then can the authentication search proceed further. This authentication process is based on the elliptic curve discrete logarithm problem, and no adversary can forge a valid authentication transcript in polynomial time. Therefore, SFBF can support message authentication on the received requests.

4. *Authenticity of the search result:* The cloud server uses access structure to satisfy the index and keyword by computing $\hat{Q}^{\hat{P}}.\overline{Q_f}? = e(\tilde{Q},\tilde{P}).\prod_{i=1}^{n} e(Q_i,P_i)$. This process outputs eMHR corresponding to the required keywords only. Hence, SFBF can achieve the authenticity of search results.

5. *Resistance to cyber attacks*: Our framework is resilient to various cyber attacks, such as replay attacks, modification attacks and impersonation attacks and are described as-
   a) *Replay attacks*: The timestamp $T_{stamp}$, and request identity $req_{ID}$ is included in $requestmsg$. So, TA can easily find the replay attack by checking the freshness of the timestamp $T_{stamp}$ and request identity $req_{ID}$.
   b) *Modification attacks*: The proposed framework uses blockchain to store the data, and transactions are immutable. Therefore, a user can trust the framework with no modification attack.
   c) *Impersonation attacks*: The user generates a trapdoor with secret credential *sk* to access the eMHR; this is communicated by the TA through a dedicated secure channel. Adversaries may try to gain access to an eMHR by forging identities, but they need a secret key. Adversaries cannot forge it in polynomial time because the computation of the secret key depends on discrete log problems that cannot be solved in polynomial time. Hence, no adversary can gain access to the data files, and SFBF can achieve the cyber-attacks requirement.

**Table 5.3.** Computation Cost

| Phases | Computation cost | | |
|---|---|---|---|
| | LFGS | EHRS | SFBF |
| System setup | $(n+1)E+P$ | $3E$ | $nE+2P$ |
| Key generation | $(4n+4)E+4E_1$ | $(3n+3)E$ | $(n+1)E+2E_1$ |
| Encryption | $(n+5)E+P$ | $(4n+1)E+P$ | $nP$ |
| Secure Index generation | $nE+2E_1$ | $4nE$ | $E+(n+1)E_1+P$ |
| Trapdoor generation | $(4n+3)E$ | $(2n+1)E+E_1$ | $(n+1)E$ |
| Search time | $E_1+3nP$ | $5E+nP$ | $E+2np$ |
| Decryption | $(n+3)P$ | $(2n+4)E+2P$ | $E+nP$ |

**Table 5.4.** Communication Cost

| Phases | Communication Cost | | |
|---|---|---|---|
| | LFGS | EHRS | SFBF |
| System setup | - | - | - |
| Key generation | $(3n+4)\|G\|+2\|Z_p\|$ | $(2n+2)\|G\|$ | $2\|G\|+\|Z_p\|$ |
| Encryption | $(n+6)\|G\|+(2n)\|Z_p\|$ | $(2n+3)\|G\|+\|Z_p\|$ | $3\|G\|+(n+1)\|Z_p\|$ |
| Secure Index generation | - | - | - |
| Trapdoor generation | $(2n+3)\|G\|$ | $(2n+3)\|G\|$ | $2n\|G\|+\|Z_p\|$ |
| Search time | $(n+4)\|G\|$ | $\|G\|+\|Z_p\|$ | $3\|G\|+n\|Z_p\|$ |
| Decryption | $(n+7)\|G\|+\|Z_p\|$ | - | - |

## 5.6.2. Analytical and Simulation Results

We perform the theoretical and numerical analysis of SFBF in this section. We analyse the computational cost, communication cost and storage cost with a different number of attributes that are compared with predicate the attribute-based encryption (ABE) schemes LFGS [87] and EHRS [92]. We also simulate the network's average latency and throughput by varying the size of blocks and networks. The ABE operations are performed by using pairing-based cryptography on Ubuntu 16. 04 OS with Intel(R) Core(TM) i7-8700 CPU @3. 20 GHZ and x64-based processor. Furthermore, the Hyperledger network is installed with the Hyperledger-composer V0. 19. 20 using the Yeoman tool [154]. Smart contract performance has also been analysed for various functions. We used type $A$ curve denoted as $\mathrm{E}(\mathrm{F_q})\colon \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{x}$, the group $G$ and group $\mathrm{G_T}$ of order $p$ are subgroups of $\mathrm{E}(\mathrm{F_q})$, where the parameters $p$ and $q$ are equivalent to 160 and 512 bits, respectively.

### 5.6.2.1. Cost Comparison

Tables 5.3 and 5.4 show the computational cost, communication cost and storage cost. The notation $E$ represents group exponentiation, $E_1$ is exponentiation in group $G_1$ and $p$ is bilinear pairing operation. $|G|$ and $|Z_p|$ denote the element length in $G$ and $Z_p$.

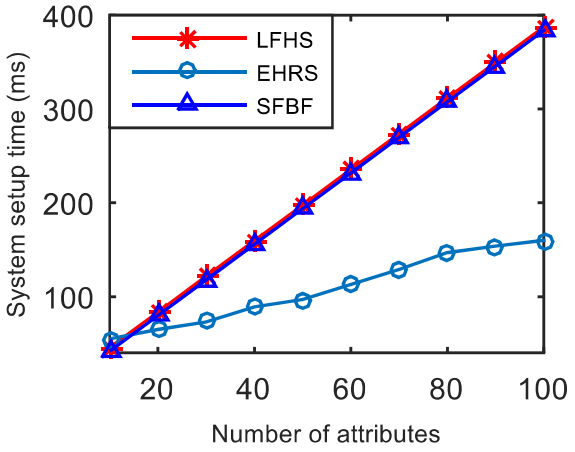



**Figure. 5.4.** System set up time

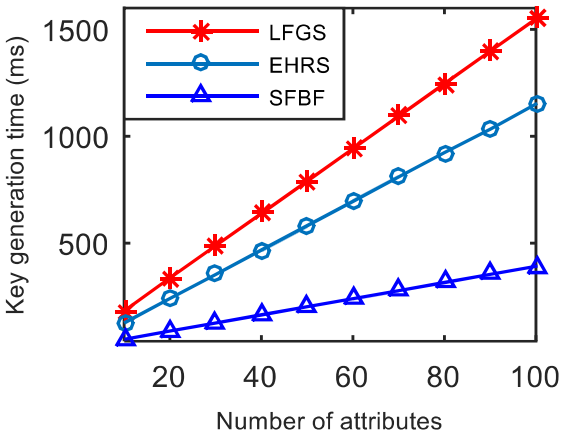



**Figure. 5.5.** Key generation time

The TA initially generates the master secret key (MSK) and public parameters (ABEParams) using the Setup algorithm. The main computation cost in system setup is n exponentiations; Fig. 5.4 shows two pairing operations and comparative simulation results for a different number of attributes. LFGS takes maximum computation time for system setup because it incurs more exponentiation operations as compared to EHRS and SFBF. When a new user joins the system in SFBF, the TA generates a secret key and public key, which takes $(n+1)$ exponentiations operations in group $G$ and two exponentiation operations in group $G1$. SFBF is 74% better than LFGS and 61% better than EHRS, as Fig. 5.5 shows. The reason for less computation cost is because the key generation needs fewer exponentiation operations as compared to other techniques, as given in Table 5.5. Furthermore, data is encrypted to ensure the security of eMHR, and Fig. 5.6 shows the simulation results. It is clear from the figure that SFBF outperforms other techniques; the reason is that it takes only n pairing operations, while LFGS and EHRS need $(n+5)$ and $(4n+1)$ exponentiation operations, respectively. A secure index is generated before outsourcing the encrypted file, and it takes one exponentiation operation and $(n+1)$ exponentiation operation in group $G1$ with one bilinear pairing for SFBF. EHRS is the most expensive in this phase and takes 1520 ms for 100 attributes due to $4n$ exponentiation operations in group $G$ and is shown in Fig. 5.7.

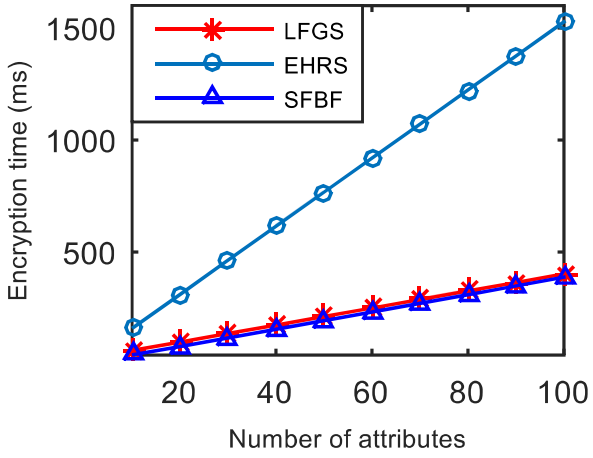



**Figure. 5.6.** Encryption time

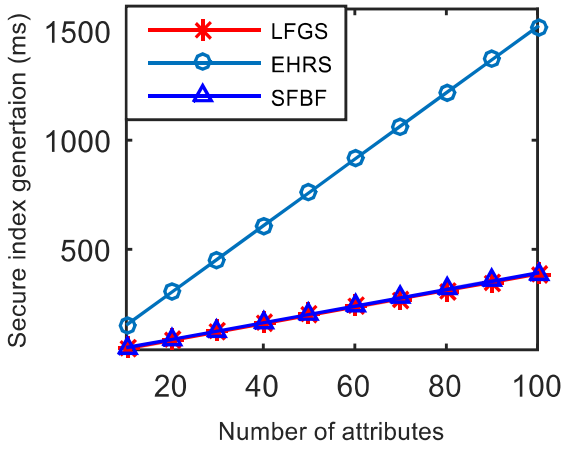



**Figure. 5.7.** Secure index generation time

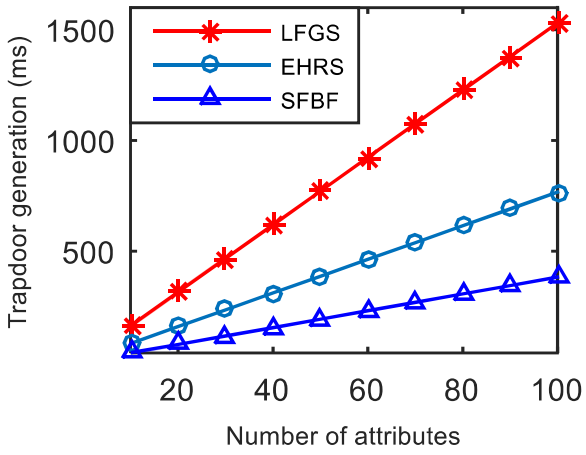



**Figure. 5.8**. Trapdoor generation time

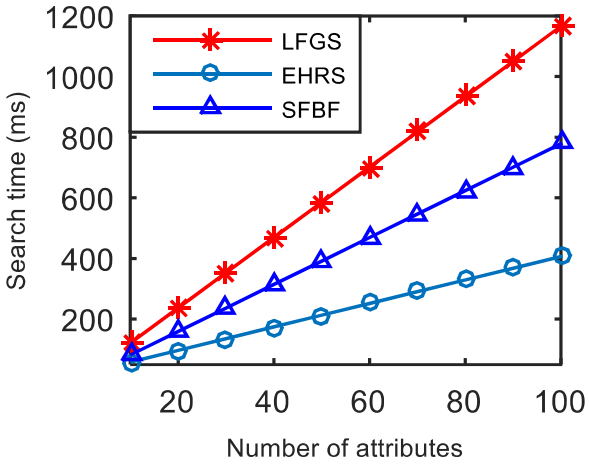



**Figure. 5.9**. Search time

Fig. 5.8 shows trapdoor generation time, and it is clear that SFBF is 74% more efficient than LFGS and 50% more efficient than EHRS. The reason for better performance is that SFBF incurs only $(n+1)$ exponentiation time to generate trapdoor $P$, and it uses smart contracts to generate the trapdoor, which is self-executable code. It helps in the fast execution of the program due to no intervention by a third party. Searching is performed in SFBF on the cloud server instead of the fog server. Searching takes one exponentiation in group $G$ and $2n$ pairing operations; Fig. 5.9 shows the results. LFGS takes 584.90 ms to search in the database for 50 attributes, while SFBF needs 391.20 ms because LFGS needs one exponentiation in group $G1$ and $3n$ bilinear

pairing operations. The graph is linear because all three schemes' search time depends on the number of attributes. After completing the search, cloud server sends the encrypted eMHR $F$ with encrypted key $k$ to the requester, and the user performs the Decryption algorithm with one exponentiation and $n$ bilinear pairings. SFBF is 54% more efficient than EHRS and is shown in Fig. 5.10.

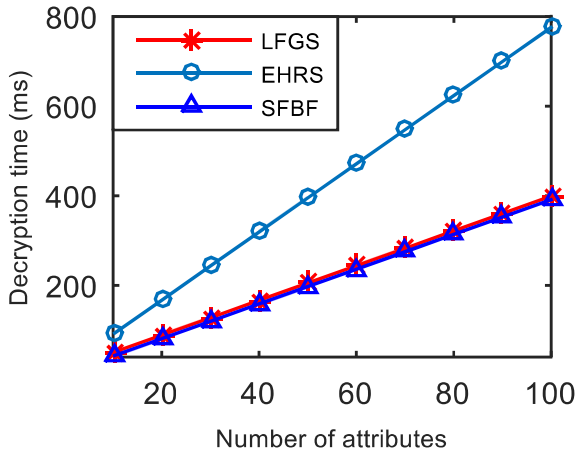



**Figure. 5.10.** Decryption time

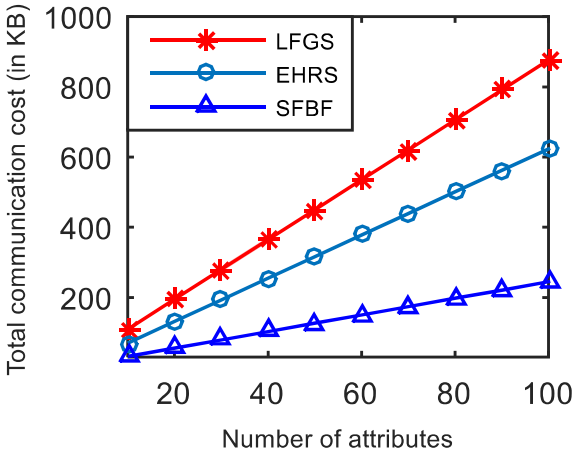



**Figure. 5.11.** Total Communication cost

Fig. 5.11 shows the communication cost. Due to space limitations, we have shown total communication costs instead of phase costs. SFBF takes 32352 ms for 10 attributes and 245472 ms for 100 attributes, which is approximately 72% and 61% better than LFGS and EHRS, respectively. The reason for better performance is that overall SFBF needs fewer operations for communication, and it is clear from the Table 5.4 that SFBF takes $(2n + 8)$ elements of group $|G|$ and $(2n + 3)$ elements of $|Z_p|$.

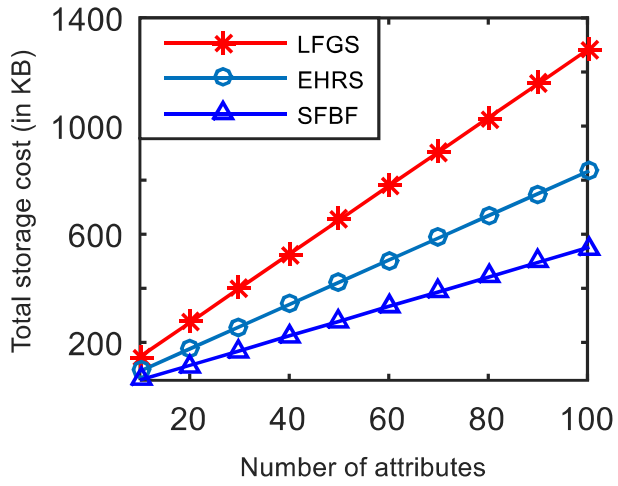



**Figure. 5.12.** Total storage Cost

**Table 5.5.** Storage cost

| Phases | LFGS | EHRS | SFBF |
|---|---|---|---|
| $TA\ (PP)$ | - | - | - |
| $Key\ storage$ | $(3n+9)\|G\|+2\|Z_p\|$ | $(2n+2)\|G\|$ | $(2n+1)\|G\|+2\|Z_p\|$ |
| $Ciphertext$ | $(4n+8)\|G\|+(2n+1)\|Z_p\|$ | $(5n+4)\|G\|+2\|Z_p\|$ | $(n+3)\|G\|+n\|Z_p\|$ |
| $Trapdoor$ | $(4n+1)\|G\|+4\|Z_p\|$ | $(n+4)\|G\|$ | $2n\|G\|+\|Z_p\|$ |
| $Retrieved\ ciphertext$ | $(n+2)\|G\|+\|Z_p\|$ | $2\|G\|+2\|Z_p\|$ | $2\|G\|+n\|Z_p\|$ |

We store various parameters in SFBF, such as master secret key, secret key and public key. As shown in Table 5.5, in total it stores $(5n+6)$ elements of $|G|$ and $(2n+3)$ elements of $|Z_p|$, Fig. 5.12 shows the simulation results. LFGS needs approximately 652160 ms and EHRS needs 422528 ms for 50 attributes, whereas SFBF needs 278624 ms, which is 57% and 34% more efficient than LFGS and EHRS, respectively.

### 5.6.2.2. Blockchain Performance Analysis

The Hyperledger network is installed with the Hyperledger-composer V0.19. 20 using the Yeoman tool [154] To analyse blockchain's performance. The blockchain runs on Ubuntu 16.04 with six cores and up to 3.2 GHz speed. We have used SHA-256 and a block's hash size is 256 bytes. Table 5.6 gives the average execution time for 10 measurements of various smart contracts. We have analysed the average latency and throughput of the system, which are defined here:

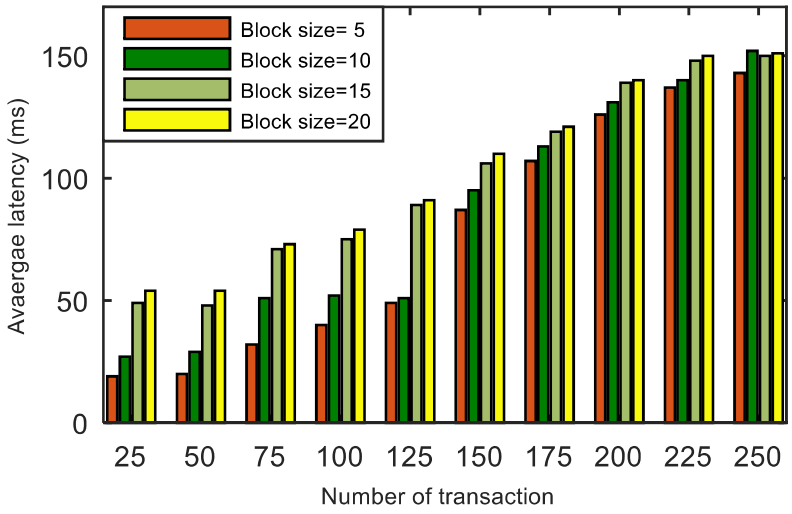
- Average latency: Average latency is the time from when the transaction is submitted to the point when the transaction is available in the network.

  Average Latency = Confirmation time –Submission time of the transaction

- Throughput: This is a parameter to measure the network's efficiency in terms of successful transactions published to the number of transactions submitted.

  Throughput = Successful transactions / (Successful transactions + unsuccessful transactions)

Fig. 5.13(a) shows the average latency in milliseconds for block size 5, 10, 15 and 20 under a number of transactions, where block size means the number of transactions a block holds. For block size 5, 100 transactions are executed in 40 ms, and 200 transactions are performed in 126 ms. Furthermore, block size 20 needs 151 ms to execute 250 transactions. Latency increases gradually as the number of transactions increases. It clearly states that the time to perform more transactions remains approximately constant for the larger block sizes. Thus, storing more transactions in a block can enhance the network's scalability.




(a)

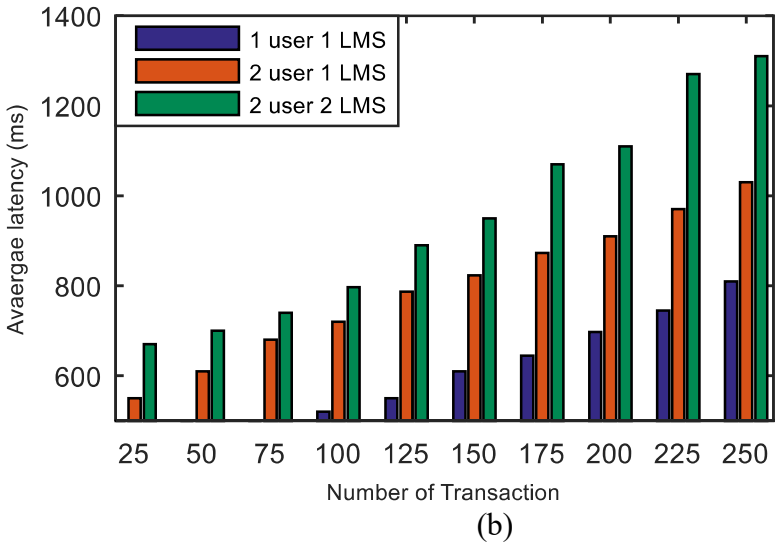



**Figure. 5.13.** Average latency (ms) (a) for block size=5, 10, 15, 20, (b) different network sizes.

The average latency for different network sizes is configured for one user one LMS, two users one LMS and two users two LMSs, shown in Fig. 5.13(b). The figure shows that one user one LMS takes 645 ms for 175 transactions, and it increases linearly to 810 ms for 250 transactions. Two user one LMS takes more time than one user one LMS and needs 720 ms to perform 100 transactions. As the network size increases from one LMS to two LMS, it does not have much impact on the average latency of the network. Two users one LMS takes 823 ms to perform 200 transactions, and two users two LMS needs 950 ms. Hence, in SFBF as the network expands and more patients join the network, latency is not greatly impacted as more LMSs also join the network and perform the blockchain operations. Therefore, this network is flexible and can be used for low computing devices.

**Table 5.6.** The average execution time of various smart contract functions

| *Functions* | *Time (ms)* |
|---|---|
| Authorization | 101.5 |
| Update | 77.55 |
| DataEncryption | 54.29 |
| MonitoringandAlertGeneration | 31.09 |
| GenerateRequest | 24.12 |

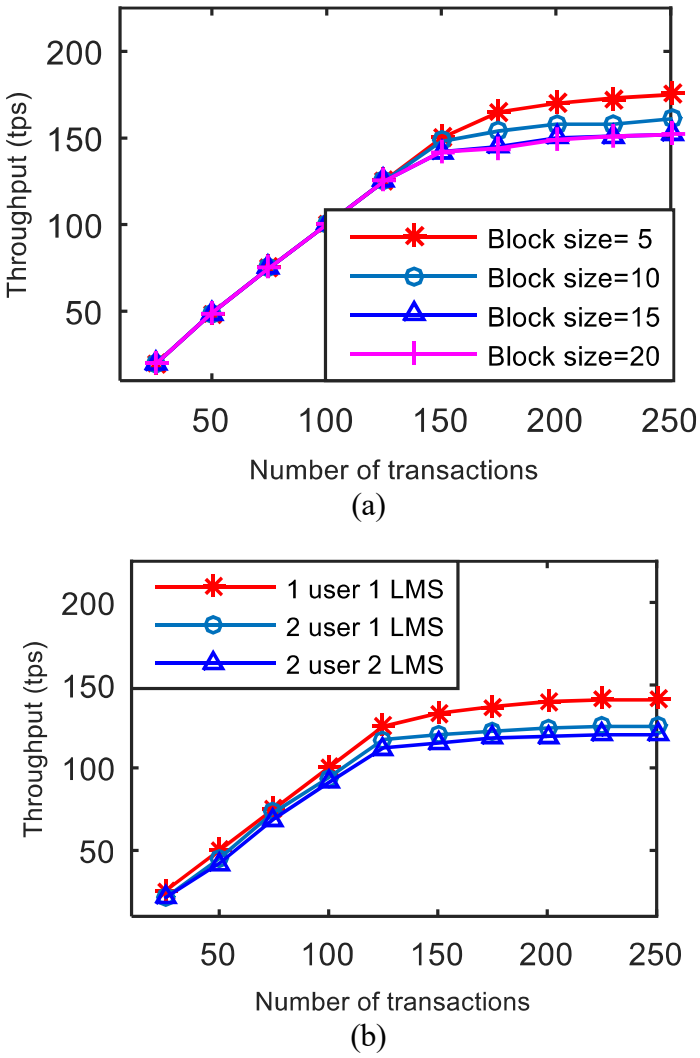



**Figure. 5.14.** Throughput (tps) vs number of transactions (a) for different block sizes, (b) For different network sizes.

Fig. 5.14 shows the throughput of the network for a different number of transactions, such as 50, 100, 150, 200 and 250. We have considered one user one LMS network for computation of throughput for block sizes 5, 10, 15 and 20, and Table 5.7 gives more parameter details. It is clear from Fig. 5.14(a) that, up to 150 transactions, all the block sizes have approximately the same throughput. For block size 5, the network can perform 165transactions successfully out of 175 transactions. For block size 20, the system performs 151 transactions out of 250 transactions, and block size 15 performs 152 transactions. Block size 20 and 15 have approximately the same

throughput. SFBF achieves marginally lower throughput on a larger block size as compared to a smaller block size, and it can be ignored to achieve scalability in the network.

**Table 5.7.** Parameter consider for simulation of blockchain

| Parameter | Value |
|---|---|
| Number of attributes | 5 |
| Protocol | PBFT |
| Transaction size | 256 bytes |
| 1LMS area | $500 \times 500m^2$ |
| Communication range | 100 m |
| Hop limit | 3 |

Fig. 5.14(b) shows the throughput of different network sizes. It is clear from the figure that maximum throughput is attained by one user one LMS due to lower computation overhead and communication cost. However, the throughput of two users one LMS and two users two LMS are approximately the same. Thus, the extension of the network does not greatly affect the overall performance. Such performance is achieved because we have use a fog server (LMS) to perform the task of blockchain instead of end users who are patients. After experimentation, it is observed that throughput and latency are inversely proportional. We can say that a lower number of transactions have better throughput with lower block sizes and a higher number of transactions have better throughput with higher block size.

## 5.7. SUMMARY

We have presented in this chapter a secure fog-enabled blockchain framework (SFBF) for next-generation eHealth (NGeH) services in the Internet of Things (IoT) environment, focusing on real-time, remote monitoring of patients and access control of electronic medical health records (eMHRs). Three smart contracts have been designed to maintain the users' profiles, eMHRs, emergency response, and access control. Blockchain and CP-ABKS work in tandem in this framework and provide the advantages of both techniques. Security analysis has been presented to prove the robustness of SFBF against cyber-attacks. SFBF's performance is analysed based on computation, communication and storage costs. The obtained results indicate the better performance of SFBF with a different number of attributes. Furthermore, blockchain performance

is analysed for throughput and latency with different network and block sizes. The outcome of the simulation results shows that latency is almost the same for different block sizes; thus, increasing the number of transactions can provide real-time response. Additionally, results show that latency and throughput are inversely proportional and can enhance the network's scalability.

# Chapter 6

# Conclusion and Future work

In this chapter, detailed analysis and evaluation of the secure and energy efficient protocols which have been suggested in the thesis are summarized. Summary of the analysis that address the prominent issues of IoT security threat, scalability, energy efficiency, privacy and authentication have been delineated. Further, future work for the problems mentioned in the thesis has been described in this chapter as well.

## 6.1. Conclusion

Various issues and applications of IoT have been discussed in brief in the first chapter and literature survey of work proposed by contemporary authors is followed in second chapter. Security protocols of IoT for trust management, privacy, scalability, and data sharing have been delineated to provide motivation for the improvement in security and energy efficiency for IoT networks.

IoT nodes remain vulnerable to variety of attacks due to their deployment in open and remote environment. In such environment internal attacks are more vulnerable than external attacks. Trust computation is one of the prominent way to deal with internal attacks such as bad mouthing attack. The accuracy of the trust between the nodes rely on the recommendations of nodes' neighbor. The nodes with low bandwidth and limited battery power do not incorporate with the performance of trust model. To improve the energy usage due to unnecessary transmission during the trust calculation process energy efficient trust evaluation (EETE) scheme is designed based on game theory. To achieve the aim, three dilemma games are designed to maintain the trust of the individual nodes and to mitigate the malicious activity. First dilemma game decides whether node should be a cluster head or cluster member to promote a balanced cluster formation. Second dilemma game is used to affirm the minimum number of trust recommendations for maintaining the balance of the trust in a cluster. Third dilemma game is an activity based trust management which helps in

mitigation of malicious activity. This game uses Nash equilibrium to choose best strategy for a cluster head to launch its anomaly detection technique which maximizes the network output and minimizes the effect of an attack. Through experimental results the performance of the EETE is comparatively analyzed with state-of-the-art such as TDDG, HIDS, CWSN, and LHIDS. Analysis is done on the different matrices such as detection rate, average energy consumption, trust evaluation time, detection time and saddle point. The simulation is performed on NS-3. The simulation results show that EETE outperforms the stare-of-the-art protocols.

Information security is another critical aspect of smart networks as all the decisions depends on the accuracy and credibility of the received data. Several signature schemes have been proposed to secure the data. Such schemes depends on solving mathematical problems such as integer factorization and discrete logarithms. These problems are infeasible to solve on classical computer. However, these problems can be solved easily by quantum computers in polynomial time. In this context, a lightweight post-quantum ID-based signature (LPQS) scheme based on supersingular isogeny curve for secure data transmission in IoT environment is designed. It is a post quantum signature scheme that reduces the complexity of the system with fewer system resources consumption. The protocol works in four phases including initialization, registration, signature and validation. For the initialization of the protocol, identity of the client is used and two isogeny curve for verification is also used which provides double-fold secure encryption. Unforgeability of LPQS under an adaptively chosen message attack is also proved. Through theoretical security analysis, resistance of LPQS has been proven against various cyber-attacks and comparative analysis with contemporary models is also performed. Through experimental results comparative analysis with state-of-the-art protocols on different matrices such as message size, energy consumption and total execution time.

IoT plays a pivotal role in shaping personalized services such as healthcare system. Such systems include smart use cases of context-aware sensor networks to gather information related to patient's activities and patient's surrounding environment to collect vital information such as blood pressure and cardiac index from a patient's body. Data of patients'

can be accessed remotely which raises issues of privacy, accuracy and scalability. It is essential to preserve confidentiality and prevent unauthorized access of sensitive electronic health records. To handle such problem a fog-based blockchain framework for eHealth services (SFBF) is designed based on attribute-based keyword search (ABKS) and blockchain. In this protocol, three smart contracts including authorization contract, emergency service contract and access control contract have been designed to streamline complex medical workflows and to ensure proper handling of electronic health records. This protocol provides secure remote health-care monitoring and access control mechanism for electronic health records based on smart contracts and ABKS. The proposed protocol is demonstrated for different security parameters such as identity privacy, traceability, message authentication and modification attack and comparative analysis is performed with the contemporary protocols. It is clear from the security analysis that the proposed protocol satisfies all the parameters. Simulation of SFBF is performed on Hyperledger-composer V0.19.20 with the Yeoman tool and performance of the protocol is measured on different matrices such as cost computation, average latency, and throughput. Comparative analysis with different state-of-the-art models shows that SFBF outperforms the contemporary protocols.

## 6.2. Discussion

In this work, analytical and simulation work is carried out through mathematical expression and network simulation techniques. The proposed protocols in this thesis are executed on NS-3, Microsoft Visual Studio, Hyperledger-composer V0.19.20 and MATLAB 2013b/2015b. After analyzing the results obtained from the simulation, we observed the following:

- It is observed that detection rate of malicious nodes of contemporary models have been drastically fall below 93% when the number of malicious nodes are 40%. Nash equilibrium strategy finds the optimal settings using the activity based trust dilemma game and classifies the nodes in three categories: Trust, Suspicious and Malicious according to their behavior in the network and improves the detection rate. EETE also removes the malicious nodes from the network who performs illegitimate for longer duration of time. This helps in reduction of malicious activity in the network.

- Energy consumption and average trust evaluation time of EETE is observed when the number of nodes vary from 2 to 20. Energy consumption of state-of-the-art models is approximately 5 times higher than EETE. This reduction comes due to the dilemma games which helps in selection of cluster heads and cluster members. It optimizes the cluster functionality that omit the unnecessary communication packets. Therefore, the overhead of trust calculation is reduced and it helps in better energy consumption.
- It is observed that we cannot avoid the situation of an attack but we can minimize the impact of the attack on the network. Such equilibrium state is obtained after a trade-off between detection rate and energy consumption and it is known as Saddle-trust equilibrium. In this model, neither the attacker gains too much of the network nor the luster head losses too much over the network.
- Public key size, private key size and signature size of LPQS is less than the proposed state-of-the-art models which are based on lattice, Multivariate, and Hash. The reason for better key sizes is the use of Isogeny curves which reduces the overhead of computation and communication.
- LPQS consumes less energy and fewer CPU cycles as compared to the contemporary models such as SPHINCS and Rainbow. The reason for better performance is the usage of two isogeny curves instead of one, which takes the previously computed values for the second verification.
- Theoretical analysis of SFBF for computational, communication, and storage cost is performed and comparatively analyzed with state-of-the-art protocols such as LFGS and EHRS. Analysis shows that proposed SFBF outperforms other models and the reason for better performance is the use of attribute based encryption which consumes less number of operations in overall execution of the protocol. Phases of the models such as key generation, encryption, secure index, trapdoor generation, and decryption takes less time as compared to the state-of-the-art models and provide better health record search mechanism.
- Average latency and throughput of SFBF is analyzed for block sizes 5 to 20 and number of transactions 25 to 250. It is observed that as the number of transactions increases, latency increases gradually and the time to perform more transactions

remains approximately constant for the larger block sizes. Thus, storing more transactions in a block enhances the network's scalability.

## 6.3. Future work

In this thesis, we achieve number of objectives by designing various secure and energy efficient protocols for IoT. However, in a research work there is always scope for further enhancement. Hence, different adaptations, tests and experiments can be performed to enhance the performance of the model or for deeper analysis of particular mechanisms in the following manner:

- In future work, authors can improve the detection rate of different external attacks like denial of service (DOS), black-hole and wormhole attack.
- Further, information security can be included in the system with the aim to maintain the privacy of the users.
- In future research, authors can extend the proposed scheme by investigating how to represent the elliptic curves efficiently and use the three-party id-based signature scheme based on the supersingular isogeny curve.
- Post-Quantum cryptography is in an infancy state. Implementation of the proposed scheme in a real environment can provide could provide new issues of the deployment.
- In future research, supersingular isogeny curves can be used to improve the key agreement protocols.
- Further, a session-based, client-centric data sharing scheme to improve the security, integrity and privacy preserving can be designed. The flexibility of the search mechanism by updating the attribute keyword keys can be incorporated in the scheme.
- Incentive based framework can be designed which will motivate patients to share their health records for other patients' diagnosis and for research purpose also by payment through cryptocurrency.

## References


[1] S. Balaji, Karan Nathani, and R. Santhakumar, "IoT technology, applications and challenges: a contemporary survey", *Wireless personal communications,* vol.108, no.1, pp.363-388, 2019.

[2] J. Cubo, A. Nieto, and E. Pimentel, "A cloud-based Internet of Things platform for ambient assisted living", *Sensors*, Vol. 14, no. 8, pp. 14070-14105, 2014.

[3] H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN-and IOT-based smart homes and their extension to smart buildings". *Sensors*, Vol. 15, no. 5, pp. 10350-10379, 2015.

[4] B. Ali, and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes", *Sensors*, vol. *18, no. 3*, p. 817, 2018.

[5] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges", *IEEE Communications Magazine*, vol. *55, no.* 9, pp.16-24, 2017.

[6] L. Zhao, J. Wang, J. Liu, and N. Kato, "Optimal edge resource allocation in IoT-based smart cities", *IEEE Network*, vol. *33, no.* 2, pp. 30-35, 2019.

[7] M. Chen, J. Yang, L. Hu, M. S. Hossain, and G. Muhammad, "Urban healthcare big data system based on crowdsourced and cloud-based air quality indicators", *IEEE Communications Magazine*, vol. *56, no.* 11, pp. 14-20, 2018.

[8] M. R. Ramli, P. T. Daely, D. S. Kim, and J.M. Lee, "IoT-based adaptive network mechanism for reliable smart farm system", *Computers and Electronics in Agriculture*, vol. *170*, p.105287, 2020.

[9] A.K. Podder, A. Al Bukhari, S. Islam, S. Mia, M. A. Mohammed, N. M. Kumar, and K. H. Abdulkareem, "IoT based smart agrotech system for verification of Urban farming parameters", *Microprocessors and Microsystems*, vol. *82*, p. 104025, 2021.

[10] T. M. Fernández-Caramés, and P. Fraga-Lamas, "Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles", *Electronics*, vol. *7, no.* 12, p. 405, 2018.

[11] S. Chen, H. Wen, J. Wu, W. Lei, W. Hou, W. Liu, and Y. Jiang, "Internet of things based smart grids supported by intelligent edge computing", *IEEE Access*, vol. *7*, pp. 74089-74102, 2019.

[12] K. Siozios, D. Anagnostos, D. Soudris, and E. Kosmatopoulos, "IoT for smart grid*s"*, *Springer*, pp. 1-282, 2019.

[13] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial internet of things based on private blockchain", *IEEE Network*, vol. *34, no.* 5, pp. 78-83, 2020.

[14] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in SDN-based industrial Internet of Things with edge computing," *IEEE Internet of Things Journal*, vol. *5, no.* 3, pp. 1351-1360, 2018.

[15] Y. Jeong, S. Son, E. Jeong, and B. Lee, "An integrated self-diagnosis system for an autonomous vehicle based on an IoT gateway and deep learning", *Applied Sciences*, vol. *8, no.* 7, p. 1164, 2018.

[16] J. Xu, Z. Hu, Z. Zou, J. Zou, X. Hu, L. Liu, and L. Zheng, "Design of smart unstaffed retail shop based on iot and artificial Intelligence", *IEEE Access*, vol. *8*, pp. 147728-147737, 2020.

[17] M. Abdel-Basset, G. Manogaran, and M. Mohamed, "Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems", *Future Generation Computer Systems*, vol. *86*, pp. 614-628, 2018.

[18] L. A. Grieco, A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. D. Paola, and G. Boggia, "IoT-aided robotics applications: Technological implications, target domains and open issues", *Computer Communication*, vol. 54, pp. 32-47, 2014.

[19] A. Aijaz, and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective", *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103-112, 2015.

[20] Y,B. Lin, "EasyConnect: A Management System for IoT Devices and Its Applications for Interactive Design and Art", *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 551-561, 2015.

[21] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[22] Hamed Hellaoui, Mouloud Koudil, Abdelmadjid Bouabdallah, "Energy-efficient mechanisms in security of the internet of things: A survey", *Computer Networks*, vol. 127, pp. 173-189, 2017.

[23] N. Kaur, and S.K. Sood, "An Energy-Efficient Architecture for the Internet of Things (IoT)", *IEEE Systems Journal*, vol. 11, no. 2, pp. 796-805, 2017.

[24] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of Internet of Things communication using ICN: A use case perspective", *Computer Communications,* vol. 142–143, 2019, pp. 95-123, 2019. https://doi.org/10.1016/j.comcom.2019.05.010.

[25] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[26] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks", *Journal of Information Security and Applications*, vol. 38, pp. 8-27, 2018.

[27] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S.A. Maisto, S. Nacchia, "Internet of things reference architectures, security and interoperability: A survey", *Internet of Things*, vol. 1–2, pp. 99-112, 2018.

[28] R. Minerva, A. Biru and D. Rotondi, "Towards a definition of the Internet of Things (IoT)", *IEEE Internet of Things Journal,* no.1, pp.1-86, May, 2015.

[29] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[30] A. Aijaz, and A. H. Aghvami, “Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective”, *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103-112, 2015.

[31] Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”, *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[32] W. Kassab, and K. A. Darabkh, “A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations”, *Journal of Network and Computer*, vol.163, 2020. https://doi.org/10.1016/j.jnca.2020.102663.

[33] Feng, Renjian, et al. "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory" *Sensors*, vol.11, no. 2, pp.1345-1360, 2011.

[34] Li, Jing-tao, et al. “A trust model based on similarity-weighted recommendation for P 2 P environments” *Ruan Jian Xue Bao(Journal of Software),* vol. 18, no.1, pp. 157-167, 2007.

[35] Piro, Giuseppe, Gennaro Boggia, and Luigi Alfredo Grieco “A standard compliant security framework for ieee 802.15. 4 networks" Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 2014.

[36] Jiang, Hai, et al “A secure and scalable storage system for aggregate data in IoT”, *Future Generation Computer Systems*, vol. 49, pp. 133-141, 2015.

[37] Khan, Muhammad Saleem, et al. “Isolating Misbehaving Nodes in MANETs with an Adaptive Trust Threshold Strategy”, *Mobile Networks and Applications,* vol. 22, no. 3, pp. 493-509, 2017.

[38] Zhou, Peng, et al. “Toward energy-efficient trust system through watchdog optimization for WSNs” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613-625, 2015.

[39] Yu, Yang, et al. “An efficient trust evaluation scheme for node behavior detection in the internet of things”, *Wireless Personal Communications*, vol. 93, no. 2, pp. 571-587, 2017.

[40] Duan, Junqi, et al. “TSRF: A trust-aware secure routing framework in wireless sensor networks”, *International Journal of Distributed Sensor Networks*, vol. 10, no.1, pp. 209436, 2014.

[41] Ahmed, Adnan, et al. “TERP: A trust and energy aware routing protocol for wireless sensor network”, *IEEE Sensors Journal*, vol. 15, no.12, pp. 6962-6972, 2015.

[42] Reddy, Vijender Busi, Sarma Venkataraman, and Atul Negi, “Communication and data trust for wireless sensor networks using D–S theory”, *IEEE Sensors Journal*, vol. 17, no.12 pp. 3921-3929, 2017.

[43] Xu, Lina, Gregory MP O’Hare, and Rem Collier “A smart and balanced energy-efficient multihop clustering algorithm (smart-beem) for mimo iot systems in future networks” *Sensors,* vol. 17, no.7, pp. 1574, 2017.

[44] Tang, Jine, et al. “An energy efficient hierarchical clustering index tree for facilitating time-correlated region queries in the Internet of Things”, *Journal of Network and Computer Applications*, vol. 40, pp. 1-11, 2014.

[45] F. Bao, I. R. Chen, M. Chang, and J. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection”, *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[46] Lu, Huang, Jie Li, and Mohsen Guizani “Secure and efficient data transmission for cluster-based wireless sensor networks”, *IEEE transactions on parallel and distributed systems*, vol. 25, no. 3, pp.750-761, 2014.

[47] Li, Xiaoyong, Feng Zhou, and Junping Du “LDTS: A lightweight and dependable trust system for clustered wireless sensor networks”, *IEEE transactions on information forensics and security*, vol. 8, no. 6, pp. 924-935, 2013.

[48] Shabut, Antesar M., et al. “Recommendation based trust model with an effective defence scheme for MANETs” *IEEE Transactions on Mobile Computing,* vol. 14, no. 10, pp. 2101-2115, 2015.

[49] Talbi, Said, et al. “Adaptive and dual data-communication trust scheme for clustered wireless sensor networks” *Telecommunication Systems*, vol. 65, no. 4, pp. 605-619, 2017.

[50] Kamhoua, Charles A., Niki Pissinou, and Kia Makki “Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy”, Communications (ICC), 2011 IEEE International Conference on. IEEE, 2011.

[51] Fang, He, Li Xu, and Xinyi Huang “Self-adaptive trust management based on game theory in fuzzy large-scale networks”, *Soft Computing* vol. 21, no. 4, pp. 907-921, 2017.

[52] Duan, Junqi, et al “An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications”, *IEEE Internet of Things Journal*, vol 1, no. 1, pp. 58-69, 2014.

[53] Chen, Zhenguo, Liqin Tian, and Chuang Lin “Trust model of wireless sensor networks and its application in data fusion”, *Sensors,* vol. 17, no. 4, pp.703, 2017.

[54] De Feo, L.; Jao, D.; Plût, J. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”, In *Proceedings of the International Workshop on Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, pp. 19–34, 2011.

[55] De Feo, L.; Jao, D.; Plût, J. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”, *J. Math. Cryptol.*, vol. *8*, pp. 209–247, 2014.

[56] Costello, C.; Longa, P.; Naehrig, M. “Efficient Algorithms for Supersingular Isogeny Diffie-Hellman”, In Proceedings of the Advances in Cryptology | CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Springer: Berlin/Heidelberg, Germany, pp. 572–601, 2016.

[57] Galbraith, S.D.; Petit, C.; Silva, J. Identification protocols and signature schemes based on supersingular isogeny problems. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–33.

[58] Adi, S. "Identity-based cryptosystems and signature schemes", In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1984.

[59] Vélu, J. "Isogénies entre courbes elliptiques", In *Comptes Rendus de l'Académie des Sciences de, C.R. Acad. Sci.*; Elsevier of behalf of the French Academy of Sciences (France): Paris, France, vol. 273, pp. 238–241, 1971.

[60] Malasri, K.; Wang, L. "Addressing Security in Medical Sensor Networks", In *Proceedings of the ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments (HealthNet'07)*; Association for Computing Machinery: New York, NY, USA,; pp. 7–12, 2007.

[61] Oliveira, L.B.; Aranha, D.; Morais, E.; Daguano, F.; Lopez, J.; Dahab, R. TinyTate. In Proceeding of the Identity-Based Encryption for Sensor Networks, White Plains, NY, USA, 19–23 March, 2007.

[62] C. C. Tan, H. Wang, S. Zhong, Q. Li, "Body Sensor Network Security: An Identity-Based cryptography Approach", In Proceedings of the ACM Conference on Wireless Security, Alexandria, VA, USA, 31 March–2 April 2008; pp. 148–153, 2008.

[63] S. Sankaran, M. I. Husain, R. Sridhar, "IDKEYMAN: An identity-based key management scheme for wireless ad hoc body area networks", In Proceedings of the 5th Annual Symposium on Information Assurance (ASIA'09), Buffalo, NY, USA, 3–4 June 2009.

[64] F. Miao, L. Jiang, Y. Li, Y. Zhang, "AES based biometrics security solution for body area sensor networks", *Bull. Adv. Technol. Res.,* vol. 3, pp. 37-41, 2009.

[65] C. Ma, K. Xue, P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks", *Secur. Commun. Netw.,* vol. 7, pp. 759-773, 2014.

[66] X. Sun, H. Tian, and Y. Wang, "Toward Quantum-Resistant Strong Designated Verifier Signature from Isogenies", *2012 Fourth Int. Conf. Intelligent Netw. Collab. Syst.*, vol. *5*, pp. 292–296, 2012.

[67] P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, "Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU", Available online: https://www.di.ens.fr/~{}prest/Publications/falcon.pdf (accessed on 10 December 2020).

[68] A. Casanova, J. C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, "GeMSS: A Great Multivariate Short Signature", Ph.D. Thesis, UPMC-Paris 6. Sorbonne Universités, Paris, France, 2017.

[69] A. Petzoldt, M. S. Chen, J. Ding, B. Y. Yang, "HMFEv-an efficient multivariate signature scheme", In Proceedings of the International Workshop on Post-Quantum Cryptography, Utrecht, The Netherlands, 26–28 June 2017; Springer: Berlin/Heidelberg, Germany; pp. 205–223, 2017.

[70] J. Ding, A. Petzoldt, "Current State of Multivariate Cryptography", *IEEE Secur. Priv. Mag.*,vol. *15*, pp. 28–36, 2017.

[71] A. Childs, D. Jao, V. Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time", *J. Math. Cryptol.* vol. *8*, pp. 1–29, 2014.

[72] K. A. Shim, C.M. Park, N. Koo, and H. Seo, "A High-Speed Public-Key Signature Scheme for 8-b IoT-Constrained Devices", *IEEE Internet Things J.* vol. *7*, pp. 3663–3677, 2020.

[73] L. De Feo, and S. D. Galbraith, "SeaSign: Compact isogeny signatures from class group actions" In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 19–23 May 2019; Springer: Cham, Switzerland, 2019; pp. 759–789, 2019.

[74] L. Parrilla, E. Castillo, J.A. López-Ramos, J.A. Álvarez-Bermejo, A. García, " Morales, D.P. Unified compact ECC-AES co- processor with group-key support for IoT devices in wireless sensor networks", *Sensors,* vol. 18, p. 251, 2018.

[75] M. S., Hussein, J. A. L. Ramos, and J.A. Álvarez-Bermejo, "Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro", *Sensors,* vol.20, p. 2242, 2020.

[76] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos and S. W. Kim, "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies", *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1121-1167, Second quarter 2020.

[77] Y. Zhang, M. Qiu, C. Tsai, M. M. Hassan and A. Alamri, "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88-95, March 2017.

[78] B. Xu, L. Da Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Transactions on Industrial informatics,* vol. 10, no. 2, pp. 1578-1586, 2014.

[79] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: a personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258-32285, 2018.

[80] R. Mehmood, and G. Graham, "Big data logistics: a health-care transport capacity sharing model," *Procedia computer science,* vol. 64, pp. 1107-1114, 2015.

[81] M. Al-Khafajiy, H. Kolivand, T. Baker, D. Tully and A. Waraich, "Smart hospital emergency system," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 20087-20111, 2019.

[82] Y. Miao, J. Ma, X. Liu, Q. Jiang, J. Zhang, L. Shen and Z. Liu, "VCKSM: Verifiable conjunctive keyword search over mobile e-health cloud in shared multi-owner settings," *Pervasive and Mobile Computing*, vol. 40, pp. 205-219, 2017.

[83] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, K. K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-healthcare clouds," *Journal of medical systems*, vol. 40, no. 11, pp. 235, 2016.

[84] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system," *IEEE Access*, vol. 7, pp. 88012-88025, 2019.

[85] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, and XS Shen, "Fine-grained data access control with attribute-hiding policy for cloud-based IoT," *Computer Networks*, vol. 153, pp. 1-10, 2019.

[86] Y. Zhao, P. Fan, H. Cai, Z. Qin and H. Xiong, "Attribute-based Encryption with Non-Monotonic Access Structures Supporting Fine-Grained Attribute Revocation in M-healthcare," *IJ Network Security*, vol. 19, no. 6, pp. 1044-1052, 2017.

[87] Y. Miao, J. Ma, X. Liu, J. weng, H. Li and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 772-785, 2018.

[88] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," *IEEE Access*, vol. 7, pp. 33202-33213, 2019.

[89] H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, "Secure fine-grained encrypted keyword search for e-healthcare cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1307-1319, 2019.

[90] X. Chen, Y. Liu, HC Chao, and Y. Li, "Ciphertext-Policy Hierarchical Attribute-Based Encryption against Key-Delegation Abuse for IoT-connected Healthcare System," *IEEE Access*, vol. 8, pp. 86630-86650, 2020.

[91] H. Wang, and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of medical systems*, vol. 42, no. 8, pp. 152, 2018.

[92] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic health record sharing scheme with searchable attribute-based encryption on blockchain," *IEEE Access*, vol. 8, pp. 7195-7204, 2019.

[93] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE access*, vol. 6, pp. 11676-11686, 2018.

[94] Y. Zhang, D. He, and KKR Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[95] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE access*, vol. 7, pp. 66792-66806, 2019.

[96] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices," *Applied Sciences*, vol. 10, no. 2, p. 488, 2020.

[97] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of things: Energy oriented path and message scheduling approach", *Sustainable Cities and Society*, 38, pp.195-204, 2018.

[98] O. Kaiwartya *et al*., "Virtualization in Wireless Sensor Networks: Fault Tolerant Embedding for Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 571-580, April 2018.

[99] K. Kumar, S. Kumar , O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-Layer Energy Optimization for IoT Environments: Technical Advances and Opportunities:, *Energies,* vol. 10, no. 12, p. 2073, 2017.

[100] S. Kumar, U. Dohare, K. Kumar, D. Prasad, K. N. Qureshi and R. Kharel, "Cybersecurity Measures for Geocasting in Vehicular Cyber Physical System Environments," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5916-5926, 2018. doi:10.1109/JIOT.2018.2872474.

[101] Aanchal, S. Kumar, O. Kaiwartya, "Green computing for wireless sensor networks: Optimization and Huffman coding approach", *Peer-to-Peer Netw. Appl*, vol. 10, issue 3, pp 592–609, 2017.

[102] U. Dohare, D. K. Lobiyal, and S. Kumar, "Energy balanced model for lifetime maximization in randomly distributed wireless sensor networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 407–428, 2014.

[103] D. K. Sheet, O. Kaiwartya, A.H. Abdullah, Y. Cao, A. N. Hassan, and S. Kumar, "Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks", *IET Intelligent Transport Systems*, vol. 11, no. 2, pp.53-60, 2016.

[104] R. Rani, and C. P. Katti, "End-to-End Security in Delay Tolerant Mobile Social Network", *International Conference on Application of Computing and Communication Technologies*, Springer, Singapore, pp. 45-54, 2018.

[105] Ishaq, Zeba, Seongjin Park, and Younghwan Yoo "A security framework for Cluster-based Wireless Sensor Networks against the selfishness problem", 2015 Seventh International Conference on Ubiquitous and Future Networks. IEEE, pp. 7-12, 2015.

[106] G. Theodorakopoulos and J. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun*., vol. 24, no. 2, pp. 318–328, Feb. 2006.

[107] Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," *Proc. IEEE INFOCOM*, pp. 1–9, 2010.

[108] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169-183, 2012.

[109] P. Kasirajan, C. Larsen, and S. Jagannathan, "A new data aggregation scheme via adaptive compression for wireless sensor networks," *ACM Trans. Sensor Netw*., vol. 9, no. 1, pp. 1–5, 2012.

[110] Fang, Weidong, et al. "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks", *Journal of Network and Computer Applications*, vol. 59, pp. 88-94, 2016.

[111] Li, Jing-tao, et al. "A trust model based on similarity-weighted recommendation for P 2 P environments", *Ruan Jian Xue Bao(Journal of Software,* vol. 18, no. 1, pp. 157-167, 2007.

[112] Lopez, Javier, et al. "Trust management systems for wireless sensor networks: Best practices", *Computer Communications*, vol. 33, no.9, pp. 1086-1093, 2010.

[113] Yu, Yanli, et al. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867-880, 2012.

[114] Yan, K. Q., et al "Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network", *Computer Science and Information Technology (ICCSIT)*, 2010 3rd IEEE International Conference on. vol. 1. IEEE, 2010.

[115] Wang, Shun-Sheng, et al. "An integrated intrusion detection system for cluster-based wireless sensor networks", *Expert Systems with Applications*, vol. 38, no. 12, pp. 15234-15243, 2011.

[116] Sedjelmaci, Hichem, Sidi Mohamed Senouci, and Tarik Taleb "An accurate security game for low-resource IoT devices", *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381-9393, 2012.

[117] L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa, and M. Abdulsalam, "A concise review on Internet of Things (IoT)-problems, challenges and opportunities," In Proceedings of the 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), Budapest, Hungary, 18–20 July 2018; pp. 1–6, 2018.

[118] A. U. Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M. R. Ahmed, and O. Kaiwartya, A. James-Taylor, "Toward a Heterogeneous Mist, Fog, and Cloud-Based

Framework for the Internet of Healthcare Things", *IEEE Internet Things J.*, vol. *6*, pp. 4049–4062, 2019.

[119] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, H. Zhou, "Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach", *IEEE Access,* vol. *7*, pp. 113311–113323, 2019.

[120] G. K. Verma, B. B. Singh, N. Kumar, O. Kaiwartya, M. S. Obaidat, "PFCBAS: Pairing Free and Provable Certificate-Based Aggregate Signature Scheme for the e-Healthcare Monitoring System", *IEEE Syst. J,* vol. *14*, pp. 1704–1715, 2019.

[121] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, R. Blatt, "Realization of a scalable Shor algorithm", *Science*, vol. *351*, pp. 1068–1070, 2016.

[122] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, F. Pawlega, "Revisiting TESLA in the Quantum Random Oracle Model", *Constructive Side-Channel Analysis and Secure Design*; Springer: Berlin/Heidelberg, Germany, pp. 143–162, 2017.

[123] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme", *IACR Trans. Cryptogr. Hardw. Embed. Syst.,* pp. 238–268, 2018.

[124] D. Stehlé, R. Steinfeld, "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices", *Proceedings of the Constructive Side-Channel Analysis and Secure Design*; Springer: Berlin/Heidelberg, Germany, pp. 27–47, 2011.

[125] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn, "SPHINCS: Practical stateless hash-based signatures", *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Sofia, Bulgaria, 26–30 April 2015; Springer: Berlin/Heidelberg, Germany; pp. 368–397, 2015.

[126] M. Hamza, K. Guenda, "A New variant of the McEliece cryptosystem based on the Smith form of convolutional codes", *Cryptologia,* vol.*42*, pp. 227–239, 2018.

[127] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies", *Proceedings of the International Conference on Financial Cryptography and Data Security,* Sliema, Malta, 3–7 April 2017; Springer: Cham, Switzerland, pp. 163–181, 2017.

[128] J.M. Couveignes, Hard Homogeneous Spaces. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.61. 5396&rep=rep1&type=pdf (accessed on 25 December 2020).

[129] A. Rostovtsev, A. Stolbunov, "Public-key cryptosystem based on isogenies", *IACR Cryptol. ePrint Arch., pp*. 145, 2006.

[130] Microsoft Research. Available online: https://www.microsoft.com/en-us/research/project/sidh-library/ (accessed on 15 December 2020).

[131] F. Li, Z. Zheng, C. Jin, "Secure and efficient data transmission in the Internet of Things", *Telecommun. Syst.*, vol. *62*, pp. 111–122, 2015.

[132] W. Lee, Y. S. Kim, J. S. No, "A New Signature Scheme Based on Punctured Reed–Muller Code with Random Insertion", *arXiv* **2017**,arXiv:1711.00159.

[133] A. Jalali, R. Azarderakhsh, M. Mozaffari-Kermani, "Efficient post-quantum undeniable signature on 64-bit ARM", *Proceed- ings of the International Conference on Selected Areas in Cryptography*, Ottawa, ON, Canada, 16–18 August 2017; Springer: Berlin/Heidelberg, Germany, pp. 281–298, 2017.

[134] R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel, C. Leonardi, "Key compression for isogeny-based cryptosystems," *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography*, Xi'an, China, 30 May–3 June 2016; pp. 1–10, 2016.

[135] U. Banerjee, A. Pathak, A. P. Chandrakasan, "2.3 An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things", *Proceedings*

*of the 2019 IEEE International Solid- State Circuits Conference—(ISSCC)*, San Francisco, CA, USA, 17–21 February 2019; pp. 46–48, 2019.

[136] S. Ebrahimi, S. Bayat-Sarmadi, H. Mosanaei-Boorani, "Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT", *IEEE Internet Things J.,* vol. *6*, pp. 5500–5507, 2019.

[137] T. John, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.*, vol. 2, pp. 134–144, 1966.

[138] M. Prasad, Y. T. Liu, D. L. Li, C. T. Lin, R.R. Shah, and O. P. Kaiwartya, "A New Mechanism for Data Visualization with Tsk-Type Preprocessed Collaborative Fuzzy Rule Based System", *J. Artif. Intell. Soft Comput. Res.*, vol. *7*, pp. 33–46, 2016.

[139] O. Kaiwartya, and S. Kumar, "Geocasting in vehicular adhoc networks using particle swarm optimization", *Proceedings of the International Conference on Information Systems and Design of Communication*, Lisbon, Portugal, 16 May 2014; pp. 62–66, 2014.

[140] M. Fengou, G. Mantas, D. Lymberopoulos, N. Komninos, S. Fengos and N. Lazarou, "A New Framework Architecture for Next Generation e-Health Services," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 1, pp. 9-18, Jan. 2013.

[141] H. Zhu et al. , "Smart Healthcare in the Era of Internet-of-Things," *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 26-30, 1 Sept. 2019.

[142] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51-58, February 2010.

[143] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma and T. Soyata, "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective", *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 53-71, Jan. 2020.

[144] M. Haghi et al., "A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring" *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5628-5647, June 2020.

[145] Y. Meng, Z. Huang, G. Shen and C. Ke, "SDN-Based Security Enforcement Framework for Data Sharing Systems of Smart Healthcare", *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 308-318, March 2020

[146] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang and J. Han, "Toward Practical Privacy-Preserving Processing Over Encrypted Data in IoT: An Assistive Healthcare Use Case," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10177-10190, Dec. 2019.

[147] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight Blockchain for Healthcare," *IEEE Access*, vol. 7, pp. 149935-149951, 2019.

[148] H. Wu and C. Tsai, "Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65-71, July 2018.

[149] L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare", *IEEE Access*, vol. 7, pp. 149935-149951, 2019.

[150] P. H. Vilela, J. J. Rodrigues, P. Solic, K. Saleem, and V. Furtado, "Performance evaluation of a Fog-assisted IoT solution for e-Health applications," *Future Generation Computer Systems,* vol. 97, pp. 379-386, 2019.

[151] H. Wang, X. Dong, and Z. Cao, "Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search," *IEEE Transactions on Services Computing,* vol. 13, no. 6, pp. 1142-1151, 2017.

[152] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p. 1207, 2019.

[153] H. Sukhwani, JM Martínez, X. Chang, K.S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 253-255, 2017.

[154] https://hyperledger.github.io/composer/v0.19/installing/development-tools.