A PRIVACY PRESERVING SECURE FRAMEWORK FOR MIOT DEVICES USING BLOCKCHAIN

A Dissertation

by

Muhammad Kashif

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Doctor of Philosophy

in the
Department of Computer Science

Özyeğin University
June 2024

A PRIVACY PRESERVING SECURE FRAMEWORK FOR MIOT DEVICES USING BLOCKCHAIN

Approved by:

Asst. Prof. Dr. Kubra Kalkan, Advisor
Dept. of Computer Engineering.
Özyeğin University

Prof. Dr. Fatih Alagoz
Dept. of Computer Engineering.
Bogazici University

Asst. Prof. Dr. Ismail Ari
Dept. of Computer Engineering
Özyeğin University

Prof. Dr. Murat Uysal
Dept. of Electrical Engineering
Özyeğin University

Date Approved: 20 May 2024

Prof. Dr. Albert Levi
Dept. of Computer Engineering.
Sabanci University

Dedicated to my beloved Family and Parents

ABSTRACT

The integration of Medical Internet of Things (MIoT) with traditional patient healthcare records (PHRs) has the potential to improve patients' quality of care by providing accurate diagnosis, track their vital signs, and provide real-time data to doctors for data analysis thereby improving the quality of life. However, PHRs are highly private, and the data sharing process raises significant security and privacy concerns. To surmount these challenges, this thesis proposes two innovative frameworks: Enhanced Privacy Preservation Based Blockchain Mechanism (EPIoT) and a Differential Privacy Preserving (DPP) framework, both leveraging blockchain technology.

The EPIoT model uses the immutability and decentralized nature of blockchain to ensure data integrity, transparency, and auditability in the patient health record (PHR) system. However, traditional blockchain systems impose high computational requirements that are not suitable for resource-constrained MIoT devices. To overcome this limitation, our proposed framework employ service-oriented layers approach in which each layers operate independently of each other, providing a flexible architecture for the MIoT ecosystem. The service-oriented layer approach comprises of four key layers:registration layer, authentication layer, privacy enforcement layer, and transaction layer. The registration layer focuses on the initial setup and registration of MIoT devices within the network. While the authentication layer is responsible for verifying the identity and authenticity of MIoT devices and the privacy enforcement layer is mainly responsible for enforcing the privacy of MIoT user by transferring control to the end user to limit how the data can be retrieved from the MIoT analytic process. The transaction layer handles the secure exchange of data and transactions within the MIoT network.

To further surmount the privacy preservation issues in MIoT based blockchain network

and to further enhance the privacy protection, we have proposed the DPP framework. DPP is a mathematical framework that ensures strong privacy guarantees. By implementing DPP at the stream level generated by IoT devices, it provides a rigorous mathematical framework that provides provable privacy guarantees, making it a more robust and reliable approach compared to the blockchain-based mechanism used in EPIoT. The DPP framework injects three different types of noises: Laplace noise, Gaussian noise, and Exponential noise, which are applied strategically to achieve privacy preservation. We have introduced a novel concept of privacy levels, which are adjustable by data owners as low, medium, and high. This flexibility addresses the varying privacy requirements of different applications and empowers data owners to customize the level of privacy preservation according to their specific needs. The impact of different parameters on the effectiveness of the approach is analyzed, providing recommendations for tuning. This comprehensive approach ensures a holistic solution for privacy preservation in MIoT-based blockchain systems without compromising the privacy of patients' sensitive health information.

Both the proposed frameworks were evaluated through simulations to assess their effectiveness in addressing security and privacy concerns in the patient health record system. In the EPIoT framework, the performance evaluation was conducted by deploying a quorum blockchain network. The simulation involved deploying three different consensus protocols (RAFT, IBFT, and PoA). The performance of the proposed architecture was assessed in terms of throughput (transactions processed per second) latency and block generation time. For each type of transaction sent, the simulation is evaluated using two modes of transmission i-e., sequential mode of transmission and multi-threaded transmission, and evaluates the performance of each network in terms of throughput and latency. On the other hand, in the DPP framework, a benchmark study between privacy and utility was first conducted using numerical simulation as implemented in Matlab. To support our argument, we plotted the privacy and utility curve for all three kinds of noises (Laplace, Gaussian, and Exponential). Further to simulate a blockchain network, a quorum-based blockchain network

is created, and evaluated the performance in terms of throughput and latency by setting the privacy level as low, medium, and high. Simulations demonstrated the efficacy of both frameworks, showing high levels of privacy preservation while upholding data utility and blockchain consistency. Furthermore, to demonstrate the efficacy of the approach, a security analysis of the proposed framework was conducted using the AVISPA tool, and the results confirmed that the framework attains the desired security goals.

In summary, this research offers a comprehensive solution for secure and privacy-preserving patient health record systems by leveraging blockchain technology. The findings showcase the immense potential of integrating MIoT devices with blockchain and can serve as a foundation for future research and development in secure and privacy-aware healthcare systems.

ÖZETÇE

Tıbbi Nesnelerin İnterneti'nin (MIoT) geleneksel hasta sağlık kayıtları (PHR'ler) ile entegrasyonu, doğru teşhis sağlayarak, yaşamsal belirtileri takip ederek ve doktorlara veri analizi için gerçek zamanlı veriler sağlayarak hastaların bakım kalitesini artırma potansiyeline sahiptir. Ancak PHR'ler son derece özeldir ve veri paylaşım süreci önemli güvenlik ve gizlilik endişelerini doğurmaktadır. Bu zorlukların üstesinden gelmek için bu tez iki yenilikçi yaklaşım önermektedir: Her ikisi de blockchain teknolojisinden yararlanan Gelişmiş Gizlilik Koruma Tabanlı blokzincir Mekanizması (EPIoT) ve Diferansiyel Gizlilik Koruma (DPP) yöntemi.

EPIoT modeli, hasta sağlık kaydı (PHR) sisteminde veri bütünlüğünü, şeffaflığını ve denetlenebilirliğini sağlamak için blokzincir değişmezliğini ve merkezi olmayan doğasını kullanır. Ancak geleneksel blolzincir sistemleri, kaynak kısıtlı MIoT cihazları için uygun olmayan yüksek hesaplama gereksinimleri gerektirir. Bu sınırlamanın üstesinden gelmek için önerdiğimiz çerçeve, her katmanın birbirinden bağımsız olarak çalıştığı ve MIoT ekosistemi için esnek bir mimari sağlayan hizmet odaklı katmanlar yaklaşımını kullanır. Hizmet odaklı katman yaklaşımı dört temel katmandan oluşur: kayıt katmanı, kimlik doğrulama katmanı, gizlilik uygulama katmanı ve işlem katmanı. Kayıt katmanı, MIoT cihazlarının ağ içindeki ilk kurulumuna ve kaydına odaklanır. Kimlik doğrulama katmanı, MIoT cihazlarının kimliğinin ve orijinalliğinin doğrulanmasından sorumluyken, gizlilik uygulama katmanı, verilerin MIoT analitik sürecinden nasıl alınabileceğini sınırlamak için kontrolü son kullanıcıya devrederek MIoT kullanıcısının gizliliğini uygulamaktan sorumludur. İşlem katmanı, MIoT ağı içindeki güvenli veri ve işlem alışverişini yönetir.

MIoT tabanlı blokzincir ağındaki gizlilik koruma sorunlarını daha da aşmak ve gizlilik

korumasını daha da geliştirmek için DPP çerçevesini önerdik. DPP, güçlü gizlilik garantileri sağlayan matematiksel bir çerçevedir. DPP'yi IoT cihazları tarafından oluşturulan akış düzeyinde uygulayarak, kanıtlanabilir gizlilik garantileri sağlayan sıkı bir matematiksel çerçeve sağlar ve bu da onu EPIoT'de kullanılan blockchain tabanlı mekanizmaya kıyasla daha sağlam ve güvenilir bir yaklaşım haline getirir. DPP çerçevesi üç farklı türde gürültü enjekte eder: Gizliliğin korunmasını sağlamak için stratejik olarak uygulanan Laplace gürültüsü, Gauss gürültüsü ve Üstel gürültü. Veri sahipleri tarafından düşük, orta ve yüksek olarak ayarlanabilen yeni bir gizlilik düzeyi konseptini kullanıma sunduk. Bu esneklik, farklı uygulamaların değişen gizlilik gereksinimlerini karşılar ve veri sahiplerine, gizlilik koruma düzeyini kendi özel ihtiyaçlarına göre özelleştirme olanağı tanır. Farklı parametrelerin yaklaşımın etkinliği üzerindeki etkisi analiz edilerek ayarlama önerileri sunulur. Bu kapsamlı yaklaşım, MIoT tabanlı blockchain sistemlerinde hastaların hassas sağlık bilgilerinin gizliliğinden ödün vermeden gizliliğin korunmasına yönelik bütünsel bir çözüm sağlar.

Önerilen çerçevelerin her ikisi de, hasta sağlık kayıt sistemindeki güvenlik ve mahremiyet endişelerini gidermedeki etkinliklerini değerlendirmek için simülasyonlar aracılığıyla değerle-ndirildi. EPIoT çerçevesinde performans değerlendirmesi, çekirdek blockchain ağının konuşl-andırılmasıyla gerçekleştirildi. Simülasyon, üç farklı konsensüs protokolünün (RAFT, IBFT ve PoA) dağıtılmasını içeriyordu. Önerilen mimarinin performansı, verim (saniyede işlenen işlemler), gecikme süresi ve blok oluşturma süresi açısından değerlendirildi. Gönde-rilen her işlem türü için simülasyon, sıralı iletim modu ve çok iş parçacıklı iletim olmak üzere iki iletim modu kullanılarak değerlendirilir ve her ağın performansını üretim ve gecikme açısından değerlendirir. Öte yandan, DPP çerçevesinde gizlilik ve fayda arasında bir kıyaslama çalışması ilk olarak Matlab'da uygulandığı gibi sayısal simülasyon kullanılarak gerçekleşti-rilmiştir. Tartışmamızı desteklemek için, üç tür gürültünün (Laplace, Gauss ve Üstel) gizlilik ve fayda eğrisini çizdik. Ayrıca bir blockchain ağını simüle etmek için çekirdek tabanlı bir blokzincir ağı oluşturulur ve gizlilik seviyesi düşük, orta ve yüksek

olarak ayarlanarak performans, verim ve gecikme açısından değerlendirilir. Simülas-yonlar, her iki çerçevenin de etkinliğini gösterdi; veri kullanışlılığını ve blokzincir tutarlılığını korurken yüksek düzeyde gizlilik koruması gösterdi. Ayrıca yaklaşımın etkinliğini göstermek için AVISPA aracı kullanılarak önerilen çerçevenin güvenlik analizi yapıldı ve sonuçlar, çerçevenin istenen güvenlik hedeflerine ulaştığını doğruladı.

Özetle bu araştırma, blokzincir teknolojisinden yararlanarak güvenli ve gizliliği koruyan hasta sağlık kayıt sistemleri için kapsamlı bir çözüm sunuyor. Bulgular, MIoT cihazlarını blockchain ile entegre etmenin muazzam potansiyelini ortaya koyuyor ve güvenli ve gizliliğe duyarlı sağlık sistemlerinde gelecekteki araştırma ve geliştirmeler için bir temel oluşturabilir.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Prof. Dr. Kubra Kalkan, my advisor, for her invaluable guidance and unwavering support throughout my research journey. Her expertise, encouragement, and constructive criticism have been instrumental in shaping the outcome of my work. Without her mentorship, I would not have been able to achieve my goals in this field of research.

I am also indebted to Dr. Ismail Ari, Prof. Dr. Murat Uysal, Prof. Dr. Albert Levi and Prof. Dr. Fatih Alagoz, members of my thesis committee for their valuable contributions and insightful feedback, which have greatly enriched the quality of my research.

I would like to extend my heartfelt appreciation to my friends who have provided me with companionship and valuable ideas during the preparation phase of my thesis. Their support has been invaluable in shaping my thoughts and refining my work.

I am grateful to Dr. Sohail Sarwar for his continuous support, technical assistance, and emotional encouragement during the challenging moments of my research. His expertise and guidance have been invaluable to me.

I am deeply thankful to my family for their unconditional love, moral support, and financial assistance throughout my educational journey. Their unwavering belief in me has been a constant source of motivation, and I am truly blessed to have such supportive and caring parents.

Lastly, I want to express my immense gratitude to my wife, Ambreen Kashif for her unwavering support in countless ways. Her presence, understanding, and encouragement have been my pillars of strength throughout this journey. I am thankful for her companionship and the sacrifices she has made to ensure my success.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

The unprecedented growth of IoT devices is paving the path for a revolutionized modern-day world in which every smart device will gather, share, and exchange information with nearby devices. The data gathered by these Internet of things (IoT) devices may encompass confidential or private information and they can be installed in different applications like health care, industrial control automation, energy systems, and transportation. The paramount figure for these IoT devices is expected to be reached more than 500 billion in the year 2030 [2]. With such astronomical amounts, the importance of IoT devices in our daily lives is ubiquitous. The sheer data of information being collected by these smart gadgets from its surrounding provides specific services to the end users. Another very eye-catching domain for the IoT is the medical internet of things (MIoT) where different sensors are deployed to measure the patient's vital signs (e.g. oxygenation level, and heart rate), enabling more proactive and preventive care by healthcare practitioners. Recently, the COVID-19 pandemic underscored the importance of MIoT (Medical Internet of Things) as a critical tool in managing the crisis. With hospitals operating at full capacity, patients were directed to remain at home, and MIoT played a pivotal role in providing remote monitoring and guidance during this challenging period. However, keeping COVID19 patients at home requires constant monitoring of vital signs and it can be achieved by adopting MIoT sensors and applications [3]. Furthermore, By leveraging the power of MIoT, all the patient's health data recorded as personal health records (PHRs) need to be updated frequently [4] and any kind of data loss or errors are intolerant as they directly impact the health of the patients. In addition, PHR sharing provides vital evidence for medical judgment, highlights negligence during treatment, and assesses medical insurance [5]. Therefore sharing

PHR data with various Internet of Medical things (IoMT) sectors has garnered significant attention from various stakeholders involving academia, government, and industry [6], [7]. Despite the popularity of MIoT and its associated networks may be irrefutable, however, these devices impose serious security and privacy threats and still face certain challenges that need to be addressed.

Security and privacy are the two fundamental concepts in the field of MIoT domain that requires delegated attention for protecting user information from various assaults. Though the notion of privacy and security is very much inter twisted, they can be distinguished from each other based on the model used to create and communicate data with the outside world. Security defines the set of protocols and protects the valuable information from prying eyes and protects it from outside cyber-attacks. Because of these MIoT devices' resource limitations, there is a strong possibility for exploiting MIoT risks like DDoS assaults, and man-in-the-middle (MiTM) attacks.

Most of the time privacy is conflated with security and secure mechanisms that are available commercially are often tagged as privacy-preserved solutions. Privacy can be defined as a mechanism where the end-user has complete control over their confidential data. Therefore the data transmission from the MIoT sensors towards the data analysis requires trust oriented framework that caters privacy-preserving mechanism providing the data owner the fine grinned control over his/her data.

1.1 Key Challenges

Here we have highlighted and listed some of the key challenges from the security and privacy aspect that MIoT devices inherently suffer from :

- Data breaches: MIoT devices are particularly vulnerable to cyber-attacks enabling the attackers to launch assaults and penetrate the MIoT network which can lead to the access of confidential and theft of sensitive data. A study found that more than 40% of MIoT devices have known security vulnerabilities, which can be exploited

by hackers [8].

- Data ownership and control: Since MIoT devices are operated and owned by third-party companies, there exists a lot of concern about data ownership. This lack of control can lead to privacy violations, such as unauthorized data sharing or data misuse [9].

- User identification: Many MIoT devices are designed to collect and access sensitive data pertaining to user location that can be used for surveillance purposes and may collect behavioral data for targeted advertisement or some other commercial purposes. This can raise privacy concerns and potentially lead to the violation of users' anonymity [10].

- Inadequate data protection: Traditional authentication methods such as weak password protection may not be practically feasible to secure MIoT devices as these devices are vulnerable to hacking or other security threats. A study found that many MIoT devices lack basic security features, such as password protection and encryption [11].

- Lack of standardization and regulation: In terms of regulation, the MIoT eco-system currently lacks clear guidelines and standards which can lead to the development of insecure and privacy-violating devices. A study found that many MIoT devices do not conform to industry standards or best practices, making them vulnerable to attacks [12].

To overcome these challenges researchers are motivated to explore and restructure the architecture of the MIoT ecosystem and suggested various cloud-based solutions to address the security and privacy concerns [13],[14],[15],[16]. Cloud is usually considered as a semi-trusted infrastructure that collects, stores, and manages a large amount of information, which may potentially lead to privacy leakage of personal information due to inside

malicious attacks or the high-end servers being compromised. However, there exist various robust encryption schemes for storage purposes and homomorphic encryption schemes for secure computations but still in some case the employees or other insiders who have access to sensitive data may intentionally or unintentionally leak or misuse the data, even if it is encrypted. Furthermore, fog and mist architecture [17] is also proposed by some of the researchers acting as network edge technology and amalgamating with MIoT ecosystem but there exists a bandwidth constraint as they suffer from the bottleneck issue by uploading every transaction in the network. Cryptographic techniques cannot be directly deployed at MIoT sensor level as MIoT devices have inherent limitations both in terms of processing and memory requirements. Many works have also considered the integration of cryptographic techniques with that of cloud computing, but there remain non-negligible drawbacks [18],[19]. To alleviate the above-mentioned issues and embrace new technologies, many researchers leverage blockchain as a new paradigm to address security and privacy issues [20]. Blockchain is considered a decentralized distributed ledger that store and keep records in an immutable fashion [21] with the capability to digitize transaction securely and efficiently. Initially, blockchain was introduced for cryptocurrency due to its specialty in handling transaction where no trust is needed, and security & reliability is achieved through a smart contract that automates the process. Recently keeping in view, the capability of blockchain, its application is now extended to other domains as well like MIoT, AI etc. In the context of MIoT, blockchain forms a P2P network allowing nodes to exchange information in a decentralized manner. Blockchain effectively mitigates fraudulent activities by broadcasting information to all nodes in a network. Only when a consensus is reached by the majority of nodes, the transaction is added to the blockchain, ensuring its integrity and reliability. This decentralized consensus mechanism enhances security and trust in the system, minimizing the risk of fraudulent behavior. Blockchain is best suited for MIoT devices to address privacy concerns as in contrast to centralized MIoT architecture,

it is very much difficult to attack several interconnected peers and collect personal information or control the entire system. Blockchain offers several other advantageous features like transparency, faster settlement, anonymity, and tamper resistance which makes it an ideal candidate for data exchange within the MIoT ecosystem [22],[23]. Even though the rising integration of blockchain with MIoT systems is auspicious but it still faces the following challenges from the privacy aspect:-

- How to ensure the authenticity of transactions made by these MIoT devices without divulging the MIoT users' privacy on the blockchain?
- How to set the personalized access control mechanism for the individual user so that data can only be shared with authorized users over the blockchain network?
- How to develop smart contracts to achieve the privacy preserved framework while maintaining the privacy of smart contracts as well?
- Most of the privacy strategies primarily follow an opt-out approach, where the data owner is compelled to accept the terms and conditions of privacy, or else the user is denied access to the services.

Therefore, it is indispensable to design and develop those devices which promote privacy by design framework, and which ensure the privacy preference as set by the data owner. Acknowledged and motivated by these challenges, this thesis presents two innovative frameworks:Enhanced Privacy Preservation Based Blockchain Mechanism (EPIoT) and a Differential Privacy Preserving (DPP) framework, both leveraging blockchain technology to address the security and privacy concerns in MIoT eco-system.

In EPIoT framework, we proposed a chain of smart contract layers that are mainly responsible for the registration, authentication, privacy enforcement policy for these MIoT devices. Additionally this work aims to focus on giving the end user complete control of his/her data and giving the complete preference by whom that data needs to be processed or

managed by the consumer. Similarly extending this concept, an end user can set the privacy preference for every data flow derived from the MIoT sensor, thereby propelling the privacy aspect to the stream level generated by MIoT devices. The concept of service oriented layers is mainly responsible for ensuring that trustworthy and reliable devices can become a part of our proposed blockchain network. Every contract will work independently from the other chain and a service-oriented chain concept is implemented to achieve the security and privacy aspect that is well suited for the MIoT domain.

In order to enhance the reliability and contribute to a more secure and trustworthy ecosystem for MIoT, we have proposed a DPP framework. This framework is based on a rigorous mathematical model that offers provable privacy guarantees, making it a more robust and reliable approach compared to the blockchain-based mechanism used in EPIoT. This module will first identify the level of privacy (low, medium, high) and utility as desired by the data owner followed by generating a controlled noise determining the trade-off between privacy and utility. Moreover, three different kind of noises: Laplace noise, Gaussian noise and Exponential noise are applied strategically to achieve the overall privacy preservation mechanism. This proposed framework will also provide a privacy monitoring aspect ensuring the level of privacy is maintained over time. Essentially the compliance check is executed via smart contract and the result is immutably stored on the blockchain so that it can be auditable as well. We theoretically analyzed the monotonicity of the Laplace, Gaussian and Exponential mechanism by measuring the trade-off between privacy and utility.

1.2 Contribution of this Thesis

The contribution of this thesis lies in addressing the security and privacy preservation issues in patient health record (PHR) systems and proposing a blockchain-based architecture as a potential solution. The thesis makes the following notable contributions:

- To address concerns regarding security and privacy, we propose a private by-design framework to integrate MIoT with consortium blockchain. This private by-design

framework empower the data owner by shifting the control from data consumers who perform data analysis to the data owner.

- We introduce the notion of service-oriented layers to alleviate the complexity constraint as needed by these MIoT devices. These four layers namely the registration layer, authentication layer, privacy enforcement layer, and transaction layers executed independently of each other to provide a complete end-to-end framework specifically for the MIoT devices.
- Our framework will provide the functionality of setting the privacy preference by the data owner for each data stream generated by an MIoT device and provide a decentralized privacy compliance check so that it can be auditable as well.
- A thorough security and complexity analysis of our proposed framework using AVISPA tool to make sure that our proposed scheme is both secure and less complex so that it can meet the stringent requirements of MIoT that can be implemented in real-world life.
- Foregoing, extending our concept, we designed a novel privacy-preserving framework by deploying a differential privacy module in conjugation with BC network. This module will first identify the level of privacy (low, medium, high) and utility as desired by the data owner followed by generating a controlled noise determining the trade-off between privacy and utility.
- The proposed framework incorporates a privacy monitoring aspect to ensure the maintenance of a desired level of privacy over time. Compliance checks are executed through smart contracts, and the results are immutably stored on the blockchain for the audit purpose.

1.3 The Outline of the Thesis

The remaining sections of this thesis are structured as follows:

- Chapter 2 provides an in-depth understanding of the blockchain and its key concepts. This section will specifically focus on the Quorum blockchain and its constituent modules which serve as a basis for building our proposed system model.

- Chapter 3 discusses various privacy preservation techniques proposed in the literature to address issues in Personal Health Record (PHR) system. The purpose of the review is to assess the current state of the field and offer valuable insights for formulating a robust framework for preserving privacy.

- Chapter 4 presents the overall privacy by design system model along with its constituent module that build the entire system model.

- Chapter 5 will explain in detail the EPIoT framework and describing its key component in detail. This section will highlight how initially our MIoT devices will be registered followed by the authentication step. The Privacy enforcement layer will make sure that data shall only be shared with outside world as per his/her privacy preference. Moreover, it provides an additional features of compliance checks for auditing purpose as well. The section will provide a clear explanation of how the information flows within the Quorum blockchain. Additionally, it will also describe the flow of information from the MIoT sensors (data owner) to the doctor (data user) in our case scenario. This explanation will help to understand the data analysis aspect in detail. Moreover this chapter will also describes the Performance analysis of our proposed EPIoT via implementing the blockchain network. The security assurance that is provided by the overall proposed system model is tested using a verification tool called AVISPA.

- To further enhance privacy protection, Chapter 6 presents the novel privacy framework by deploying differential privacy module in conjugation with Quorum blockchain network. Three different kind of noises: Laplace noise, Gaussian noise and Exponential noise are introduced determining the trade-off between privacy and utility

followed by the Performance analysis of our proposed DPP framework integrated with blockchain.

- Chapter 7 concludes the study by providing a concise summary of the significant findings and contributions derived from the research. The key findings obtained through the simulations shed light on various aspects of the proposed methods, providing valuable insights into their effectiveness and performance. These findings serve as empirical evidence, demonstrating the feasibility and potential of the developed approaches in addressing the research problem.

CHAPTER II

THEORETICAL BACKGROUND

This chapter provides an in-depth exploration of the theoretical foundations surrounding blockchain technology, smart contracts, and privacy preservation techniques. It sets the stage for addressing the privacy concerns associated with integrating MIoT (Medical Internet of Things) devices with blockchain.

To begin, we dive deep into the basics of blockchain and smart contracts followed by the Quorum blockchain which laid the foundation of our proposed framework. Secondly we discussed the various distributed consensus mechanisms such as RAFT, Istanbul byzantine fault tolerance (IBFT) and Proof of Authority (PoA). Additionally, we examine the privacy preservation model formulating the problem statement for our research.

2.1 Blockchain and Smart Contracts

Blockchain is considered as decentralized distributed ledger that store and keep records in an immutable fashion with the capability to digitize transaction securely and efficiently [24]. In a blockchain, a transaction represents a transfer of value or information between two parties, and it needs to be validated and processed before being added to the blockchain. The linkage between blocks in the blockchain is established by utilizing the hash value of each block, creating an immutable chain of blocks that is highly resistant to tampering or modification. This structure ensures the integrity of the blockchain and provides a permanent record of all transactions as shown in Fig. 1. The blockchain is maintained and updated by a network of nodes, or computers, that are engaged in the consensus protocol to verify transactions and incorporate new blocks into the chain. Complementing blockchain, smart contracts are self-executing agreements with predefined rules encoded directly into

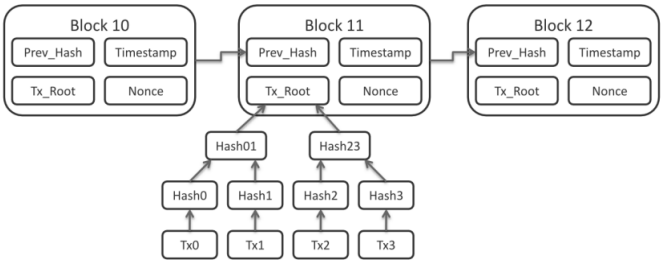

Figure 1: Blocks in a Chain

the blockchain. These contracts automatically execute and enforce the terms of an agreement without relying on intermediaries [25]. By eliminating human intervention, smart contracts enable trust and efficiency in every business interactions. They provide a reliable and transparent framework for parties to engage in transactions, ensuring that the agreed-upon conditions are met. By leveraging these capabilities of smart contracts, the integration of smart contracts and blockchain framework enables the automation and enforcement of various security and privacy-preserving mechanisms in MIoT domain. Smart contracts can be used to define and implement access control policies, data sharing agreements, and other rules governing the system, ensuring that all parties adhere to the agreed-upon protocols. For example, smart contracts can be used to automate the process of patient consent management, allowing individuals to control the access and usage of their medical data. They can also be used to facilitate secure and transparent medical device authentication and thus enhancing the overall security and privacy of the MIoT infrastructure. To summarize, by incorporating blockchain and smart contract-based solutions, the MIoT system can overcome the limitations of traditional centralized approaches and provide a more robust, secure, and privacy-preserving framework for medical data management and device integration. The decentralized and transparent nature of these technologies can empower patients, healthcare providers, and other stakeholders to collaborate more effectively, while maintaining the necessary level of control and trust over sensitive medical information. Table 1 presents a compilation of significant attributes associated with blockchain.

Table 1: Features of Blockchain

Property	Details
Decentralized	Transfer of control or decision making from an individual to a distributed node.
Transparency	Every transaction is traceable and can be viewed by all the nodes in the network
Data Immutability	Distributed database to remain unchanged, unaltered, and indelible
Consensus	All the transactions are validated by the majority of nodes. Transaction can be denied as well if they don't follow the endorsement policy
Highly Secure	Difficult to attack as there is no single point of failure or the node comprises

2.2 Blockchain Types

Blockchain technology is evolving rapidly, and there are various hybrid models and novel implementations that combine aspects of different types of blockchains to address specific requirements and use cases. Broadly, blockchain is classified in three main categories. (1) Public Blockchain (2) Private blockchain (3) Consortium Blockchain.

2.2.1 Public Blockchain

Public blockchains are decentralized and open to anyone to participate as the name indicates, validate transactions, and maintain the blockchain [26]. One of the advantages of blockchain is that all transactions and data are visible to all participants, thus promoting transparency, trust and accountability. They are more secure as they used consensus mechanisms (e.g. Proof of Work) to ensure the integrity and security of the network and they are highly resistant to single points of failure. In order to discuss their disadvantages Public blockchain often face scalability challenges due to the large number of participants and transaction volumes. Also, Public blockchains typically have limited privacy features, as

transaction data is visible to all participants. Bitcoin [27] is a well-known example of a public blockchain where anyone can participate as a miner [28] and validate transactions.

2.2.2 Private Blockchain

Private blockchains are restricted to a specific group of participants, and the network is controlled by a single entity or organization [29]. Private blockchains can provide better privacy and confidentiality for participants, as transaction data can be selectively shared and they can achieve higher scalability compared to public blockchains by reducing the number of participants. Since private blockchains have a limited number of trusted participants, consensus mechanisms can be more efficient. As a downside, Private blockchains are controlled by a single entity, which raises concerns about trust and potential manipulation so we can say that they are less decentralized and they can be more susceptible to single points of failure and malicious attacks. Hyperledger Fabric [30] is a popular example of a private blockchain framework used for enterprise applications.

2.2.3 Consortium Blockchain

Consortium or permissioned blockchains are governed by a group of known and trusted entities, typically formed for specific use cases or industries [31]. Consortium blockchains allow for shared control and decision-making among participating organizations and thus have better governance. Also, participants in a consortium blockchain can have more granular control over data sharing and access permissions. Consortium blockchains has an added advantage of achieving higher transaction throughput compared to public blockchains, making them suitable for enterprise applications. Quorum and R3 Corda is an example of a consortium blockchain platform designed for financial institutions and other industry-specific use cases.

Our proposal is also based on Quorum blockchain [32] which is a platform designed for enterprise use cases, particularly in the finance industry. It was developed by J.P. Morgan, one of the largest banks in the world, and is open-sourced under the Apache 2.0 license. The

Quorum blockchain is a technology which is developed by J.P. Morgan and has recently gained attention due to its innate capability of providing smart contract and transaction privacy. It is based on permissioned and private distributed ledger technology making it a favorable concept for privacy measurement when compared with Ethereum, Hyperledger, and other blockchain networks. These significant features can successfully pave the way for the mass adoption of MIoT networks in a real environment addressing security and privacy concerns. In this section, we provide an overview of the fundamental features of the Quorum blockchain and its constituent modules.

2.2.4 Quorum Blockchain

Quorum, developed by J.P. Morgan and now owned by ConsenSys, is a blockchain platform that originated as a soft fork of the Ethereum blockchain [33]. It enables controlled network access by establishing a peer-to-peer network exclusively among authorized nodes. A distinctive feature of Quorum is its native support for transaction privacy, as it selectively shares private information solely with a subset of network participants. While originally designed with a primary emphasis on financial applications, Quorum is an open-source project with a growing range of use cases. Fig. 2 shows the key components in Quorum's architecture. In Fig. 2, the Quorum blockchain, derived from go-Ethereum, incorporates a

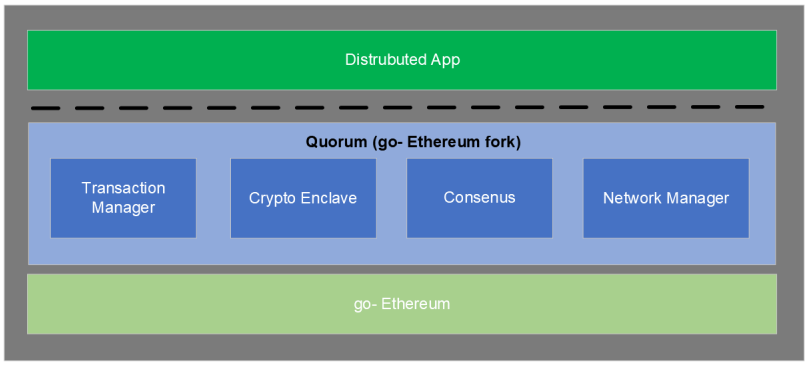

Figure 2: Quorum's Architecture and Components

Transaction Manager responsible for accessing encrypted transaction data in private transactions. This component facilitates local data storage management and communication

with other transaction managers, but does not have access to sensitive private keys. Instead, the Crypto Enclave assumes the critical role of managing private key operations and handling encryption and decryption of private transaction data. The Enclave collaborates closely with the Transaction Manager to ensure that encryption and decryption processes take place within a secure and isolated environment. Operating as a virtual Hardware Security Module, the Enclave functions independently from other system components.

Another critical component of Quorum is the Network Manager, which governs network access and facilitates the creation of permissioned networks among participating nodes. By controlling network permissions, the Network Manager helps maintain the integrity and privacy of the overall system. The Quorum blockchain incorporates several key features, including:

- The Quorum blockchain offers inherent confidentiality for transactions and smart contracts, ensuring that access is granted only to authorized participants involved in specific transactions.

- Provides support for diverse consensus mechanisms based on voting, including RAFT, Istanbul Byzantine Fault Tolerance (IBFT), and Proof of Authority (PoA).

- Additionally, Quorum enhances scalability and network performance, enabling efficient handling of increased transaction volumes while optimizing overall system efficiency.

By leveraging the inherent confidentiality, consensus mechanisms, and scalability features of Quorum blockchain, they can be more suitable for addressing privacy preservation issues in the context of Medical Internet of Things (MIoT) and Personal Health Records (PHR) system. All patient sensitive data, such as medical records or personal health information, can be securely stored on the blockchain and accessed only by authorized participants involved in specific transactions. This feature ensures that privacy is preserved and that data is

not visible to unauthorized entities. Since MIoT systems generate a large volume of transactions and data, which can pose challenges for traditional blockchain networks. Quorum blockchain can addresses this by implementing techniques such as transaction privacy and optimized network communication protocols. These optimizations enable efficient handling of increased transaction volumes, ensuring that MIoT systems can process data in a timely manner while maintaining privacy and preserving the overall system's efficiency.

The Quorum blockchain's overarching architecture consists of the following components: (1) Quorum Client: A modified version of geth, the Quorum Client plays a pivotal role in processing private transactions within a designated group of participants. (2) Privacy Manager: The central entity responsible for implementing the privacy features of Quorum. The Privacy Manager comprises two key modules: the Transaction Manager and the Encryption/Decryption Enclave. These modules facilitate secure and encrypted data exchange among nodes within the network.

2.2.4.1 Transaction Manager

The transaction manager is the key actor mainly responsible for providing privacy to private transactions in Quorum blockchain. It provides the following three tasks:-

- Automatically discover all nodes in the network by establishing a P2P connection with other node's transaction managers.
- Provides an interface to encryption and decryption enclave to provide confidentiality feature to the payload.
- Provide storage to encrypted payload.

Quorum blockchain endorsed Tessera as a reliable transaction manager in its latest version. It is written in java and is mainly responsible for establishing and distributing private transactions to other nodes in a network.

2.2.4.2 *Encryption/ Decryption Enclave*

This module provides encryption/ decryption functionality as well as key management. It is considered a virtual hardware security module (HSM). This method enables to store all sensitive operations in a fully isolated mode thus reducing the impact of outsider attacks as well.

2.2.4.3 *Consensus Protocol*

Consensus algorithms are employed to achieve consensus among networks of nodes in a distributed system. These algorithms must fulfill three essential properties:-

- Agreement: All correctly functioning processes within the system must reach an agreement on the same value.
- Validity: The value agreed upon must have been proposed by a process within the system.
- Termination: Eventually, every correct process will arrive at a decision and settle on a value.

Three different consensus protocols can be implemented in the Quorum blockchain. RAFT [34], IBFT [35] and PoA [36]. Since Quorum is a permissioned blockchain in which every node needs to be authenticated first before joining the network so there is no need to deploy a strong cryptographic puzzle solving consensus protocol like proof of work (PoW) to keep the network safe. Consensus protocol hones in on a famous trilemma of a distributed system called the CAP theorem. It is a fundamental theorem for any distributed system pertaining to achievable properties. CAP stands for three main components as Consistency, availability, and partition tolerance. By deploying these three-consensus protocols in the quorum blockchain we will evaluate the performance of each consensus protocol and will provide the trade-off between consistency, availability, and partition tolerance concerning the CAP theorem [37].

2.2.4.4 RAFT

Raft [27] stands for replicated and fault-tolerant is distributed consensus algorithm based on Paxos [38]. Raft is a crash fault tolerant algorithm where the maximum node can exhibit crash failure if $n > 2f + 1$, where n represents the number of nodes and f represents the crash failure node. There is three node state transition state in Raft (1) Follower (2) Candidate (3) Leader. Initially, when the nodes start up it is in the follower state. It may be the first time the node started, or a node may be recovered after it crashes. For the node to become a leader it has first to become a candidate. Raft elects its leader first among the group of nodes and gives full authority to a leader, a leader node accepts transaction request, propose new blocks, and manages the replication of logs on the other nodes. A leader election process is deterministic it means that to converge the network the leader must be elected by the majority of nodes. The leader node will continuously send its periodic heartbeat to the follower hence it remains a leader for the many rounds of protocol execution. The leader is assumed to be honest in Raft and all the remaining nodes must follow the leader. From a CAP theorem frame of reference, Raft exhibits C-P system. It ensures strong consistency while guaranteeing partition tolerance. When there is a network partition, those partitions with a majority of nodes can execute a client request while those who are a part of minority nodes, they simply skip the client request hence availability is abdicated. Therefore, the Raft ensures immediate finality [39] which means that no forks are produced in Raft.

2.2.4.5 Istanbul Byzantine Fault Tolerance (IBFT)

IBFT, introduced by Castro and Liskov [40] and referenced as [35], is a Byzantine fault tolerance algorithm. It shares similarities with Raft in that it involves electing a proposer or leader and conducting multiple rounds of communication for block proposal and commitment. However, IBFT distinguishes itself by requiring multiple rounds of voting by validator nodes for each block, rather than blindly trusting a leader as in Raft or other crash

fault tolerance algorithms. In an IBFT network, a maximum of f faulty or dishonest nodes can be accommodated in a network of N = 3f + 1 nodes. In the presence of a network partition, where there are more faulty nodes than honest nodes, the protocol halts until the partition is resolved. Consequently, IBFT demonstrates characteristics of C-P (consistency and partition tolerance) based on the CAP theorem. Similar to Raft, IBFT achieves finality, thereby preventing forks from occurring.

2.2.4.6 Proof of Authority (PoA)

Proof of Authority PoA consensus algorithm [36] is purposely designed for a private network to emulate the design of PoW consensus. PoA has an inbuilt feature of a high transaction rate and high tolerance rate as compared to PoW. In contrast to Practical byzantine fault tolerance (PBFT), PoA requires minimum exchange of messages among the nodes hence low overhead as compared to other consensus algorithms. A new block is created or mined by a group of authority nodes, which are presumed to be trustworthy. It is required that the number of honest nodes is at least N/2 + 1, where N represents the total number of nodes in the network. Each authority node is permitted to propose a new block following a schedule of N/2 + 1 block intervals. If any node in the authority list exhibits erroneous behavior, it can be voted out by the remaining nodes in the authority list, effectively preventing it from impacting the network any further. Since PoA guarantees eventual consensus finality so from the perspective of CAP theorem, it can be deduced that it satisfies the A-P property of CAP theorem. It compensates for strong consistency over availability and partition tolerance. Hence forks are produced due to inconsistency which is resolved later. It is important to mention over here that the performance analysis of any blockchain network and its implemented consensus protocol depends on various parameters and factors like throughout, latency, immediate finality and fault tolerance as shown in Table 2

Table 2: Comparison of Blockchain Consensus Algorithms

Property	RAFT	IBFT	PoA
Complexity	$\theta(n)$	$\theta(n^2)$	$\theta(n)$
Finality	Instant	Instant	Eventual
Forks	No	No	Yes
Fault tolerance	$(n \geq 2f+1)$	$(n \geq 3f+1)$	$(n \geq 2f+1)$
CAP analysis	C-P	C-P	A-P

2.3 Privacy Preservation Model

Mostly privacy policy is specified by a consumer iterating which personal information they will collect from the individual stating their purpose, describing how long they will keep the information, and whether the data collected shall be available for third-party usage or not. On the other hand, the data owner specifies the privacy preference in terms of purpose, holding time, and an arbitrator release. We adopted privacy model as adopted in [1] which is mainly designed for MIoT scenario. According to [1] purposes are hierarchically organized into a tree-based structure which is known as purpose tree (PT) as shown in Fig. 3. Such tree-based architecture has the advantage of limiting the number of purposes as specified in a privacy preference.

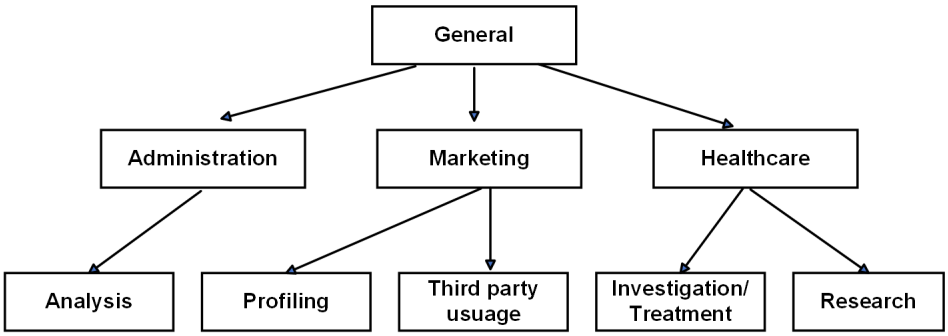

Figure 3: An example of purpose Tree [1]

Definition 1(Data Owner intended purpose DOip): Data intended purpose mainly comprises of two parameters (Allowed Dip and outlier) where ADip is a set of purposes authorizing the access mainly derived from purpose tree PT, whereas outlier OT represents the non-authorize access to the set of purposes descent from the elements in Allowed Dip such

that

$$DOip = ADip - OT \tag{1}$$

Definition 2(Data Owner privacy preference DOpp): Data owner privacy preference is a tuple mainly comprises of following parameters

$$DOpp = SD, Consumerid, DOip, HT, Arbitratorrelease \tag{2}$$

Where SD id is the unique identity of stream of data collected by the MIoT sensor, consumer id identify the set of identities to whom privacy preference policy applies, DOip is the data owner intended purposes define the set of purposes that will be used by the consumer, HT (holding time) is the maximum duration mentioning how long the data would be available for the data analysis and after the time elapsed the data analyst needs to subscribe again and request from the data owner for the data availability, and arbitrator release specify whether the private data collected would be available for third party usage or not.

Example 1 : Let us consider an example of private data of a patient who is the data owner and whose respiration rate, heart rate, and oxygen saturation level are sensed by MIoT devices, and it needs to be remotely monitored by a doctor in the hospital namely the consumer. Since all this data is private therefore data owner can set a privacy preference (pp) for each data stream originated by a monitoring system. For simplicity, the patient or the data owner only wants to monitor his/her oxygen level and such data the patients want to share for administration and medical purposes with the hospital. The data should not be available for any marketing or research purposes. Moreover, the patient does not want to save this information for more than 30 days and does not want to share this information with any third party for any usage To model privacy preservation for our considered example 1, Eq 1 implies

$$DOip = ADip - OT \tag{3}$$

Where ADip is the intended purpose set from the purpose tree (PT), which is for healthcare and administration purposes for this example and (OT) is the outlier list to whom data

is not allowed to be shared for any purposes like marketing or research as stated in example 1. Eq 1 would become:

$$DOip = (healthcare, admin) - (marketing, research) \tag{4}$$

A data owner can set privacy preference (pp) as implied by equation 2:

$$DOpp = SD, Consumerid, DOip, T, Arbitratorrelease \tag{5}$$

SD is the oxygen level which the data owner wants to share Consumer mainly comprise of hospital as stated in example 1 T is 30 days' time period, Arbitrator release is the Boolean expression, and it is expressed in terms of true or false. In our particular example it is false as the data owner don't want to disseminate this information with any third party. So, arbitrator release is false Eq 2 would become

$$\begin{aligned} DOpp = &\text{oxygen level, hospital,} \\ &\text{[(healthcare, admin) - (marketing, research)], 30d, false} \end{aligned} \tag{6}$$

When the consumer data usage policy complies with the data owner's privacy preference only then the data will be transferred to the consumer. The privacy compliance check will regulate and monitor all the policies set by the data owner so that the consumer complies with the data owner's will.

2.4 Privacy Enhancing Technologies (PETs) for Data Privacy

Privacy Enhancing Technologies (PETs) encompass a range of techniques and tools designed to safeguard data privacy. These techniques aim to minimize the collection, use, and disclosure of personal information, while still allowing for effective data analysis and utilization. Some of the common PETs techniques used for data privacy are Anaonmyzation, homomorphic encryption, Secure multiparty computation (SMC), and Zero knowledge proof and differential privacy.

Anonymization techniques transform or remove personally identifiable information (PII) from datasets to prevent the identification of individuals. This can involve techniques such as data masking, generalization, or perturbation to obfuscate sensitive attributes while preserving the overall utility of the data. In the realm of data privacy, three prominent anonymization techniques have gained recognition: k-anonymity [41], l-diversity [42], and t-closeness [43]. These techniques serve the purpose of de-identifying individuals' private data, safeguarding their sensitive information from being easily attributed to specific individuals. By employing these anonymization methods, data privacy can be effectively preserved, allowing for meaningful data analysis and secure data sharing. However, Anonymized data can still be re-identified using external information or by combining multiple datasets. Such techniques may sacrifice data granularity or accuracy, affecting the usefulness of the data for certain analyses and it is quite challenging to find the right level of anonymization that adequately protects privacy while maintaining data usefulness.

Similarly cryptographic based approach like homomorphic encryption allows computations to be performed on encrypted data without decrypting it, thereby preserving data privacy. This technique enables secure data processing and analysis while keeping the original data encrypted. Since Gentry's seminal work in 2009 [44, 45], which introduced the first functional fully homomorphic encryption scheme, there has been a surge of interest in this field. The prospect of performing computations on encrypted data in real-world applications has captivated researchers. Notably, Rodriguez et al. [46] proposed a security-enhanced architecture with an access control scheme for users to regulate access to their health data. By leveraging homomorphic encryption on individual components, they ensured communication security and query privacy while performing computations on users' health data. Similarly, Jayaraman et al. [47] presented an IoT architecture that employed homomorphic encryption to achieve privacy-preserving access control. This approach enabled users to control data access while allowing service providers to store, analyze, and extract valuable insights without compromising users' personal information. However, it

is important to acknowledge that fully homomorphic encryption still faces challenges in terms of efficiency, making it less suitable for resource-constrained MIoT devices. Certain computations, such as machine learning algorithms, may pose difficulties or inefficiencies when executed on encrypted data, particularly in resource-constrained MIoT environments.

In addition, Secure multiparty computation (SMPC) enables multiple parties to jointly compute a function on their private inputs [48] without revealing the inputs to each other. It allows for collaborative data analysis and computation while maintaining data privacy. However the critics mentioned that SMPC protocols can be computationally expensive, especially for large-scale computations involving multiple parties. Also the security of MPC relies on trust assumptions among participating parties and the correctness of the underlying cryptographic protocols.

Some work also proposed Zero-knowledge proof of knowledge [49] to maintain the privacy of transactions. Zero-knowledge proof is a mathematical technique to verify the truthfulness of information without revealing the information itself, but the technology receives critics that the protocol is susceptible to cyber-attack when the intruder behaves like an actual user. Moreover, the protocol has a significant problem of high computation power that limits its usage, especially when applying it to the MIoT domain. In recent years, there has been a growing body of research that leverages differential privacy as a mechanism for designing Privacy Enhancing Technologies (PETs) in the context of IoT.

Differential privacy enables the analysis of complete user behavior datasets without disclosing individuals' private information. This technique involves introducing noise into the dataset, ensuring the desired level of privacy protection under this framework. Notably, Google LLC utilizes differential privacy to collect Chrome usage data from users while upholding their privacy [50]. Darwish et al. [51] proposed an architecture for safeguarding the privacy of IoT healthcare systems. The architecture incorporates pseudonymization and anonymization techniques to protect sensitive information of patients. To provide an additional layer of protection, a differential privacy analyzer is employed to assess whether the

query results meet the requirements of differential privacy. In a similar vein, Xu et al. [52] introduced a privacy-preserving framework that leverages the differential privacy mechanism at the edge of the IoT network. By employing differential privacy, sensitive data leakage is minimized before transmitting the data to the cloud for further analysis. This approach ensures data privacy while preserving the utility of the data for subsequent analysis. By utilizing differential privacy, these studies demonstrate the efficacy of this mechanism in preserving data privacy within IoT applications. The incorporation of differential privacy techniques enables the analysis of sensitive data while maintaining a strong level of privacy protection. Some of the authors combine the concept of differential privacy with other mechanism such as access control mechanism to provide more fine grinned control of the data. Likewise, Fernández et al. [53] proposed a category-based access control with privacy policies and differential privacy. When people conformed to what the privacy policies specified, the system would utilize the differential privacy mechanism over the personal data before transmitting the data to the authorized people. Jung and Park [54] introduced an access control scheme incorporated with the differential privacy, which allowed the data owners to adjust the accuracy of the query results by inserting noise determined by means of game theory. To embrace new technologies, many researchers also leverage blockchain as a new paradigm to address security and privacy issues [55]. Blockchain is considered a decentralized distributed ledger that store and keep records in an immutable fashion [56] with the capability to digitize transaction securely and efficiently. Since we have also used differential privacy in our proposed framework, we will explain this concept in detail in the following subsection.

2.5 Differential Privacy

Differential privacy is a widely recognized technique for preserving privacy that offers robust assurances that the output of a data analysis algorithm does not disclose any sensitive information about individuals. In this section, we will introduce the foundational concepts

of differential privacy. Let's consider a database denoted as x, which contains records from a universal set of data types X. In this context, x can be represented as $x \in N^{|\chi|}$, where x_i represents the number of elements in the database x of type $i \in \chi$. Here, N represents the set of all non-negative integers.

The measurement of the distance between two databases, x and y, is quantified using the ℓ_1 norm, denoted as $|x-y|_1$, which is given by Equation 29:

$$\ell_1 \text{ norm} = |x-y|_1 \tag{7}$$

To ensure privacy in the context of differential privacy, techniques such as Laplace noise, Gaussian noise, and Exponential noise are commonly used. These noise mechanisms obscure sensitive information contained in the data, providing privacy guarantees.

Definition 3 (Differential Privacy) A randomized algorithm M, defined on the domain $N^{|\chi|}$, is classified as differentially private if, for any subset S in the range of M and for all $x, y \in N^{|\chi|}$ satisfying $\|x-y\|_1 \leq 1$, the following inequality holds:

$$P(M(x) \in S) \leq e^{\varepsilon} P(M(y) \in S) + \delta$$

When δ is equal to 0, the algorithm M is said to possess ε-differential privacy.

Laplace Noise Laplace noise is well suited for scenarios where the sensitivity of the query is known as it allows for precise control over privacy budget allocation. The sensitivity of a query refers to the maximum amount by which the query result can change when the data of a single individual is modified or removed from the dataset. Within the framework of differential privacy, utility refers to the usefulness or accuracy of the query result or data analysis obtained while ensuring the preservation of privacy guarantees.

Definition 4 (ℓ_1-Sensitivity) The ℓ_1 sensitivity of a function f can be expressed as:

$$\Delta f = \max_{x,y} \|f(x) - f(y)\|_1 \tag{8}$$

Definition 4 (Laplace Mechanism) The Laplace mechanism is defined for any function

f as:

$$f'(x) = f(x) + \text{Laplace}\left(\frac{\Delta f}{\varepsilon}\right) \tag{9}$$

A stronger degree of privacy is achieved with a smaller value of ε. As ε approaches zero, the level of noise added to the query result increases, making it more challenging to differentiate the impact of an individual's data on the final output. On the other hand, a larger value of ε allows for less noise and may provide a relatively weaker level of privacy. The choice of ε depends on the desired trade-off between privacy and utility in a specific context.

Definition 5 (ℓ_2- sensitivity) The l2 sensitivity of a function f can be expressed as:

$$\Delta_2 f = \max_{x,y} \|f(x) - f(y)\|_2 \tag{10}$$

Guassian Noise

Additionally, Gaussian noise is useful when the sensitivity of query is not precisely known or when the data distribution is assumed to be Gaussian, also Gaussian noise adds noise proportional to the ℓ_2- sensitivity of the query.

Definition 5 (Gaussian Mechanism) The Gaussian mechanism is defined for any function f as:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{11}$$

The standard deviation (σ) is a measure of the dispersion or spread of the Gaussian distribution. It determines the width of the bell-shaped curve. A larger value of (σ) indicates a wider spread of the distribution, while a smaller value indicates a narrower spread. The mean (μ) represents the center or average of the Gaussian distribution. It determines the location of the peak or the highest point of the bell-shaped curve. The mean also represents the expected value or average value of the random variable that follows the Gaussian distribution.

Theorem1 The Expected Estimation Error (EEE) of the Laplace mechanism exhibits a decreasing trend as the privacy budget ε increases.

Proof: The probability density function of Laplace distribution can be expressed as:

$$f(x) = \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right) \tag{12}$$

whereas b is equal to $b = \frac{\Delta f}{\varepsilon}$. Then

$$\text{EEE} = \int_{-\infty}^{\infty} \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right) |x| \, dx \tag{13}$$

$$\text{EEE} = -\int_{-\infty}^{0} \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right) |x| \, dx + \int_{0}^{\infty} \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right) |x| \, dx \tag{14}$$

Solving equation 14will gives us

$$b = \frac{\Delta f}{\varepsilon} \tag{15}$$

Therefore,

$$\frac{dEEE}{d\varepsilon} = -\frac{\Delta f}{\varepsilon^2} < 0 \tag{16}$$

Equation 16shows that EEE of Laplace mechanism decreases as we increase the privacy budget (ε).

Corollary 1 The modulus of characteristic function $\phi(t)$ increases as we increase the (ε).

Proof: The characteristic function of Laplace mechanism is given by

$$\phi(t) = \left(\frac{\varepsilon^2}{\varepsilon^2 + \Delta f^2 t^2}\right) \tag{17}$$

Where as modulus is

$$|\phi(t)| = \left(\frac{\varepsilon^2}{\varepsilon^2 + \Delta f^2 t^2}\right) \tag{18}$$

Therefore, the derivative of $(|\phi(t)|)$ with respect to (ε) is equal to

$$\frac{d}{d\varepsilon}|\phi(t)| = \frac{2\varepsilon \Delta f^2 t^2}{(\varepsilon^2 + \Delta f^2 t^2)^2} \geq 0 \tag{19}$$

This equation 19shows that as the modulus of characteristic function increases privacy budget (ε) of Laplace mechanism increases.

Theorem2 The Expected Estimation Error (EEE) of Gaussian mechanism decreases as the privacy budget (ε) increases.

Proof: The probability density function of Gaussian distribution is given by

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{20}$$

The value of σ) is often chosen based on the desired privacy level or the sensitivity of the function being computed. A larger value of (σ) corresponds to a higher amount of noise and may provide stronger privacy guarantees but can also lead to more distortion in the query result. On the other hand, a smaller value of (σ) reduces the amount of noise but may provide weaker privacy guarantees.

$$\text{EEE} = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right) |x| dx \tag{21}$$

Integrating equation 21yields

$$\text{EEE} = \frac{\sqrt{2}\sigma}{\sqrt{\pi}} = \frac{2\Delta_2 f\sqrt{\ln\left(\frac{1.25}{\sigma}\right)}}{\varepsilon\sqrt{\pi}} \tag{22}$$

Therefore,

$$\frac{dEEE}{d\varepsilon} = \frac{2\Delta_2 f\sqrt{\ln\left(\frac{1.25}{\sigma}\right)}}{\varepsilon^2\sqrt{\pi}} < 0 \tag{23}$$

EEE of Gaussian mechanism decreases as the privacy budget (ε) increases.

Corollary 2 The modulus of characteristic function of Gaussian mechanism $\phi(t)$ decreases as we increase the (ε) privacy budget

Proof:

$$\phi(t) = \exp(\frac{-\Delta_2 f^2 t^2 \ln\left(\frac{1.25}{\sigma}\right)}{\varepsilon^2} \tag{24}$$

The modulus function is given by

$$|\phi(t)| = \exp(\frac{-\Delta_2 f^2 t^2 \ln\left(\frac{1.25}{\sigma}\right)}{\varepsilon^2} \tag{25}$$

Therefore, the derivative of $(|\phi(t)|)$ with respect to (ε) is equal to

$$\frac{d}{d\varepsilon}|\phi(t)| = (\frac{2\Delta_2 f^2 t^2 \ln\left(\frac{1.25}{\sigma}\right)}{\varepsilon^3} \exp(\frac{-\Delta_2 f^2 t^2 \ln\left(\frac{1.25}{\sigma}\right)}{\varepsilon^2} \geq 0 \tag{26}$$

This equation 26clearly shows that modulus of characteristic function of Gaussian mechanism increase as the privacy budget (ε) increases.

Exponential Noise Exponential noise serves as a fundamental component in the realm of differential privacy, an important privacy-preserving concept in data analysis. Exponential noise is commonly employed as a mechanism to add random perturbations to sensitive data, thereby safeguarding individual privacy while allowing statistical analysis. In the context of differential privacy, exponential noise is derived from the exponential distribution. This distribution is characterized by its rate parameter, denoted as λ, where smaller values of λ correspond to higher noise intensity. By adding exponential noise to sensitive data, such as individual records or query results, the privacy of individuals is protected, as the added noise obscures specific details about individuals while still preserving the overall statistical properties of the data.

Definition 6 (Exponential Mechanism) The mathematical equation for adding exponential noise as a differential privacy mechanism is given by:

$$\tilde{x} = x + \text{Exponential}\left(\frac{1}{\lambda}\right) \tag{27}$$

where $\tilde{x}$ represents the perturbed or noisy value of the original data x. The term Exponential $\left(\frac{1}{\lambda}\right)$ denotes the exponential distribution used to generate the random noise and the rate parameter λ controls the scale of the noise.

CHAPTER III

LITERATURE REVIEW

In this chapter, we provide a comprehensive literature review, analyzing the existing research and solutions related to privacy preservation while integrating Medical Internet of things (MIoT) devices with blockchain. We critically evaluate the strengths and weaknesses of prior approaches, identify research gaps, and highlight the research directions that need to be explored.

Furthermore, We identify the existing gaps and challenges in preserving privacy when integrating MIoT devices with blockchain. By reviewing the current literature, we identify the limitations of existing techniques and the need for an innovative approach. Our goal is to propose a novel solution that addresses the privacy concerns while ensuring the benefits of blockchain technology in the context of MIoT devices.

Overall, this chapter serves as a foundation for understanding the existing literature related to blockchain, and privacy preservation issues in the context of MIoT devices. It sets the stage for presenting our proposed solution in the subsequent chapters, aimed at addressing the identified privacy challenges and contributing to the advancement of secure and privacy-preserving integration of MIoT devices with blockchain technology.

3.1 Blockchain based Applications in E-Health

Although, the use of blockchain technology has generated significant interest in E-Health applications but the E-Health ecosystem presents unique privacy challenges due to the sensitive nature of the data that needs to be stored and shared with various stakeholders. The studies conducted in [57] and [58] provide a comprehensive review and analysis of current research on blockchain applications in the healthcare domain. The primary objective of these work is to identify the potential use cases for blockchain technology in the healthcare

sector and to shed light on the associated challenges that need to be addressed. Some of the work also focus on cloud-based E-Health scenarios, [59] discussing the potential application of blockchain to enhance security and privacy aspects. In this cloud based architecture, the authors emphasize the need for off-chain storage mechanisms that allow medical data to be erased under certain circumstances to comply with privacy laws, such as GDPR's Article 17 ("Right to be forgotten"). However,cloud is usually considered as a semi-trusted infrastructure that may potentially lead to privacy leakage of personal information due to inside malicious attacks or the high end servers being compromised. Moreover, some of the authors proposed polynomial-based blockchain structure [60] to address the security and privacy concerns in Electronic health record system. A polynomial-based blockchain structure refers to an approach where the blockchain data structure is built upon polynomial functions instead of the traditional linked list of blocks. In this approach, the blockchain data is represented using polynomial functions rather than the conventional chained blocks. However the critics mentioned that the computations involved in encoding the blockchain data into polynomial functions and performing computation is more complex compared to the traditional linked list-based structures. Additionally, [61] explores the use of Intel SGX [62] and blockchain to implement a patient-centric personal health data management system with accountability and decentralization in E-Health scenarios. Intel SGX is considered a hardware-based Trusted Execution Environment (TEE), providing a secure and isolated execution environment within the host system. However, the additional security measures and isolation provided by Intel SGX can introduce performance overhead, particularly for computationally intensive blockchain operations, such as consensus algorithms, smart contract execution, and cryptographic operations. [63] introduces a framework called Ancile, which utilizes smart contracts in an Ethereum-based blockchain to store hashes of data references and employs proxy re-encryption to securely share EHRs, focusing on preserving the privacy of medical data while considering security, interoperability, and efficiency aspects for accessing medical records. However, Ethereum, as a public blockchain,

faces scalability issues due to the increasing number of transactions and the limited block size and block time. Also the proxy re-encryption technique requires the management of multiple keys, including the data owner's private key, the proxy's re-encryption key, and the recipient's public key.

3.2 Blockchain-Based PHR Sharing With Security and Privacy

Various schemes have been proposed to construct blockchain-based Personal Health Record (PHR) sharing systems with security and privacy using cryptographic algorithms. For example Li et al. [64] proposed a blockchain-based medical data storage system that focused on ensuring data integrity and factuality. They employed blended encryption algorithms to protect patients' privacy. However, this approach resulted in considerable storage wastage on the blockchain. Zhang and Lin [65] introduced a secure and privacy-aware PHR-sharing scheme based on blockchain to enhance disease diagnosis. Their scheme utilized searchable keyword encryption for the PHR sharing protocol but only supported single keyword search. Liu et al. [66] proposed a blockchain-based Electronic Medical Records (EMRs)-sharing scheme with privacy preservation. Their approach combined the CP-ABE (Ciphertext-Policy Attribute-Based Encryption) algorithm and content extraction signature to protect security and privacy. Wang et al. [67] developed a blockchain-based and cloud-assisted secure Electronic Health Records (EHRs)-sharing system. They employed public-key encryption with searchable keyword and proxy re-encryption techniques. This scheme aimed to enhance security and privacy in EHR sharing. Liu [68] designed a medical data-sharing scheme using a private blockchain instead of cloud storage. However, the private blockchain implementation could hinder communication and collaboration between different medical institutions. In [69], an efficient EMR-sharing scheme using cloud storage with a private blockchain was introduced. This scheme adopted multiple ABE (Attribute-Based Encryption) to provide precise control over accessing PHRs. However, the mentioned ABE-based PHR-sharing schemes lacked support for data retrieval.

3.3 Blockchain-Based PHR Sharing With Access Control

Effective control and personalized sharing of Personal Health Records (PHRs) by patients is a crucial issue. Several approaches have been proposed to address this concern. A patient-centric access model [70] was introduced to empower patients with control over their EHR data. The model incorporated secure multiparty computing to allow untrusted third parties to perform calculations on patients' health data while preserving privacy. However, it did not offer a specific algorithm for implementation. Zaghloul et al. [71] designed a smart contract-based health data management scheme to enable patients to autonomously manage and share their EHRs. This approach aimed to reduce patients' reliance on data generation organizations and provide them with greater freedom in utilizing their PHRs. In [72], a blockchain-based hospital network was proposed to facilitate distributed mutual authentication of patients. This network securely recorded medical data across geographically diverse hospitals and facilitated convenient migration of patients to other federal hospitals. Existing open-source blockchain platforms were utilized to develop PHR-sharing frameworks that provide patients with convenient access control. Dagher et al. [73] presented a secure and interoperable framework based on blockchain for efficient user access to EMRs using Ethereum and smart contracts. However, the scalability of searching for different smart contracts could become challenging as the number of users increased. Li et al. [74] leveraged edge computing devices and combined Amazon Web Servers with Ethereum to establish a secure health data-sharing framework. However, this scheme may face limitations in sustaining a real home environment based on Ethereum. Zhuang et al. [75] proposed a programmable data exchange protocol implemented through smart contracts on the Ethereum blockchain to protect data security without compromising patients' privacy. This approach aimed to give patients control over their PHR data but had limited scalability.

3.4 Blockchain-Based Differential Privacy Preserving Framework

Researchers have also explored the integration of differential privacy techniques with blockchain to safeguard sensitive information. One approach involves introducing noise into the data to prevent the identification of individual transactions. Yang et al. [76] proposed a blockchain data-sharing system in a federated cloud that incorporated a differential privacy mechanism. Their approach utilized the Hyperledger Fabric blockchain and focused on four query functions (sum, average, max, and min) using Laplace noise in their evaluation. However, their study did not consider the privacy-utility trade-off in their simulation. Similarly, Z. Qian et al. [77] presented a differential privacy-preserving framework for smart contracts in blockchain. The framework employed an algorithm to add noise to the smart contract data, making it challenging to link the smart contracts to specific individuals. The results demonstrated the effectiveness of the framework in preserving smart contract privacy while maintaining blockchain security and transparency. Nevertheless, the introduction of noise to smart contracts can reduce data accuracy, which can impact the analysis performed by the smart contract. The study did not address techniques to mitigate the accuracy issues in their simulation work. Raisaro et al. [78] proposed a privacy-preserving blockchain protocol that combined homomorphic encryption with differential privacy. However, the combination of performing operations on encrypted data and injecting noise for privacy preservation can significantly slow down the data analysis process. In [79], a framework for privacy-preserving data aggregation in the Internet of Things (MIoT) using blockchain and differential privacy was proposed. The study employed a hierarchical aggregation scheme and a differential privacy mechanism to ensure the privacy and security of user data. Similarly, in [80], a privacy-preserving data collection and sharing framework for MIoT in healthcare was introduced. The framework utilized blockchain and differential privacy techniques, employing a differential privacy algorithm to protect patient data privacy while enabling healthcare providers to access and share data for research purposes.

Overall, these studies highlight the potential of integrating differential privacy with

blockchain to enhance privacy protection in various domains. However, challenges such as the privacy-utility trade-off, data accuracy, and performance impact need to be catered. In this regard, further research is needed to develop comprehensive and practical models that address the specific requirements and challenges of PHR sharing on the blockchain while ensuring security, privacy, and scalability. Considering these factors, this research aims to fill this gap by introducing a privacy-preserving framework that empowers end users with complete control and the right to tune the performance parameters of added noise to their data determining the trade-off between privacy and utility. Our proposed DPP framework will first identify the level of privacy (low, medium, high) and utility as desired by the data owner, thus shifting the control from data consumer to data owner. Additionally, considering the resource limitations of MIoT devices, our proposed framework incorporates a lightweight consensus protocol and a computationally efficient cryptographic method in our simulation to illuminate the path for the real-world implementation of MIoT sensors with the blockchain.

CHAPTER IV

BLOCKCHAIN BASED SYSTEM MODEL FOR PATIENT-CENTRIC AND PRIVACY PRESERVING PHR SHARING

Our main goal is to provide a secure and private framework for MIoT devices that allows data to be transferred securely while respecting the data owner's privacy preferences. These preferences include specifying how long the data should be retained, for what purpose it can be used, and whether it can be shared with third parties. All these specifications must meet the user's consent and be transmitted securely. To achieve this goal, we have proposed a framework that combines service-oriented layers and a secure private transaction workflow layer to ensure that our data is secure and meets the user's consent preferences.

In this chapter, we introduce the overall architecture of the system model, which includes both a EPIoT framework and a DPP framework. We also identify the key modules for each layer that make up the complete system. This integration approach aims to improve the overall security and privacy of individuals' data when conducting statistical analysis.

4.1 System Architecture

In this section, we introduce the overall architecture of the proposed blockchain based framework as show in Fig. 4. The key idea is that the data owner can leverage on blockchain for privacy compliance before their data are sent to consumers. We have proposed two frameworks: EPIoT framerork and DPP framework to model our smart environment. EPIoT framework employs service oriented layers approach which consists of mainly registration contract, authentication contract, and privacy enforcement contract. Every contract works independently of each other and provides a flexible architecture for MIoT eco-system. The

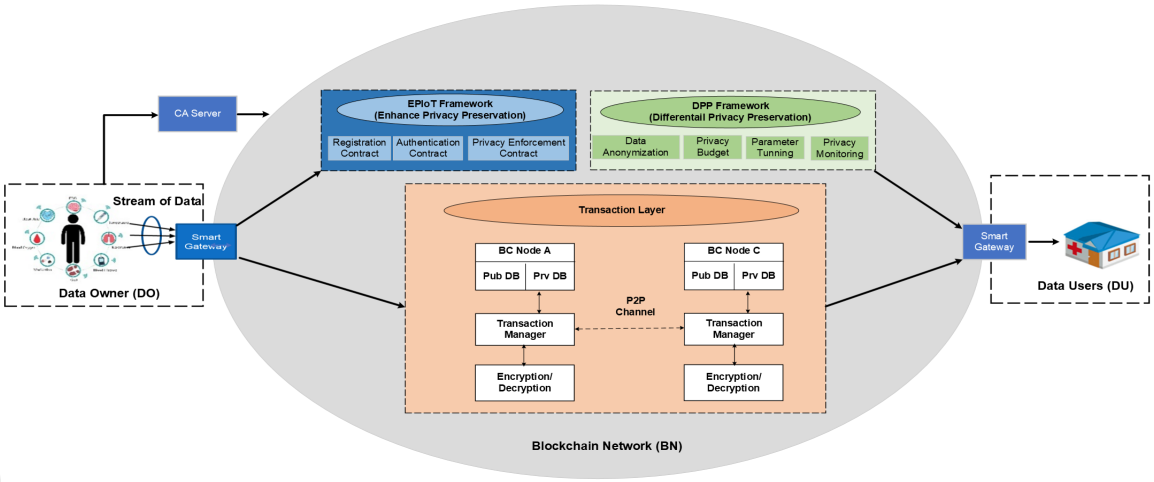

Figure 4: System model

registration layer focuses on the initial setup and registration of MIoT devices within the network followed by authentication layer which will be responsible for verifying the identity and authenticity of MIoT devices and smart gateways (SG) accessing the network. Privacy enforcement layer is the vital layer that is mainly responsible for enforcing the privacy of MIoT user by transferring control to the end user to limit how the data can be retrieved from the MIoT analytic process. This layer will ensure that consumer policy will abide by the rules and regulations as set by the MIoT user in his/ her privacy preference via privacy smart contract.

In DPP framework, we have introduced a novel concept of privacy levels, which are adjustable by data owners as low, medium, and high. This flexibility addresses the varying privacy requirements of different applications and empowers data owners to customize the level of privacy preservation according to their specific needs. This framework is further comprised of data anonymization, privacy budget, parameter tuning and privacy monitoring module. Data anonymization module will anonymize the data in a way that it will preserves privacy while still allowing for meaningful analysis. Similarly, privacy budget module will set the amount of privacy loss that will allowed in any given data analysis. Parameter tuning module will be tuned to optimize the trade-off between data privacy and data utility.

Privacy monitoring module module is mainly responsible to ensure that the level of privacy is maintained over time. This includes auditing and monitoring of data access and usage as well as periodic assessment of the effectiveness of Laplace noise, Gaussian noise and Exponential noise while protecting privacy.

More precisely, we model a smart environment at the data owner side in which set of MIoT sensors are connected via smart gateways before their data is propagated to blockchain network. Privacy Enforcement module and Differential privacy module are mainly responsible for providing end to end private by-design framework empowering the data owner by shifting the control from data consumer who perform data analysis.

In this chapter, we first explain the key components and entities that are mainly responsible for constituting this entire framework.

- *MIoT devices*: MIoT are the sensors that generate data in the MIoT network. They can be sensors, actuators or, any kind of device that can interact with the physical environment. Our proposed system model comprises of sensors hereafter referred to as medical MIoT sensors (MIoT) which sense the vital signs of the patients or data owners.

- Data owners (DOs): Dos are the patients who want to share their medical record data with authorized data users over the consortium blockchain network via smart gateways.

- *Smart gateways (SG)*: SGs are the first point of contact with the blockchain network for sharing DO MIoT medical data. In addition to performing their normal gateway functionality, they act as a first line of defense to preserve the privacy of MIoT devices by limiting the amount of data that is transmitted to the blockchain network

- *Certificate Authority (CA) Server*: Certificate Authority CA is an integral part of our proposed architecture which generates signatures, keys, and certificates and is a fully trusted entity. CA is mainly responsible for the registration of MIoT sensors and all

nodes in the network. Furthermore, it provides credential validation, and signature verification functionality as well.

- *Data Users (DUs)*: DUs are the data requesters such as doctors, clinical laboratories, pharmacists, or research institutions who may use the patient health data either for treatment of disease or do some research analysis over it.

- *Blockchain network (BN)*: BN is considered as a backbone of this proposed privacy-preserved framework. In our proposed system we leverage on Quorum blockchain which natively supports public and private transactions. Classification of public and private transactions has been done at the stream level generated by the MIoT device. Quorum blockchain entails two separate databases to handle these public and private transactions. Every blockchain is connected to its associated transaction manager and encryption and decryption module. Both the module are mainly responsible for maintaining the privacy of MIoT transactions by sending the private data to the recipient BC node while the other intermediary nodes simply skip the transaction as it is not meant for them.

- Privacy Enforcement layer: Privacy Enforcement layer is mainly comprises of service-oriented layer working independently of each other to avoid any complexity of a system and is composed mainly of the Registration contract, Authentication contract, Privacy enforcement contract.

- Registration Contract is mainly responsible for registering MIoT devices and smart gateways to a blockchain network. This layer will provide an automated process for the registration of new MIoT devices and smart gateways and securely on-board the network via registration smart contract. Registration layer will provide an additional secure trust between the connecting device and the network which they want to connect and communicate by leveraging the innate features of CA. Our proposed

framework will provide an explicit solution for resource constrain MIoT devices and establish a trusted relationship with smart gateway and blockchain nodes.

- Authentication Contract assures and authenticate a valid MIoT device and smart gateway to get connected with the block-chain network via authentication smart contract. In our proposed framework the process is initiated by establishing a secure TLS connection between MIoT and smart gateway followed by another secure TLS session between smart gateway and blockchain node. At each step the MIoT device and smart gateway authenticate each other through the nonce value generated during the TLS session and subsequently encrypted the nonce value and certificates using the session keys allowing only the intended MIoT users and smart-gateways to authenticate each other. After each MIoT device successfully validates and verifies the blockchain node which it wants to communicate, a trusted relationship is established among the MIoT node, smart gateway and blockchain node.

- Privacy enforcement Contract is the vital layer that is mainly responsible for enforcing the privacy of MIoT user by transferring control to the end user to limit how the data can be retrieved from the MIoT analytic process. This layer will ensure that consumer policy will abide by the rules and regulations as set by the MIoT user in his/her privacy preference via smart contract. In our proposed system model, smart gateway will first analyze the collected MIoT data and will process and forward the data as per the rules set by the data owner. If the gateway encounters a new or unverified privacy preference, it will provoke a privacy compliance check to cross verify that the consumer privacy policy matches with the privacy policy as set by the data owner or not. Finally, the result of the compliance check will be uploaded to the blockchain for a subsequent audit purpose. Once the privacy contract is validated by the majority of nodes in a blockchain network, encrypted data will then be transmitted to the recipient node.

- *Differential privacy Layer*: Differential privacy is the key layer that is mainly responsible for catering to the privacy of sensitive data by implementing differential privacy techniques. It involves adding a noise mechanism to the data in a way that makes it difficult to identify specific individuals while still preserving the overall statistical properties of data. The key components of a differential privacy layer as shown in Fig. 4 typically include the following: (1) Data anonymization: The module must anonymize the data in a way that preserves privacy while still allowing for meaningful analysis. This can be done through techniques such as adding noise to the data, or by aggregating data in a way that removes individual identifying information. (2) Privacy budget: The module must have a privacy budget, which is the amount of privacy loss that is allowed in any given data analysis. The privacy budget must be set based on the level of privacy protection required and the sensitivity of the data being analyzed. (3) Parameter tuning: The module must be tuned to optimize the trade-off between data privacy and data utility. This involves selecting appropriate values for the privacy budget, the noise added to the data, and other parameters that affect the privacy and utility of the data. Privacy preservation in MIoT-based blockchain is a crucial aspect of MIoT security. (4) Privacy Monitoring: This module is mainly responsible to ensure that the level of privacy is maintained over time. This includes auditing and monitoring of data access and usage as well as periodic assessment of the effectiveness of Laplace noise, Gaussian or Exponential noise while protecting privacy.

- *Transaction Layer*: The Transaction layer will handle both public and private transactions. Public transactions are those transactions that will be broadcasted to all nodes in the network and will be processed similarly as done by Ethereum blockchain while private transactions are accessible to those blockchain nodes that are a part of the transaction while the rest of the blockchain nodes will simply skip this transaction as it is not designated for them.

Transaction Layer is mainly composed of:

- Public and Private database: This database entails two separate virtual databases to accommodate public and private transactions. Public transactions are stored in a public database and their transaction flow is similar to Ethereum BC network by broadcasting the information to all nodes in the network while private transactions are stored in a private database and their flows involve the addition of corresponding transaction managers as well as encryption and decryption module allowing the encrypted transaction to remain private between the sender and the recipient node. Public transactions can be specially beneficial in MIoT domain where devices like wearable sensors or medical implants continuously collect health monitoring data. Such data can be used by healthcare providers or researchers for population health analysis, disease surveillance, or public health planning. Similarly, private transactions can be used for secure communication between healthcare providers and patients, preserving the confidentiality of personal health information related to prescriptions, such as dosage, frequency, or specific medications.

- Transaction Manger: This module act as a gateway by establishing P2P connection with other nodes transaction managers. It provides an interface to the encryption/ decryption module to provide a confidential feature to the private transactions

- Encryption and Decryption Module: This module encrypts the data and enables to store all sensitive information in a fully isolated mode. It act as a virtual hardware security module (HSM).

The main objective of this proposed privacy preserved framework is to empower data owners to control the data according to his/her own need and requirements. The data owner can leverage blockchain for setting the privacy preference and privacy compliance check before the data is sent to other consumers for extracting meaningful insight from the information being shared.

CHAPTER V

ENHANCED PRIVACY PRESERVATION BLOCKCHAIN BASED FRAMEWORK

IoT data privacy is a complex and multifaceted issue that requires comprehensive solutions to address the entire data life-cycle. In general, a privacy policy is specified by the consumer to state which personal data it will collect from the individual. However, most policies are based on an opt-out strategy where the end user must abide by the set rules as defined by the consumer. This lack of flexibility often forces the data owner to accept the data consumer's policies, especially in critical services related to MIoT.

To resolve this issue, we propose a framework that implements privacy preferences set by the data owner in a more secure and reliable manner. This mechanism shifts control from the data consumer to the data owner, enabling the owner to enforce their privacy preferences on the delivered data.

We then analyzed the performance of our proposed framework in terms of throughput and latency by deploying three different consensus protocols: RAFT, IBFT, and PoA. By investigating the efficacy and performance of the proposed approach, we aim to contribute to the development of privacy-enhancing solutions for medical MIoT devices. This will foster trust among patients, healthcare providers, and stakeholders in the evolving landscape of healthcare data management.

Lastly, we discuss the security assurance provided by each layer of our proposed framework using AVISPA, a verification tool.

5.1 Scheme Construction

In this section, we introduce the overall architecture of the EPIoT based framework articulated with blockchain as shown in Fig. 5. Our proposed framework is the agglomeration of service-oriented layers and a secure private transaction work-flow layer. The following summarizes the key role of various elements that constitute this framework.

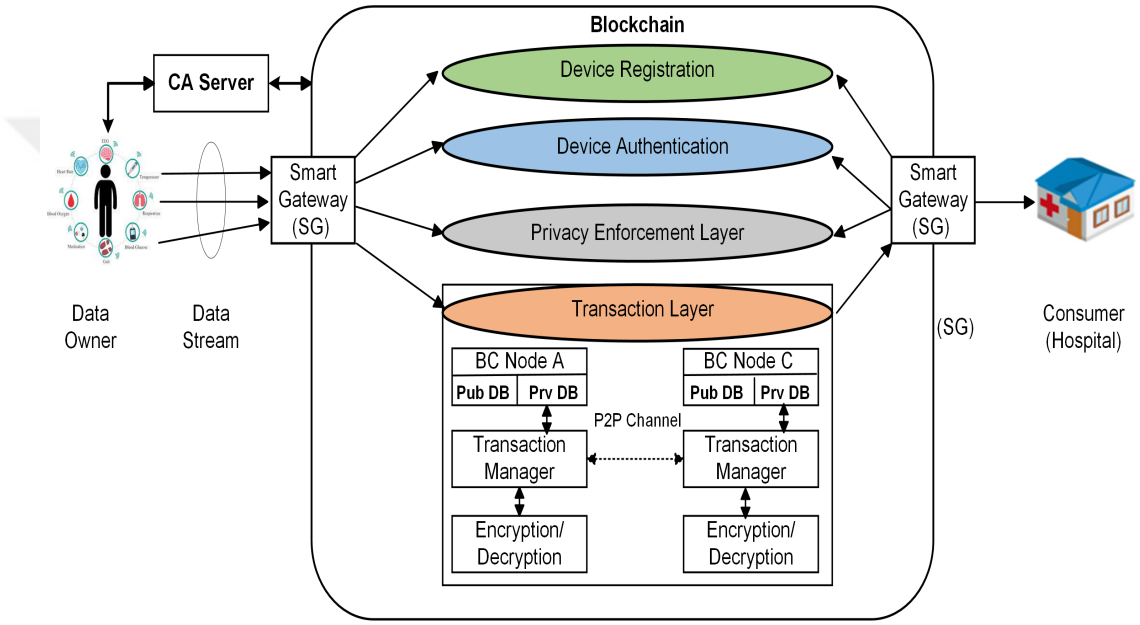

Figure 5: EPIoT based System Model

5.2 Registration Layer

This layer is mainly responsible for the registration of all MIoT devices, and smart gateways that want to become a part of a system via registration smart contract. Each MIoT device needs to be registered with CA and then it will be sub sequentially verified and validated by the smart gateway through the certificates issued by CA as shown in Fig. 5. Once the MIoT device is registered, its credential will be uploaded to the blockchain node. This process ensures that only the authorized MIoT node and smart gateway become part of a blockchain network. The local registration process for an MIoT node will follow Algorithm

1 to complete the device registration process. For every transaction received by SG, it verifies if the transaction is initiated by the valid MIoT device or not. If the MIoT device is registered, then Algorithm 2 will be used for verification purposes. The transaction flow for registering MIoT devices in our proposed framework is shown in Fig. 6.

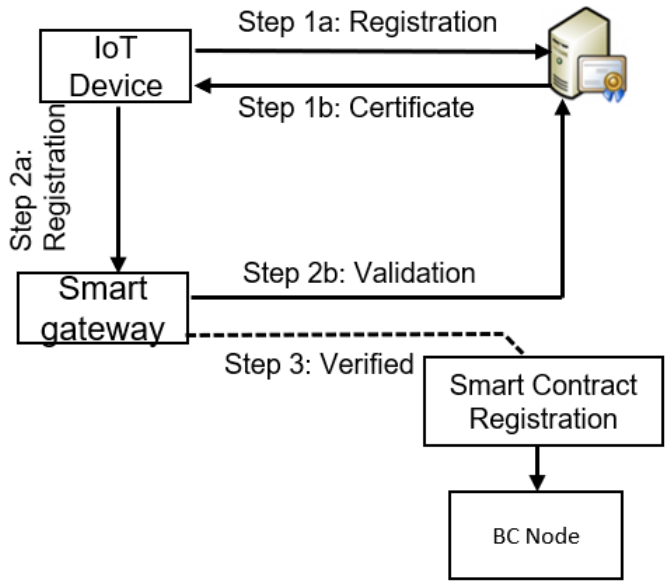

Figure 6: MIoT device registration phase

Algorithm 1 Device Registration

Input :*Device id* $d_{id} = (d1, d2 \ldots\ldots dn)$
Output :*MIoT* $d_{id}.SG_{id}$
Set MIoTdevice$_{id} \leftarrow d_{id}$
Set SGdevice$_{id} \leftarrow SGd_{id}$
Request Sign & certificate of $d_{id} \rightarrow CA$
if d_{id} Sign and Certificate **then**
    $d_{id} \rightarrow SG(Sign(d_{id}), d_{id})$
    if $SG(Sign(d_{id}))$ **then**
        return MIoTdevice d_{id}. SG_{id}
    else
        d_{id} *sign or certificate is not valid*
else
    Request rejected

The following steps will completely illustrate the registration process while registering MIOT devices to our proposed blockchain network.

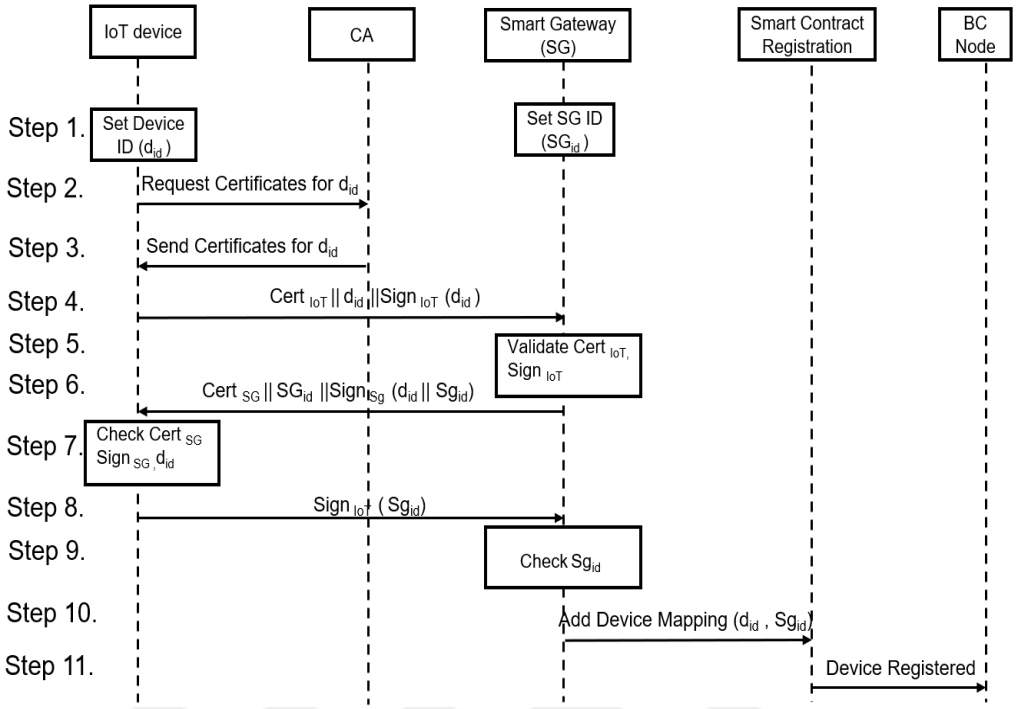

Figure 7: MIoT device registration transaction flow

- Step 1: First the MIoT device will set its device ID (d_{id}) followed by SG device ID (SG_{id})

- Step 2 & Step 3: MIoT device will request a certificate from the CA. CA will issue a device certificate against each MIoT device id to help ensure that only legitimate MIoT device gets a certificate issued by the CA and it can be validated.

- Step 4: After receiving a certificate, the MIoT device will send its certificate along with the device id and digitally sign the device id with its private key to the SG.

- Step 5: MIoT certificate is validated by SG from CA as shown in Fig. 6 and check the integrity of (d_{id}) based on the provided signature.

- Step 6: Once they are validated, SG responds back to MIoT device by sending its certificate and node identifier (SG_{id}) along with its signature.

- Step 7: MIoT device after receiving the SG certificate and validating its signature,

Algorithm 2 Device Verification

Input : *Requested MIoT* $d_{id}.SG_{id}$
Output : *True or False*;
if (MIoT $d_{id}.SG_{id}$) $\doteq$ SG **then**
    if $Sign(SG)$ *and* ($Sign(d_{id})$is verified) **then**
        return True
    else
        return False
else
    return False
end

guarantees that both SG and MIoT node are trustworthy devices and they are communicating with each other only.

- Step 8: MIoT node will send the device id of SG as received in step 6 and is digitally signed towards SG.
- Step 9: Based on the signature of MIoT node, SG will examine and check the integrity of message (SG_{id}) ensuring that SG id is not tempered by one in the network.
- Step 10 & Step 11: SG will make a call to smart contract registration and through add device mapping function both a legitimate MIoT node and SG will be linked together (d_{id}, SG_{id}) and the registration ID for the device becomes $(MIoTd_{id}.SG_{id})$ which is logged on the blockchain and will be used for subsequent later transactions.

5.3 Authentication Layer

This layer is mainly responsible for authorizing the legitimate MIoT device to become a part of a blockchain network via an authentication scheme. Mostly MIoT system rely on centralized architecture and third-party servers such as open authorization (OAuth) protocol to get authenticated but this approach has a serious drawback of a single point of failure and is prone to cyber-attacks, ultimately resulting in breaching the privacy of the end user. In our proposed framework a novel scheme is proposed by establishing a TLS connection between MIoT device and SG followed by another TLS session between SG and BC node.

The transaction flow for authenticating MIoT devices in our proposed framework is shown in Fig. 8 for secure authentication.

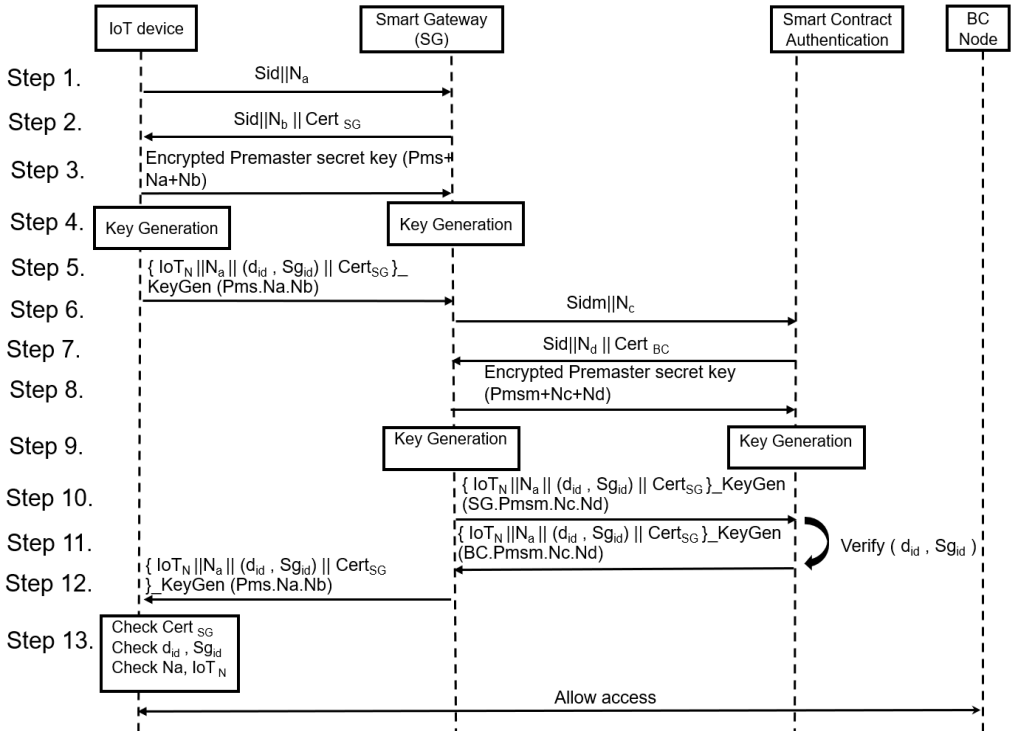

Figure 8: MIoT device authentication transaction flow

- Step 1: First the MIoT device will pick a random nonce value (N_a) along with session id (S_{id}) and initiates the authentication process by establishing a TLS handshake with SG.

- Step 2: The SG will respond to this message by generating another nonce value (N_b) along with session id (S_{id}) and the SG certificate issued by the CA. MIoT device will provisionally authenticate SG during this handshake process with the SG unauthenticated server certificate.

- Step 3: MIoT device will create a random pre-master secret (Pms) key and encrypts it with the public key from the SG certificate, transmitting encrypting Pms to the SG.

- Step 4: After receiving the Pms, both MIoT device and SG will generate master secret key along with the session keys based on the Pms.
- Step 5: Once a secure channel is established between the MIoT device and SG, MIoT device will generate another nonce value $(MIoT_N)$ concatenating it with (N_a), $(MIoTd_{id}.SG_{id})$ and SG certificate and encrypt it with the session key generated previously during the TLS session.
- Step 6: Before SG communicate with the authentication smart contract, another TLS handshake is established first by sending the session id (S_{idm}) along with the randomly generated nonce (N_c).
- Step 7: Smart contract authentication will respond back to SG via random nonce value (N_d) along the session id (S_{idm}) and the blockchain (BC) certificate issued by the CA server.
- Step 8: SG will create a random pre-master secret (Pms) key and encrypts it with the public key from the BC certificate, transmitting encrypting Pmsm to the BC node.
- Step 9: A master secret key is generated at both ends of the SG and BC node.
- Step 10: SG exchange MIoT device information that is received in step 5 and encrypt it with the session key and transfer it to smart contract authentication.
- Step 11: Smart contract authentication verifies the SG by verifying SG certificate, $(MIoTd_{id}.SG_{id})$ and send the response back to SG by encrypting it with the session key.
- Step 12: SG will respond back to MIoT node by exchanging the response received earlier and encrypted the message using the session key generated in step 5.
- Step 13: MIoT device completes the provisional authentication of SG by validating the SG certificate and checks the previously generated nonce values $(MIoT_N, N_a, MIoTd_{id}.SG_{id})$.

After formal approval, MIoT device can send transactions to the blockchain nodes.

5.4 Privacy Enforcement Layer

This layer is mainly responsible for the pursuance of privacy preferences as set by the data owner. A smart privacy contract will ensure that consumer policy will abide by the rules and regulations as set by the MIoT user in his/ her privacy preference. Moreover, it provides an additional feature of compliance checks for auditing purposes as well. The transaction flow steps involved in privacy contract is shown in Fig. 9

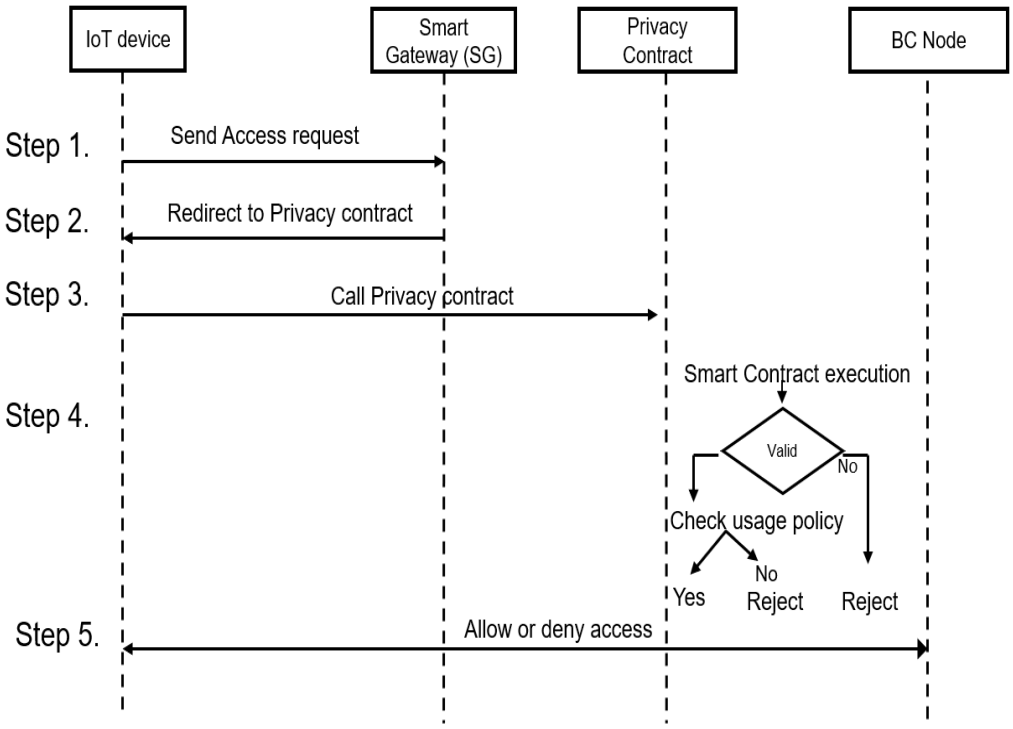

Figure 9: Privacy enforcement transaction flow

- Step 1: Anyone who want to access MIoT sensors data must subscribed him/herself from the data owner. Once subscribed and allowed, MIoT device will make an access request to SG so that the private data shall be used by the consumer.
- Step 2 & Step 3: SG will redirect it to privacy contract, and MIoT device will make a call to smart contract privacy.

- Step 4: Privacy contract once executed will make a compliance check and examine whether the policies set by the data owner comply with the guidelines as prescribed by the consumer.

- Step 5: Once all the policies are checked and verified, MIoT device will be granted access to send data to blockchain node.

Definition 3: Let TRN_d is the stream of transactions which is generated by an MIoT sensor and is forwarded to SG as shown in fig 5.1. MIoT device transmit their data inside payload PL_d such as

$$PL_d = MIoT_{id}, Prv_d, PL_{sn}, TRN_{did}, Payload, hash(Payload) \quad (28)$$

Where $MIoT_{id}$ is the device id, Prv_d is the tag of payload expressing that the data sensed by an MIoT device is a private data, PL_{sn} represents the sequence number of payload in TRN_d, TRN_{did} is the id of each transactions generated by an MIoT sensor, and payload is the actual sense data by an MIoT device followed by hash(payload) representing the hash value. It is important to mention, that each MIoT device is calculating the hash value by itself so that once the consumer receives the data it cannot be manipulated or corrupted by anyone in the network. Secondly to alleviate the burden of blockchain node these hash values are calculated by the MIoT sensors and it will be digitally signed to check the integrity of message as well.

Example 2: Let us consider a use case in which MIoT sensor is transmitting a stream of private information that needs to be consumed by the consumer which is the hospital in this case scenario as explained earlier. This MIoT sensor is connected to BC node A through its SG while the hospital is connected to BC node C via its respective SG. The format of each data generated by MIoT sensor is shown in Table 3.

Three different sensors have been considered in our example where each sensor is differentiated by its sensor id. A data type is considered only private whereas PL_Sn represents the sequence number of MIoT payload in each data stream. In our proposed framework,

Table 3: MIoT transaction payload example

$MIoT_{id}$	$Payload\ type$	TRN_{did}	$Payload$	$Hash$	PL_{sn}	$MIoTSig$
$MIoT_{id1}$	Prv	TRN_{id1}	$Oxygenlevel$: 95	$0x96cd3f29$	PL_{sn1}	$0x24cd51f7$
$MIoT_{id2}$	Prv	TRN_{id2}	$Heartrate$: $60-100bpm$	$0x54bc3a84$	PL_{sn1}	$0x15ab57fe$
$MIoT_{id3}$	Prv	TRN_{id3}	$Bloodpressure$: 120/80	$0x32ac45fa$	PL_{sn1}	$0xad34f27c$

every MIoT sensor is connected to SG and it acts as a point of contact for each interaction of MIoT with the blockchain network. Before sending this data, each MIoT owner will first formulate a privacy policy for each data stream generated by the MIoT sensor. Consumers can then be subscribed to these data streams. In case, a policy is not set by the owner, or the consumer wants to access more data for detailed analysis, the consumer needs to be subscribed and proper acceptance is required from the data owner. Moreover, a consumer will also publish their policies on the blockchain as well for the compliance check and for audit purpose. The SG will append privacy policy to each transaction stream id as previously defined through the privacy tuple Tp with the following structure.

$$Tp = MIoT_{idx}, TRN_{idx}, Consr_{idx}, PP_{idx} \tag{29}$$

$Cosnr_{idx}$ represent the consumer id and privacy policy id PP_{idx} represent the data owner privacy policy as set for the data stream generated by the MIoT sensor. It is important to reiterate that each policy privacy set by the data owner will take MIoT id, stream id and consumer id as a parameter input and will return a unique id UPPid for each tuple policy once executed by the smart contract on blockchain. This unique id for each tuple policy will provide an association between the MIoT id, stream id and Cid which can be used further for the privacy compliance check for an audit purpose. Moreover, it is also utmost important to mention over here that this tuple does not contain any actual data generated by the MIoT sensor. Data will only be released to the subsequent consumer after the compliance check

is performed by all the nodes of the blockchain. The privacy policy set by the data owner for each data stream is formulated using the following algorithm 3. Similarly, all those privacy policy set by the data owner must be satisfied and should be in accordance to the Algorithm 4.

Algorithm 3 Privacy Contract

Let : T_p be the privacy policy set by owner
Let : $UPPid$ be the privacy policy identifier
Let : CP is the Consumer policy
Function DataownerPrivacyPolicy(T_p)
Checkseqnumber(T_p)
$T_{pp.pp} = T_p.Dataowner$
$NewUPPid$
Privacy policy smart contract $\rightarrow (UPPid, T_p)$
Privacy Compliance check ($UPPid$)
end
Function PrivacyComplianceCheck($UPPid$)
$T_p \leftarrow (UPPid)$
$Consumer \leftarrow (T_p.TRN_{id})$
for all $Cons_{id}$ **in** *consumer*
$UPPid \leftarrow (T_p.TRN_{id}, Cons_{id})$
$T_p \leftarrow (UPPid)$
$Allow =$ check$(T_{pp.pp}.pp, T_p.UPPid)$
$Check.add(Cons_{id}, UPPid, Allow)$
end

5.5 Transaction layer

For the secure transaction over the blockchain, we propose a secure key exchange algorithm that is based on the Diffie-Hellman Key exchange algorithm also called an exponential key exchange. This algorithm employed a number raised to specific power to produce decryption keys based on components that are never transmitted before thus making it mathematically overwhelming to break the code. This protocol will provide forward secrecy and transport layer security as well. The implementation of the protocol uses a multiplicative group of integers called modulo followed by the following steps:

- Assume a prime number q

Algorithm 4 Data Owner Privacy Function check

Let : $DOPP$ be the data owner privacy policy
Let : CP is the Consumer Privacy Policy
Function $Check(DOPP, CP)$
Let : $IP = False$
Let : $HT = False$
Let : $ArbitratorRel = False$
if $CP.up \in DOPP.ip$ **then**
    $IP = true$
else
    $return\ IP = False$
if $CP.HT \leq DOPP.HT$ **then**
    $HT = true$
else
    $return\ Rt = False$
if $CP.ArbitratorRel \leq DOPP.ArbitratorRel$ **then**
    $ArbitratorRel = true$
else
    $return\ ArbitratorRel = False$

- Select α, which must be a primitive root of q, such that $\alpha < q$.
- α is the primitive root of q if and only: $\alpha modq$, $\alpha^2 modq$, $\alpha^3 modq$ ..... $\alpha^{q-1} modq$ = $1, 2, 3 \ldots . q-1$

A detailed explanation of the proposed protocol is shown in Fig. 10.

- Step 1: BC node A when it receives a private transaction in its private database will make a call to its transaction manager A and forward the private data to it. Sender transaction manager will first establish a TLS session with the recipient transaction manager. The protocol is based on Diffie- Hellman key exchange algorithm.
- Step 2: The foremost step of this process is that BC node A will pick a secret integer a and random nonce value N_a .
- Step 3: BC node A will pass on its certificate, $\alpha^a modq$ and the freshly picked nonce N_a which is digitally signed by its private key containing the information of $\alpha^a modq$, N_a and BC node C id towards BC node C.

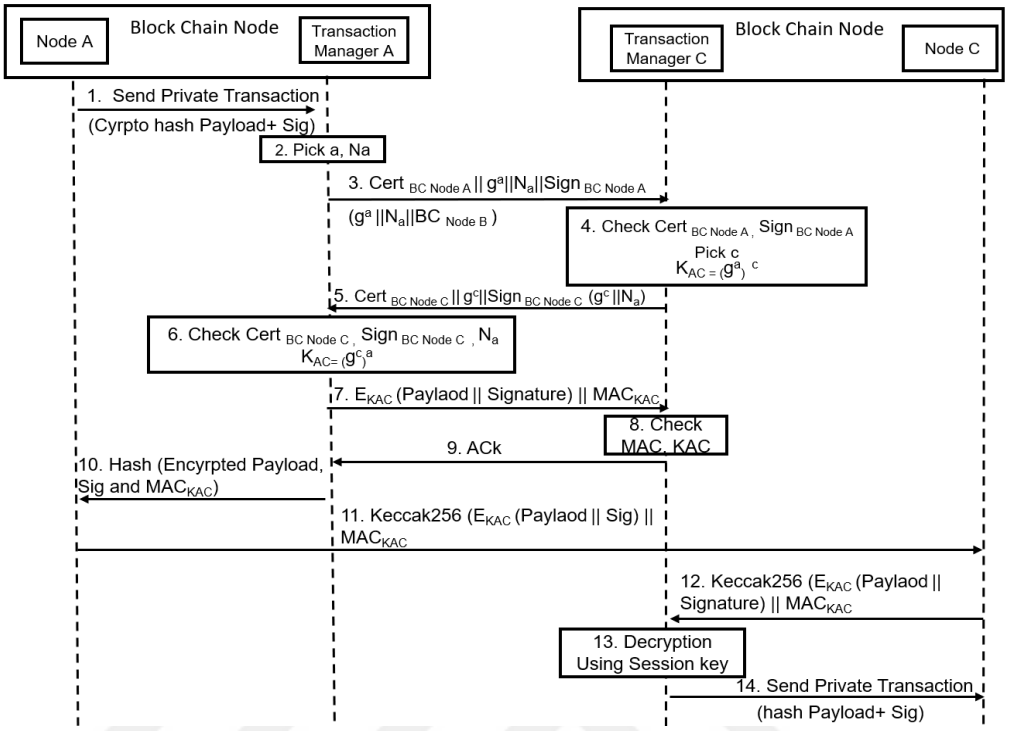

Figure 10: Privacy Transaction flow

- Step 4: The recipient node id will make sure that the desired message is intended for BC node C. BC node C will inspect the certificate and the provided signature assuring that message is not forged by anyone in the network. Once the check is successful, BC node C will generate a secret integer c and construct a shared secret key such that $KAC = (\alpha^a)^c modq$.

- Step 5: BC Node C will send its certificate, $\alpha^c modq$ and, digitally signed the message containing $\alpha^c modq$ information along with the random nonce N_a generated earlier.

- Step 6: As soon as BC node A receives the information, BC node A validates the certificate with the provided signature and generated nonce followed by the generation of a shared secret key as $KC = (\alpha^c)^a modq$. If the protocol is successfully terminated it endorses that the shared secret key is only known to BC node A and BC node C. Once the shared secret key is generated at both ends, subsequent communication will

take place over the confidential secret channel.

- Step 7: A message is encrypted with the secret key along with its MAC by using the secret key that is generated by the key exchange protocol between BC node A and BC node C and sent to the transaction manager of BC node C.
- Step 8 & Step 9: The receiver transaction manager checks the integrity of the message via MAC and sends a positive acknowledgment to BC node A transaction manager.
- Step 10: Transaction manager A will send the hash of the encrypted payload to BC node A where it replaces the original payload with this hash. This hash of the encrypted payload will be broadcasted to all nodes in the network.
- Step 11 & Step 12: When BC node C receives this hash, it will make a call to its respective transaction manager if it holds the encrypted payload or not. If it holds, the transaction manager will forward this encrypted payload to the decryption module.
- Step 13: Decryption module will decrypt the payload suing the session key created earlier.
- Step 14: Transaction manager C will send the decrypted hash payload to to BC node C form where it will be forwarded to the connecting device via SG as shown in system model.

5.6 Security Analysis

In this section, we will discuss the security assurance that is provided by each layer of our underlying proposed framework by using a verification tool called AVISPA [81]. The semantic of the proposed protocols is verified and tested by using SPAN tool [82] and the subsequent results are presented in this section. AVISPA is a state of art automated tool

that provides a complete analysis of security-sensitive protocol over the internet. Dolev-Yao model is implemented in the AVISPA tool which mentioned that the intruder has full control over the network and the message can be intercepted, altered, and falsely sending the message to any agent by impersonating another agent but hard for the intruder to encrypt or decrypt the message without prior knowledge of a key. It is important to mention over here that our proposed architecture achieved security from two different perspectives. One is at the infrastructure level which comprises of registration of new MIoT devices and smart gateways to the blockchain network and the second is at the privacy level where transaction flow is carried out among the designated blockchain nodes maintaining the security aspect while articulating transaction privacy as set by the data owner as well. We assume that each MIoT node, smart gateway, and blockchain node is untrustworthy and may be attacked by an outsider to fulfill their conflicting interest. Our security analysis will be based on the following assumptions:-

Assumption 1: CA is a trustworthy entity and all the digital certificates issued by CA are specified by the X.509 standard. It is not possible to forge a signature by any entity

Assumption 2: The same nonce cannot be chosen twice, if chosen it can be done with minimum probability

Assumption 3: Each MIoT device and SG will calculate the hash and will digitally sign the data.

Infrastructure: To corroborate a secure environment, and flow of communication among MIoT nodes, smart gateways, and blockchain nodes, we leverage the registration, digital certificates, and public and private keys as provided by CA. which is based on X.509 standards. In smart contract registration protocol where each MIoT device sends a registration request to smart gateway using the certificate issued by CA and the SG subsequently validate its certificate from the CA is evaluated and tested by AVISPA. The results obtained by AVISPA tool is shown in Fig. 11 For the authentication of MIoT devices, We evaluate the following security properties of our prosed framework using AVSIPA and SPAN tools.

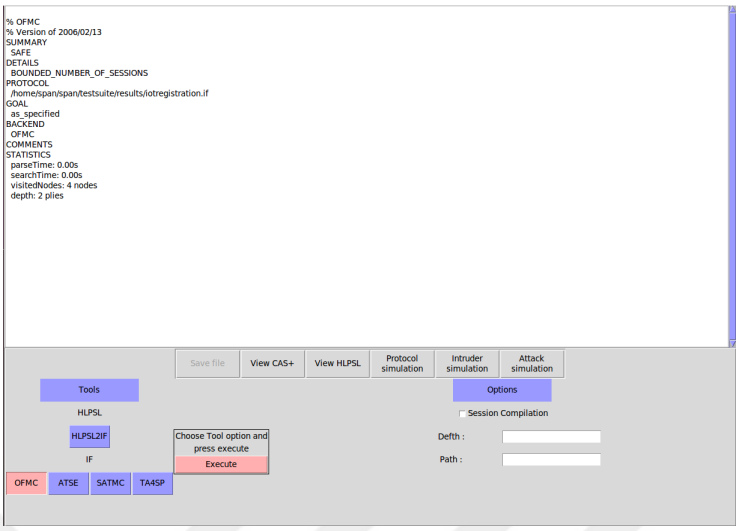

Figure 11: MIoT device registration

Authentication: As mentioned in the smart contract privacy, three actors are mainly involved while authenticating the MIoT device to the blockchain node. MIoT device first establish a secure TLS session with a smart gateway to get authenticated the smart gateway provisionally using the smart gateway's unauthenticated server certificate. Later after receiving the smart gateway certificate, MIoT completes the authentication process of the smart gateway while receiving the same SG certificate in step 12 of MIoT authentication process. Smart gateway and smart contract authentication authenticates each other during a normal TLS session. Smart contract authenticates the MIoT node using its device id which is already available over the blockchain during the registration process. The authentication property of the protocol is tested using the request and witness parameters which is declared as an authentication goal in the goal specification of High-Level Protocol Specification Language (HLPSL). This property asserts that one node can be a peer of another node and both of them agree on the nonce value before authentication.

Confidentiality/Secrecy: This property revealed that the message exchange remains confidential, and it does not disclose this information to any third party during the transmission. Our proposed framework strictly complies to confidentially as the message is transmitted first by establishing a secure TLS session between the sender and receiver.

Replay attacks: This kind of attack normally occurs when an intruder eavesdrops on a secure network and intentionally delays or repeats the message while impersonating the legitimate agent. Different techniques are used to eliminate replay attacks by adding freshness to the message including nonce, timestamp or session ID. We prevent this attack by adding the nonce value during the TLS hand shake process. The tested result of MIoT authentication as done by AVISPA tool is shown in Fig. 12 Moreover, blockchain nodes

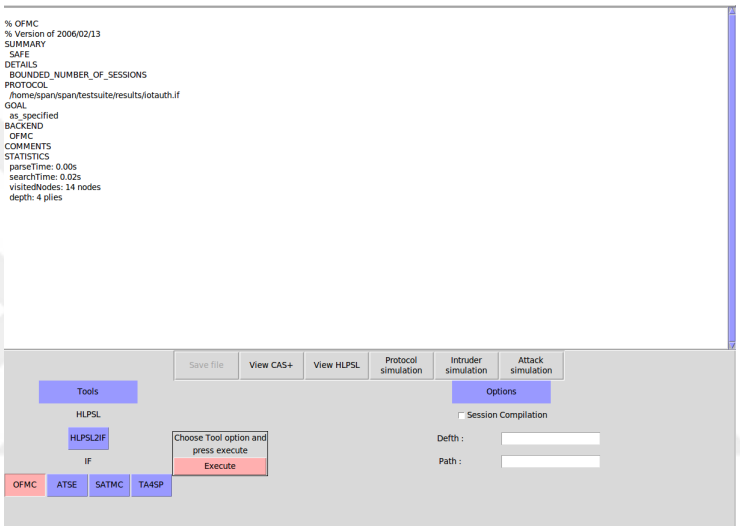

Figure 12: MIoT device authentication

themselves might be vulnerable to different kinds of threats and attacks e,g double spending, Sybil attack and, smart contract coding inadequacy etc. To cater such kind of issues we adopted permissioned Quorum blockchain in our proposed framework in which every node needs to be pre- authenticated before joining the network. Therefore, any malicious behavior adopted by any node is accountable and can be restricted from joining the network. Although the privacy policy adopted via smart contract runs on the top of blockchain even in an untrusted environment, we leverage Quorum blockchain which natively supports smart contract privacy thus reducing the errors and bugs that can be incorporated via smart contract. It is also possible that an untrusted gateway can send the data to an unauthorized node, or an attacker performs eavesdropping. Since in our proposed framework our data is encrypted with the secret key generated by the Diffie–Hellman key exchange algorithm,

even if the data is shared with an unauthorize node, data cannot be accessible. Furthermore, the risk of eavesdropping is limited by the secure TLS connection established between the sender and receiver. Result analysis of MIoT transmission from blockchain node to the consumer (hospital) is declared as safe by AVISPA tool as shown in Fig. 13

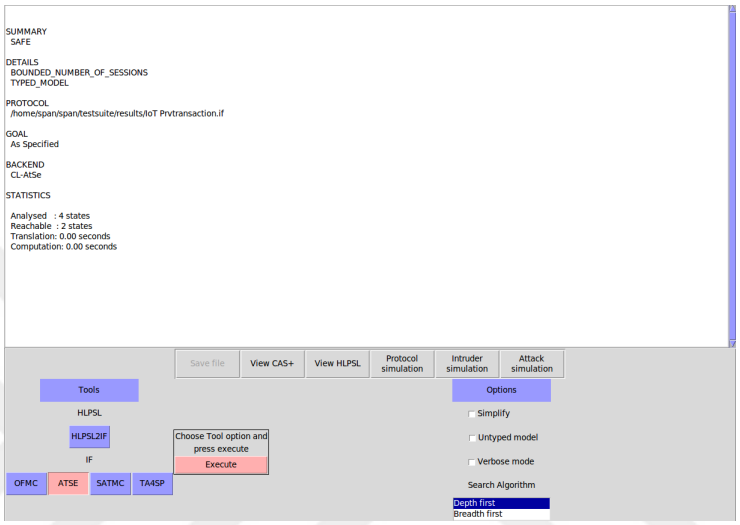

Figure 13: MIoT transmission

Privacy Layer: Attackers can attack the MIoT nodes and smart gateways and can generate a fake policy or try to modify the policy as set by the data owner. In our proposed framework as per assumption 3, each SG node needs to digitally sign the privacy preference, if a fake policy is signed by the SG, the data owner can cross verify the privacy policy stored on the blockchain and detect the malicious MIoT or SG node. Furthermore, the proposed framework provides the full capability to the data owner to directly set the privacy preference for each data stream generated on the blockchain. This will rule out any tampering done by the compromised MIoT node or smart gateway. Another possible attack is in a scenario where MIoT device perform DDoS attack where each MIoT device can trigger excessive number of privacy preference tuple and tries to stimulate privacy contract enforcement. To counter such kinds of attacks, smart gateways are fully equipped with countermeasures against DDoS attacks such as detection and monitoring, MIoT logs scanning, and notification. A malicious gateway can also duplicate, modify, or omit the privacy policy set for the

tuple. To cater, each MIoT device will sign the privacy preference tuple before sending it to a smart gateway. It can be easily identified by the blockchain due to signature invalidation. Privacy preference cannot be duplicated due to sequence number since it is included in the signature.

5.7 Simulation Results

To illuminate the path for the real-world implementation of MIoT sensors with the blockchain, we evaluated the performance of our proposed algorithm and architecture by deploying the quorum blockchain. Chain-hammer [83], a bench-marking software tool is used to evaluate the performance of our proposed framework by implementing it on a quorum blockchain testbed. In terms of hardware, we used Intel Core i7-10700 CPU 2.90 GHz processor, and 8 GB RAM machine as our testing environment. Initially, a testbed is created by deploying four nodes acting as a fully functional quorum blockchain on this machine. Additionally, we have used Solidity and Truffle framework to develop, test and deploy our smart contracts. Data which is generated inside the smart contract is comprises of $MIoT_{id}$ which is the device id, Prv_d,the tag of payload expressing that the data sensed by an MIoT device is a private data, PL_{sn} represents the sequence number of payload in TRN_d, and TRN_{did} is the id of each transactions generated by an MIoT sensor. Moreover, we assume that each MIoT node and SG joins the blockchain network with the prior certificate from the authorized certificate authority. In the setup, simulations are evaluated by deploying three different consensus protocols RAFT, IBFT, and PoA by varying the private transactions thus varying the load in terms of changing the number of transactions from 1000 to 10,000 transactions on the blockchain peers. Also, we have assumed that there is no faulty nodes in the network or election process that need to be held for selecting any kind of leader in the consensus protocol. We evaluated the performance of our proposed architecture in terms of throughput which is the number of transactions processed per sec and latency. Each type of network tested is comprised of 5 sets of transactions, the first comprises processing 1000

transaction, followed by 2000 transactions, then 5000 transactions and ultimately increasing it to 10,000 transactions. For each type of transaction sent, the simulation is evaluated using two modes of transmission i-e., sequential mode of transmission and multi-threaded transmission, and evaluate the performance of each network in terms of throughput and latency. In a sequential mode of operation, tasks are performed sequentially one after the other and each operation needs to wait before the first operation is completed. While in multi-threaded environment operations are performed in a parallel fashion and we have used 3 threads in our multi-threaded environment considering the hardware limitation capabilities we have on our local machine. In our simulation results, we have employed both these two different modes of operation and evaluated the performance of the blockchain network.

It is also highlighted here that since the simulation is conducted on our local machine, and our local machine typically have limited hardware resources compared to dedicated servers and factors such as the number of CPU cores, available memory, and storage performance can greatly impact the overall throughput and transaction processing capabilities of the blockchain as observed in our simulation. The available hardware resources, such as the number of CPU cores and the amount of RAM, is shared among the 4 quorum blockchain nodes running on the local machine. This resource contention can lead to performance degradation, as the nodes compete for the limited computing power and memory, resulting in increased latency and reduced transactions per second (TPS). The degree of parallel processing, is also limited by the number of available CPU cores and threads on the local machine. Improvements such as scaling up the local machine, using a dedicated server, and implementing distributed simulation, can help overcome the limitations and further improve the blockchain network's performance. The average throughput of the implemented scheme is show in Fig. 14. It is evident from the graph that RAFT performs better in terms of throughput when compared to IBFT and PoA consensus protocol and as we know that RAFT is super fast in terms of its default block minting time as well as it does

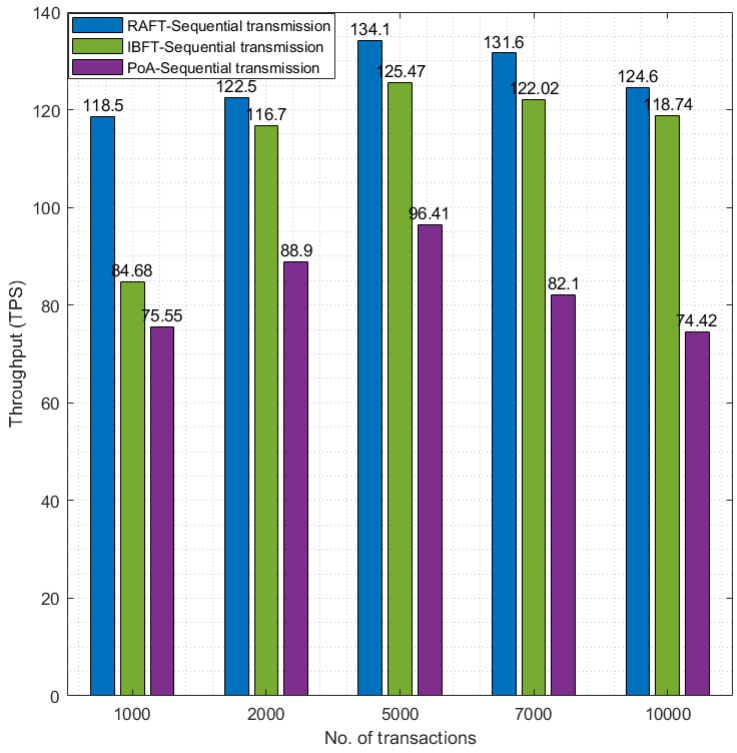

Figure 14: Throughput analysis- Sequential mode of operation

not mint empty blocks thus giving us an optimized throughput. In addition, there are no forks produced and transaction finality ensures it during the transaction processing. IBFT on the other hand mints blocks at a constant rate and even they mint empty blocks ultimately resulting in consuming more space and storage. In addition to this, IBFT encounters a lot of messages overhead that gets exponentially worse as the number of validator nodes increases due to which its throughput performance is slightly less than RAFT. However IBFT performs better in throughput when compared to PoA, it is due to instant consensus finality and speed of convergence of network. PoA, on the other hand, does not have any immediate finality and due to the generation of forks, its throughput depreciated when compared to both RAFT and IBFT respectively. For example, during the processing of 5000 transactions in sequential mode, the throughput reaches 134.1 TPS for RAFT consensus which is the highest TPS achieved with the implemented network as shown in Fig. 14. Moreover,

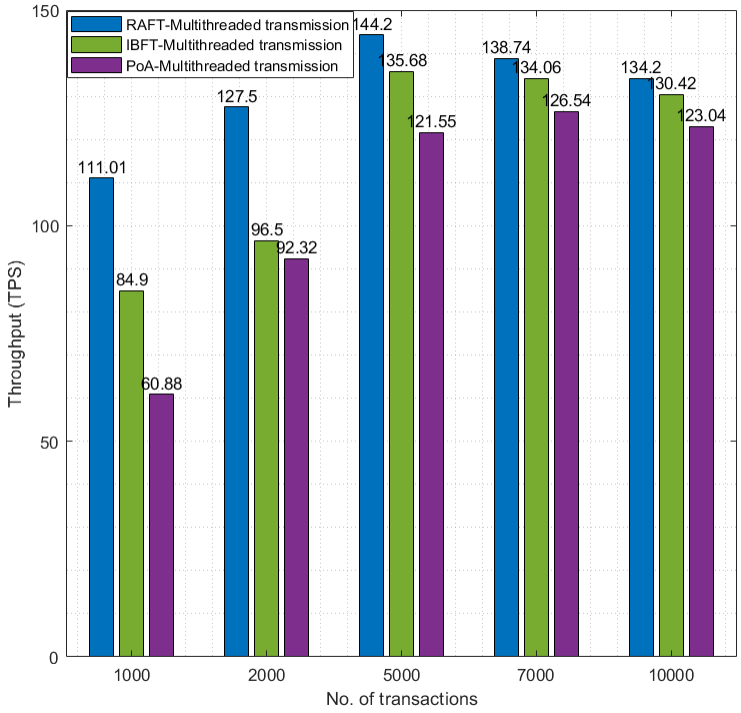

Figure 15: Throughput analysis- Multi-threaded mode of operation

it is also observed that as we increase the number of transactions, throughput decreases which is due to an increase in communication overhead and workload both in the case of IBFT and PoA as well.

Additionally the performance of consensus protocols is also tested with multi-threaded environment as shown in Fig. 15. As expected with the same four nodes network setting, a multi-threaded environment achieves better throughput as compared to the sequential mode of transmission due to better BC node responsiveness and enhanced speed processing as well. Here as well, RAFT outclasses the contemporary approaches due to its fast convergence time and high speed as compared to IBFT and PoA. For example for the initial transactions i-e., for 2000 transactions, an accelerated throughout of 127.5 TPS has been achieved as compared to IBFT and PoA. Similarly, the same response of decreasing throughput is seen here as well as we increase the number of transactions iterating that as the length of blockchain increases throughput decreases.

Furthermore, to give more insight about transaction latency, block time which is the time required to mint a block is shown in Fig. 16 comparing the overall minting block time of RAFT, IBFT and PoA. Block time is provisioned initially during the network setup when the transactions are batched into block. As we discussed previously, RAFT is super fast

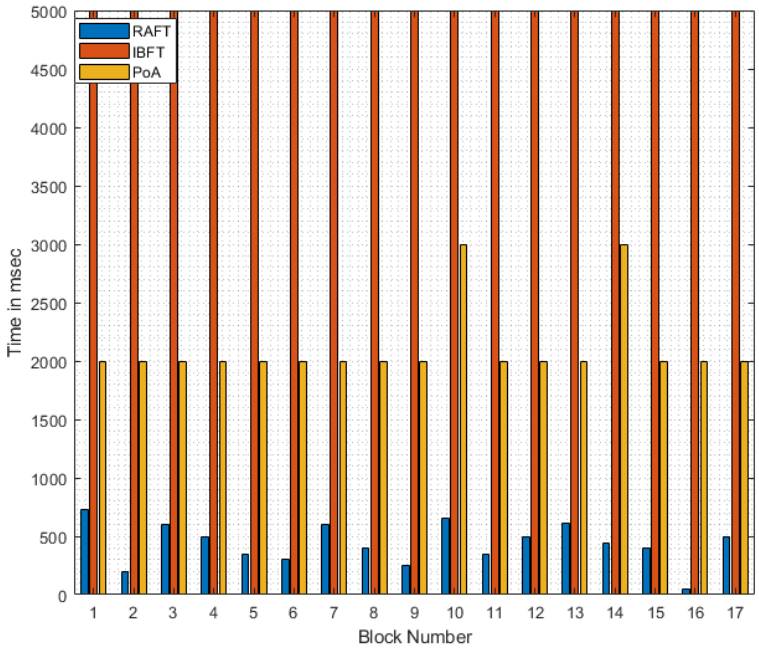

Figure 16: Comparison of Block Time for RAFT, IBFT and PoA

in terms of its default block minting time and it is also shown in Fig. 16 that RAFT block minting time is much faster as compared to IBFT and PoA and approaching to block time of approximately less than 500 ms. On the other hand, IBFT protocol has a default block time of 5000 ms while PoA achieves an average block minting time of 2000 ms.

To show the overall transaction latency for sequential mode of transmission, graph is shown in Fig. 17 depicting the latency curve among RAFT, IBFT and PoA consensus algorithm for sequential mode of transmission. As expected RAFT shows the lowest latency for 10,000 transactions with a delay of 32.20 sec while PoA achieving the highest latency of 43.28 sec for the same number of 10,000 transactions as shown in Fig. 17. Although the block time of PoA is much faster as compared to IBFT, but the overall transaction delay

of IBFT is much better when compared to PoA. As we mentioned previously, that PoA protocol favours availability over consistency as they do not ensure consistency ultimately resulting in generation of forks which need to be resolved sooner or later ultimately resulting in much higher delay. We also noted an increase in transaction delay as the number of transaction increases and this increase is due to the increase in compliance check on privacy preference and policies as set by the data owner. An improved latency of the three

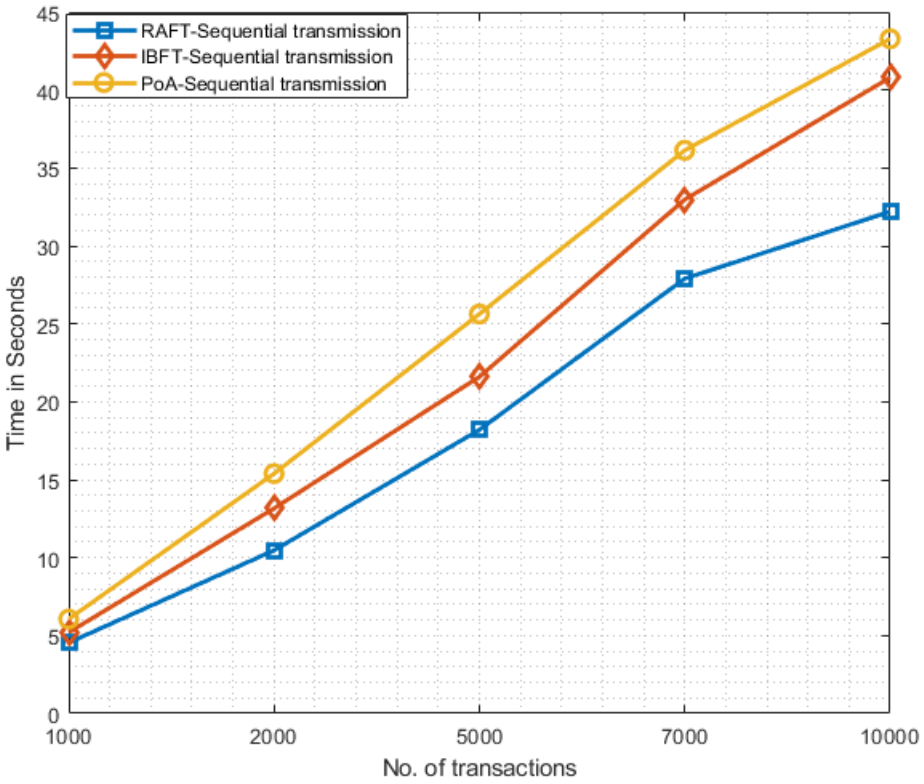

Figure 17: Transaction delay analysis- Sequential mode of operation

implemented schemes is achieved during the multi-threaded mode of transmission which is shown in Fig. 18. According to this graph, RAFT achieves the lowest latency of 24.50 sec for 7000 transactions, while IBFT and PoA being at the highest delay of 26.90 sec and 28.75 sec respectively. We assess from the latency results that as the number of transactions increases, time delay increases because the compliance check on privacy preference and policies consume much more time to make sure that data can only be available to the

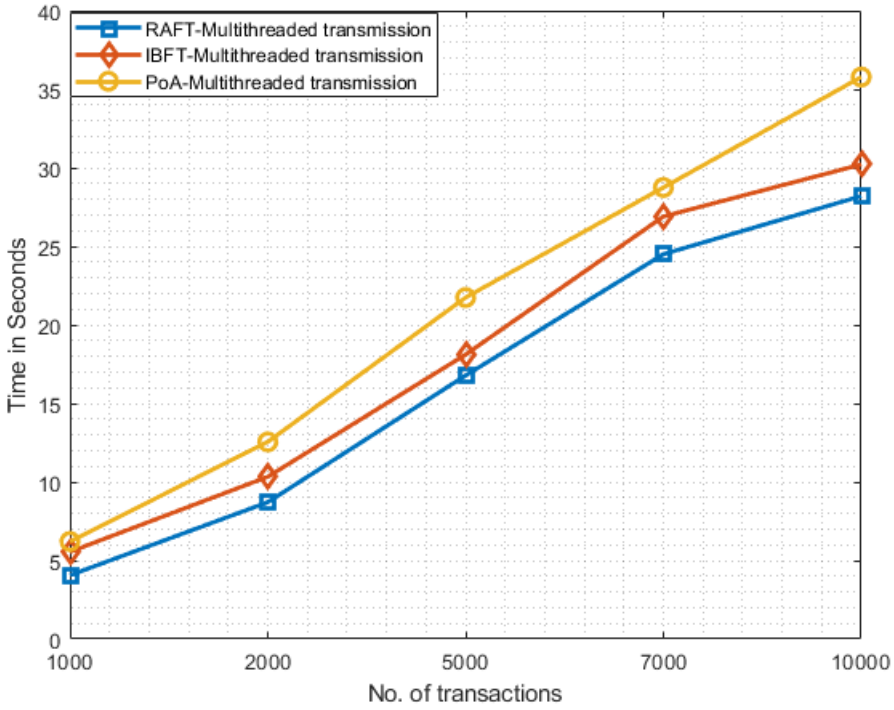

Figure 18: Transaction delay analysis- Multi-threaded mode of operation

authorize consumer only.

To conclude, RAFT proves itself to be a well adapted consensus algorithm specially for private blockchain like Quorum and performs better in terms of throughput and latency both for sequential and multi-threaded mode of transmission. These results can be considered as a first milestone for exploring blockchain in this domain and can paved the path for subsequent experiments while integrating MIoT with blockchain network.

To further surmount the privacy preservation issues in MIoT based-blockchain network and to further enhance the privacy protection, we have proposed the DPP framework. DPP is a mathematical framework that ensures strong privacy guarantees. By implementing DPP at the stream level generated by IoT devices, it provides a rigorous mathematical framework that provides provable privacy guarantees, making it a more robust and reliable approach compared to the blockchain based mechanism.

CHAPTER VI

DIFFERENTIAL PRIVACY BASED FRAMEWORK USING BLOCKCHAIN

More recently, differential privacy has emerged as a promising privacy-preserving framework for MIoT data analysis. Differential privacy provides a rigorous mathematical definition of privacy guarantees by injecting carefully calibrated noise into the data. However, despite its potential, implementing differential privacy in the context of medical MIoT devices has its own set of challenges, including the choice of appropriate noise mechanisms, determining privacy parameters, and managing the trade-off between privacy and utility. In this chapter, we focus on addressing the privacy challenges in medical MIoT devices by employing differential privacy mechanism by adding three different kind of noises i-e Laplace noise, Gaussian noise and exponential noise as a differential privacy mechanism. We explore the integration of these three different kind of noises with blockchain technology to enhance the security and integrity of medical data. By leveraging the advantages of both differential privacy and blockchain, we aim to provide a robust privacy-preserving solution that ensures individual privacy while enabling secure and efficient data sharing and analysis in the medical domain.

In this chapter we first introduce the notion of privacy and utility metrics to create a balance between privacy and utility. We then explain the mechanism how the controlled noise shall be generated using differential privacy mechanism followed by its distribution over the blockchain network. Next we analyzed the performance of our proposed framework in terms of throughput and latency by deploying three different consensus protocol RAFT, IBFT and PoA. By investigating the efficacy and performance of the proposed approach, we aim to contribute to the development of privacy-enhancing solutions for medical

MIoT devices, fostering trust among patients, healthcare providers, and stakeholders in the evolving landscape of healthcare data management.

6.1 Scheme Construction

In this section, we introduce the overall architecture of the DPP based framework articulated with blockchain as shown in Fig. 19. The following summarizes the key role of

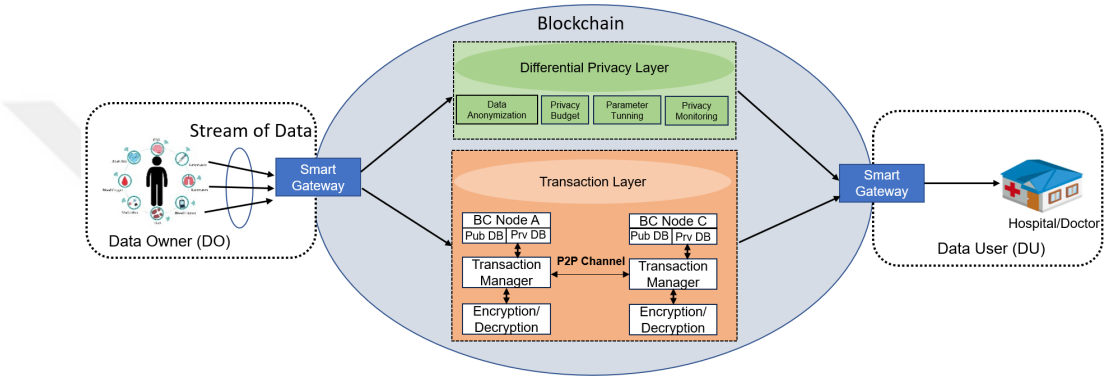

Figure 19: DP system model

various elements that constitute this framework.The workflow of DPP framework is consisted of three phases: Data generation phase, Data Sharing phase and Data Analysis phase as shown in Fig. 20.

As a case scenario, let us consider an example in which DO is connected to blockchain node A via SG wants to send his/her private data to the DU which is doctor in our case connected to blockchain node C as shown in Fig. 20.

6.2 Phase 1: Data Generation phase

In the data generation phase, MIoT devices are generating multiple stream of data for instance acquiring the heart rate, blood pressure (B.P) or sugar level as shown in Fig. 21 .

The sensed data must reach to the hospital namely the doctor who takes care of the treatment. The following steps need to be performed by the DO while transmitting his/her

Algorithm 5 Data Generation - Laplace Noise

Let ε be the epsilon value set by the data owner
Let Δ be the sensitivity value set by the data owner
Let $PrvMIoT_{PL}$ be the MIoT private payload data
Let S be the sequence number of MIoT private payload data
Let $Func$ be the noise function selected by the data owner
Let $AdjustNoise$ be the adjustment parameter for noise effectiveness
Let $PrivacyLevel$ be the privacy level set by the data owner (low, medium, or high)
Input: $PrvMIoT_{PL}$, S, ε, Δ, $Func$, $AdjustNoise$, $PrivacyLevel$
Output: P_d, PM_ε
for each j in S **do**
    $\varepsilon_L \leftarrow$ Laplace Privacy Budget based on $PrivacyLevel$
    $\Delta \leftarrow$ Database sensitivity
    Generate Laplace Noise
        $noise_j = \text{Lap}(Func, \varepsilon_L, PrvMIoT_{PL})$
    Adjust Noise Level
        $noise_j \leftarrow AdjustNoise \times noise_j$
    Calculate $P_{dj} = PrvMIoT_jPL + noise_j$
    $PM_\varepsilon(P_{dj}, PrvMIoT_{jPL})$;
return P_{dj}, PM_ε
Function PM_ε
    $PrvMIoT_{PL} \leftarrow$ MIoT private payload data
    $P_d \leftarrow$ Perturbed Value
    $PM_\varepsilon = |P_d - PrvMIoT_{PL}|$
End Function

Algorithm 6 Data Generation - Gaussian Noise

Let ε be the epsilon value set by the data owner
Let Δ be the sensitivity value set by the data owner
Let $PrvMIoT_{PL}$ be the MIoT private payload data
Let S be the sequence number of MIoT private payload data
Let $Func$ be the noise function selected by the data owner
Let $AdjustNoise$ be the adjustment parameter for noise effectiveness
Let $PrivacyLevel$ be the privacy level set by the data owner (low, medium, or high)
Input: $PrvMIoT_{PL}$, S, ε, Δ, $Func$, $AdjustNoise$, $PrivacyLevel$
Output: P_d, PM_ε
for (each j in S) **do**
    $\varepsilon_G \leftarrow$ Gaussian Privacy Budget based on $PrivacyLevel$
    $\Delta \leftarrow$ Database sensitivity
    Generate Gaussian Noise
        $noise_j = \text{Gaussian}(Func, \varepsilon_G, PrvMIoT_{PL})$
    Adjust Noise Level
        $noise_j \leftarrow AdjustNoise \times noise_j$
    Calculate $P_{dj} = PrvMIoT_jPL + noise_j$
    $PM_\varepsilon(P_{dj}, PrvMIoT_{jPL})$;
return P_{dj}, PM_ε
Function PM_ε
    $PrvMIoT_{PL} \leftarrow$ MIoT private payload data
    $P_d \leftarrow$ Perturbed Value
    $PM_\varepsilon = |P_d - PrvMIoT_{PL}|$
End Function

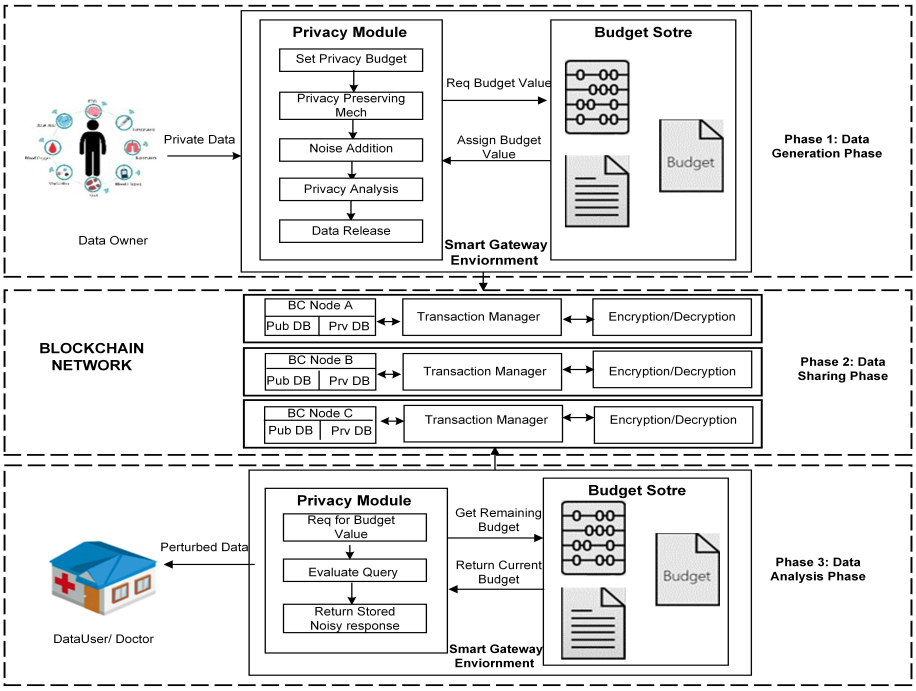

Figure 20: Proposed Framework

private data to the SG.

- Step 1: DO will first determine the level of privacy protection as desired (low, medium, high) and set the privacy budget (epsilon) , and sensitivity (delta) of the data by requesting budget value from the budget store inside the SG. The privacy budget represents the maximum amount of privacy loss that the system can tolerate. In the smart contract *setparamters* function is used to set the privacy budget and sensitivity of data and calculate the standard deviation based on these parameters.

- Step 2: The budget store will assign the budget value based on the level of acceptable privacy risk as identified by DO.

- Step 3: Based on the budget value, the privacy module will generate noise from either Laplace, Gaussian or Exponential distribution as requested by the DO via smart contract. The smart contract contains *addnoise* function to generate a specific amount of noise. The choice of technique depends on the type of data and desired level of

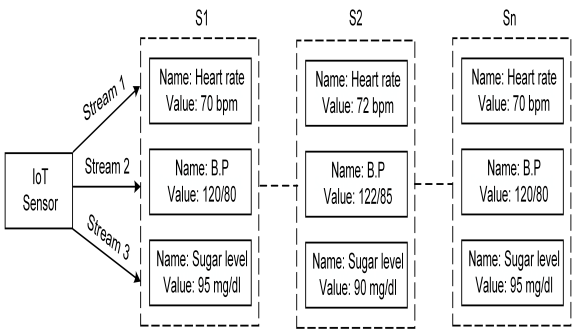

Figure 21: MIoT Stream of Data

privacy. For example if the data is very sensitive, more noise may need to be added to protect the privacy of DO.

- Step 4: To ensure that either the added Laplace noise, Gaussian noise or Exponentail noise is effective, *privacymonitoring* function is added in the smart contract which calculates the statistical measure of the noisy data and compares them to the original data value. If the statistical measures are close to the original data values, then the added mechanism is considered to be effective.

- Step 5: If the noise addition mechanism is not effective, DO will adjust the noise parameter such as privacy budget or sensitivity to improve the level of privacy protection. This is done by adding $adjustNoiseParameter$ inside the smart contract.

- Step 6: Based on the effective added noise, EEE will be calculated which is the measure of accuracy or expected value of the difference between the noisy output of function and the true output of the function

- Step 7: Calculate the utility metric

- Step 8: Once the effective noisy data is generated, SG will forward the noisy payload to its associated connected BC node

Algorithm 7 Data Generation - Exponential Noise

Let ε be the epsilon value set by the data owner
Let Δ be the sensitivity value set by the data owner
Let $PrvMIoT_{PL}$ be the MIoT private payload data
Let S be the sequence number of MIoT private payload data
Let $Func$ be the noise function selected by the data owner
Let $AdjustNoise$ be the adjustment parameter for noise effectiveness
Let $PrivacyLevel$ be the privacy level set by the data owner (low, medium, or high)
Let λ be the rate parameter for exponential noise
Input: $PrvMIoT_{PL}$, S, ε, Δ, $Func$, $AdjustNoise$, $PrivacyLevel$, λ
Output: P_d
for each j in S **do**
    $\varepsilon_L \leftarrow$ Laplace Privacy Budget based on $PrivacyLevel$
    $\Delta \leftarrow$ Database sensitivity
    Generate Exponential Noise
        $noise_j = \text{Exponential}(\lambda)$
    Adjust Noise Level
        $noise_j \leftarrow AdjustNoise \times noise_j$
    Calculate $P_{dj} = PrvMIoT_jPL + noise_j$
return P_{dj}

6.3 Phase 2: Data Sharing phase

This phase is mainly responsible for transmitting and processing the private transactions inside the blockchain network. The detailed steps followed during the transmission of private information among the blockchain nodes and its constituent transaction managers are already described in Fig. 10. Here at this step, we are sending the noisy payload which need to be transmitted over the blockchain network. Rest of the steps are similar to as described in section 5.5. To summarise, BC node A when it receives the nosiy payload, it will transfer it to its constituent Transaction manager which will first establish a secure TLS session with the recipient transaction manager. After successful validation, shared secret key will be generated and subsequent communication will occur over the confidential secret channel. Transaction Manager A computes the hash of the encrypted noisy payload and replaces the original payload with this hash. The hash of the encrypted noisy payload is then broadcasted to all nodes in the network. Recipient transaction manager will forwards it to the decryption module. The decryption module uses the previously established session

key to decrypt the noisy payload.

6.4 Phase 3: Data Analysis phase

The data analysis need to be performed by DU as shown in Fig. 22 and is comprised of

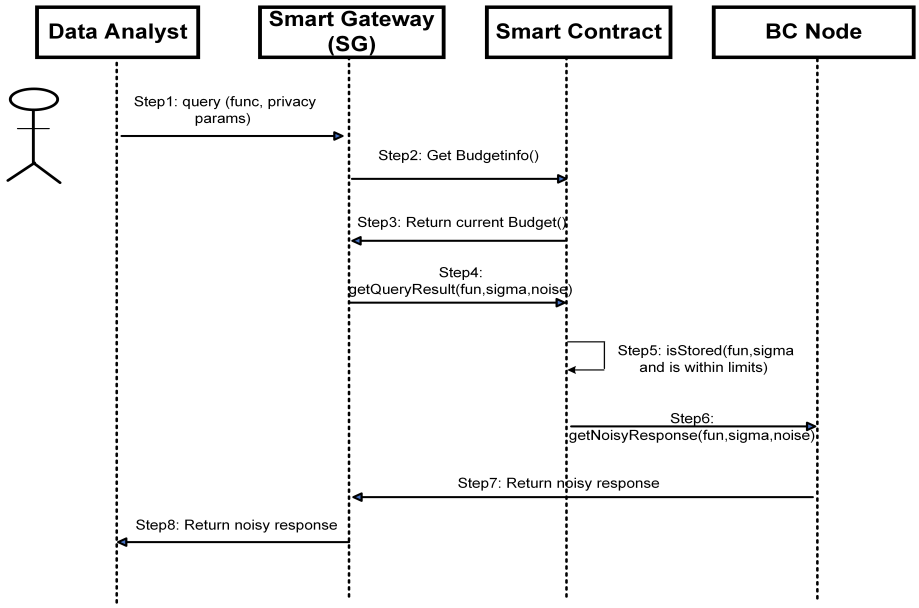

Figure 22: Data Analysis Phase

the following steps:

- Step1: DU will submit a query to SG which will include a function parameter indicating that what kind of noise is added and what are the privacy parameters (Budget value) from a privacy module
- Step2 & Step 3 : SG via its privacy module will check for the budget value and amount of noise added to the data from budget store and will return the current budget vale to the DU
- Step4: DU will submit the query along with the current budget value to privacy module.

- Step5: Smart contract will perform a check whether the current budget value is within the limits as set by the DO.

- Step6 & Step 7 : If the condition is true, smart contract will query for the noisy data that is stored on the BC network and the BC node will return the noisy response to the SG. If the condition is false the query will be rejected.

- Step8: In the last step, DU will get the noisy response from its associated SG and perform the analysis accordingly as per the privacy level and utility level maintained by the DO. Overall, the proposed framework provides the tracking mechanism of the privacy budget value as well to check whether the added noise is effective in providing privacy to the sensitive data or not and its value will be stored on BC for the audit purpose as well

6.5 Simulation Results

In this section the execution of propose DPP system model is evaluated and analyzed. Firstly to evaluate a benchmark study between privacy and utility, simulation is conducted and implemented in Matlab (R2013b) and run our simulations on a desktop computer with Intel core i7-10700 2.90 GHz processor, 8GB RAM, and Windows 10 platform. The detailed parameter settings used in our simulations are implemented as shown in Table 4 in

Table 4: Parameter Settings for Simulation

Mechanism	Parameter	Value
Laplace distribution	Δf, Δt	$\Delta f = 1$, $\Delta f = 2$, $\Delta f = 3$, and $\Delta t = 1$
Gaussian distribution	$\Delta_2 f$, Δt	$\Delta_2 f = 1$, $\Delta_2 f = 2$, $\Delta_2 f = 3$, and $\Delta t = 1$
Exponential distribution	$\Delta f, \lambda$	$\Delta f = 1$, $\Delta f = 2$, $\Delta f = 3$, and $\Delta\lambda = 0.5$

which Δf refers to L1 sensitivity of Laplace mechanism, $\Delta_2 f$ refers to L2 sensitivity of Gaussian mechanism and Δt is the parameter of the characteristic function of both Laplace

and Gaussian mechanism. Where as λ is the exponential noise parameter. The simulation results show that how different privacy parameters, such as the sensitivity of the data or the level of noise added, affect the trade-off between privacy and utility. Our results demonstrate that increasing the privacy parameter, such as the amount of noise added, can increase the level of privacy but decrease the accuracy of the data, and similarly decreasing the privacy parameter will increase the utility. To support our argument first we plotted the privacy curve for both Laplace Gaussian and exponential mechanism as a function of expected estimation error (EEE) vs epsilon values and analyze the behavior of privacy plot by varying the epsilon values and then plotted the utility curve as a function of modulus of characteristic function with respect to epsilon values and eventually explore its behavior for all the Laplace, Gaussian and exponential noise mechanism respectively. We first plotted the privacy and utility plot for both the Laplace and Gaussian noise followed by the privacy and utility plot of Exponential to provide more clear understanding of the noise affect in all three different scenarios. In Fig. 23, we can observe that the EEE decreases

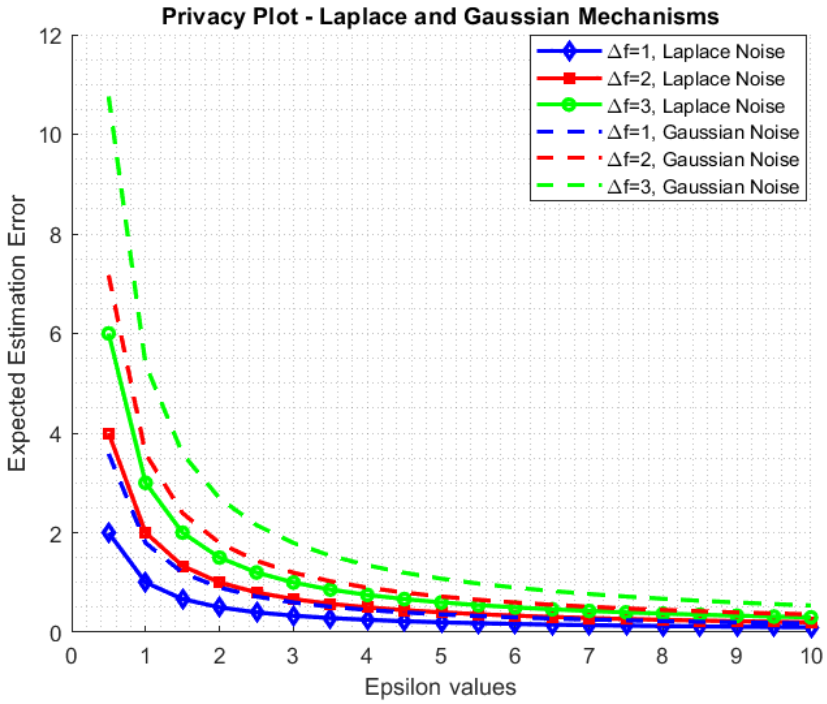

Figure 23: Privacy plot

as the privacy budget (ε) increases when using Laplace or Gaussian as a noise addition mechanism. The overall curve is plotted by varying the Δf parameter as well showing the behavior of privacy with respect to different ε values. The privacy plot curve is computed by setting $\Delta f = 1$, $\Delta f = 2$, and $\Delta f = 3$ in our simulation results. Fig. 23 depicted that a smaller value of ε yields better privacy with respect to higher ε values. This behavior is consistent with Theorem 1 as well as demonstrating that as we increase the (ε) value, privacy decreases. Similarly for the Gaussian noise, the same approach has been observed while plotting the privacy with respect to budget ε values showing that lower values of ε results in better privacy as compared to increase in ε values which proves to be consistent with Theorem 2 as well. Fig. 23 depicted that Gaussian noise provide strong privacy at low ε values as a comparison to Laplace noise for different $\Delta f = 1$, $\Delta f = 2$, and $\Delta f = 3$ values. This behavior is due to the fact that Gaussian noise has a smooth bell-shaped distribution, which means that it has smaller tails compared to the Laplace distribution. This characteristic makes Gaussian noise less likely to introduce large outliers or extreme values, even for small amounts of noise. As a result, the impact on the data is more localized and concentrated around the true values, preserving the overall utility of the data. This localization of noise helps to provide better privacy guarantees, especially at low epsilon values.

Similarly to give more insight and to show the affect of adding Exponential noise, Fig. 24 describes the privacy behaviour by varying the Δf parameter with respect to different ε values. A similar trend is observed while comparing it with Laplace noise and Gaussian noise mentioning that a high privacy is achieved at low epsilon values and privacy curve decreases as we increase the epsilon values. Similarly in Fig. 25, we plotted the utility curve as a function of modulus of characteristics function $|\phi(t)|$ with respect to epsilon values for both Laplace and Gaussian noise mechanism. For different $\Delta f = 1$,$\Delta f = 2$, and $\Delta f = 3$ values, the utility curve is plotted demonstrating that as we increase the budget ε values the utility increases. This verifies Corollary 1 and Corollary 2 as well. Additionally Fig. 25 depicted that Laplace noise, with its heavier tails, is more

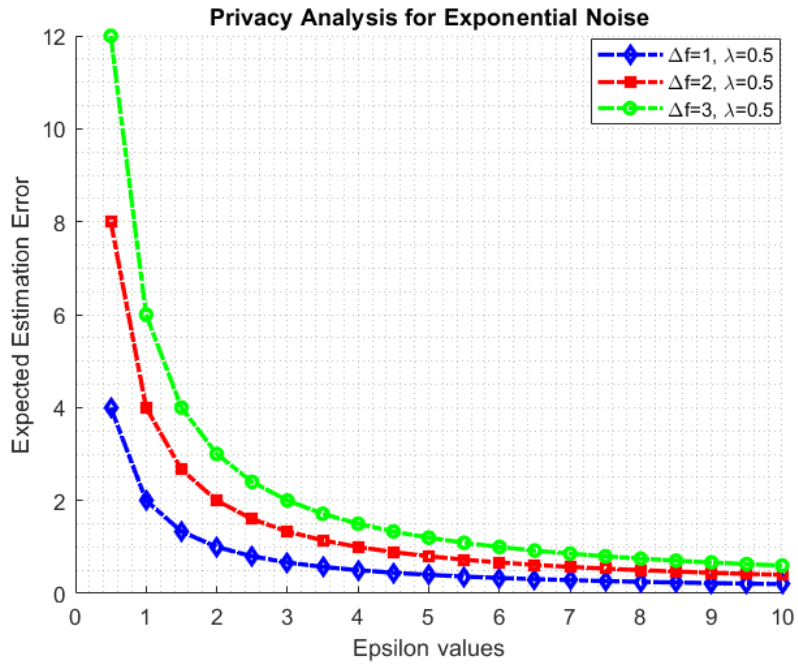

Figure 24: Exponential privacy plot

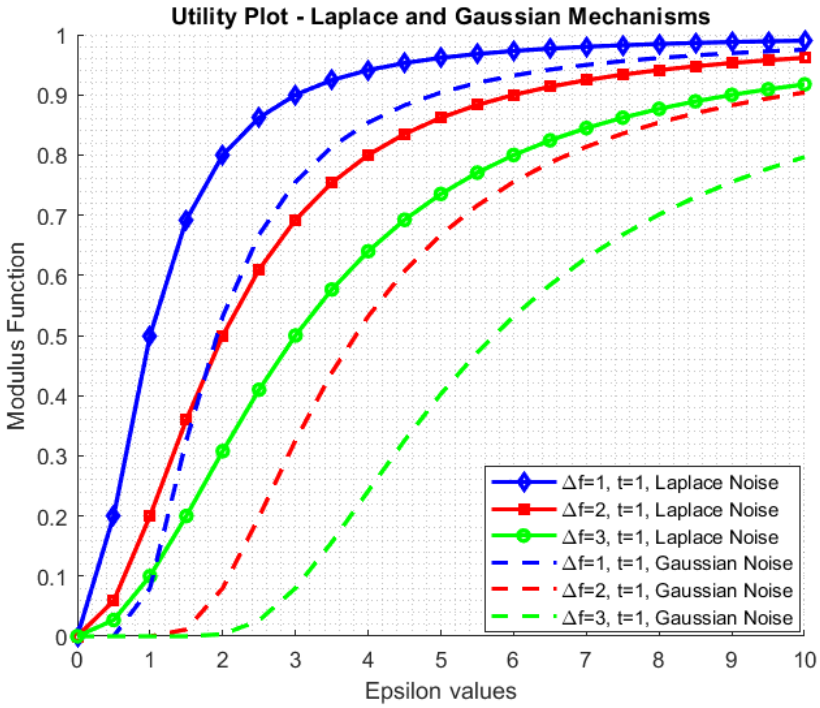

Figure 25: Utility plot

robust to small changes in the data compared to Gaussian noise. This robustness can result in lower distortion of the original data, which translates to higher utility at lower epsilon values as shown in Fig. 25. In addition, Exponential utility plot is shown in Fig. 26 depicting the same behaviour that as we increases the budget ε values the utility increases.

In Fig. 27, Fig. 28 and Fig. 29 we visually inspect the behavior of Laplace noise, Gaus-

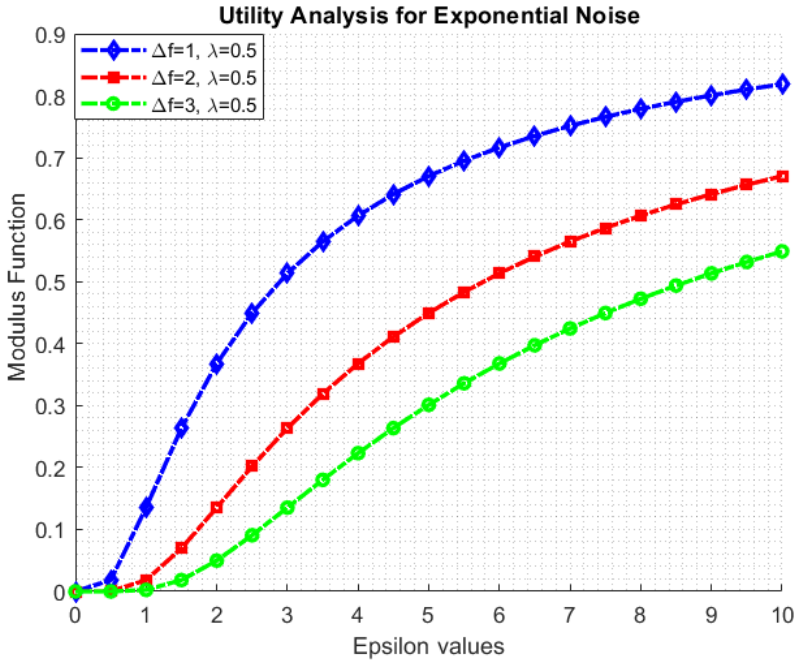

Figure 26: exponential Utility plot

sian noise and Exponential noise in comparison to original data by varying the parameter of differential privacy $\varepsilon = 0.05$ as a high privacy level, $\varepsilon = 0.5$ as a medium privacy level and $\varepsilon = 1$ as a low privacy level. It is observed that for $(\varepsilon = 0.05)$, high magnitude noise is generated by the Exponential noise as compared to the Laplace and Gaussian mechanism. This behavior is due to the fact that exponential distribution has a heavier tail as compared to Laplace and Gaussian noise. This means that probability of generating larger noise values is higher in the case of Exponential noise. This larger noise magnitude in Exponential noise provide stronger privacy protection or achieve a high level of randomness, but they

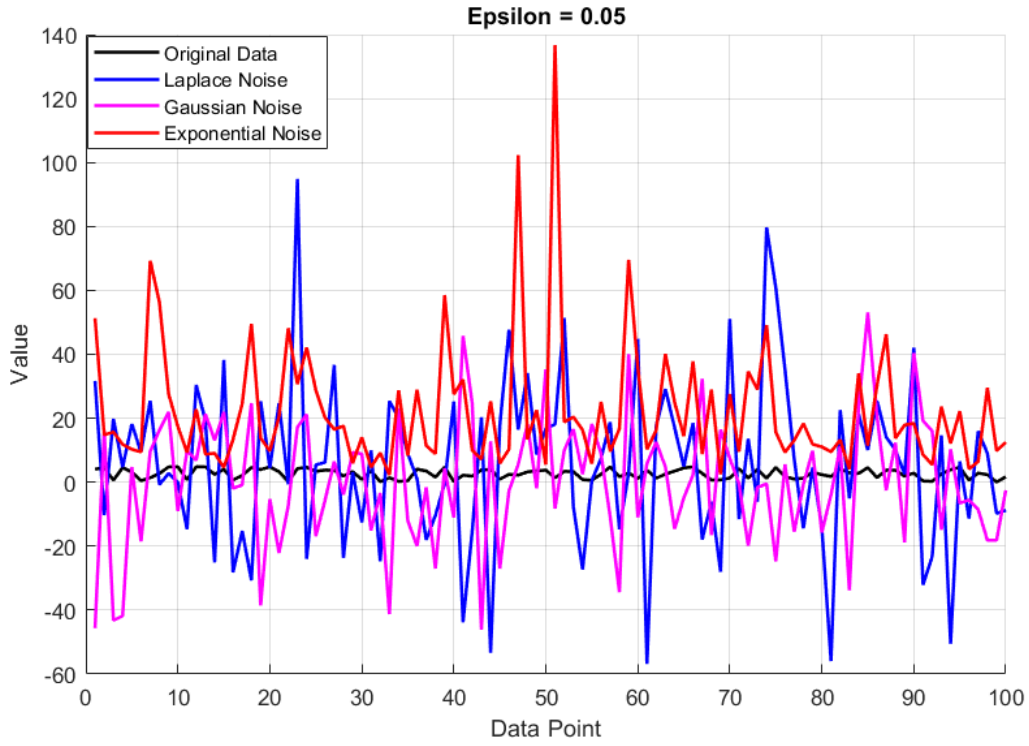

Figure 27: Impact of noise at epsilon=0.05- High Privacy Level

also introduce more distortion or perturbation to the data. To simulate a blockchain network, a quorum based blockchain network of four nodes is created using chain-hammer [83] as a benchmark tool for the performance analysis of our proposed framework with the same specification of the local machine as mentioned in section 5.7. We evaluated the performance of three different consensus protocols i-e RAFT, IBFT and PoA. The evaluation involves sending transactions across various loads including 1000 txs, 2000 txs, 5000txs, 7000 txs and 10,000 txs respectively over the BC network. To comprehensively analyze the performance of our blockchain network in terms of throughput and latency, we employed two modes of transmission sequential mode and multi-threaded mode. In sequential mode, each task needs to wait for the completion of the previous task before it can start. While in multi-threaded mode, operations are performed in a parallel fashion and we have used 3 threads in our simulation due to hardware limitations we have on our local machine.

Also applying differential privacy in conjugation to blockchain often requires complex

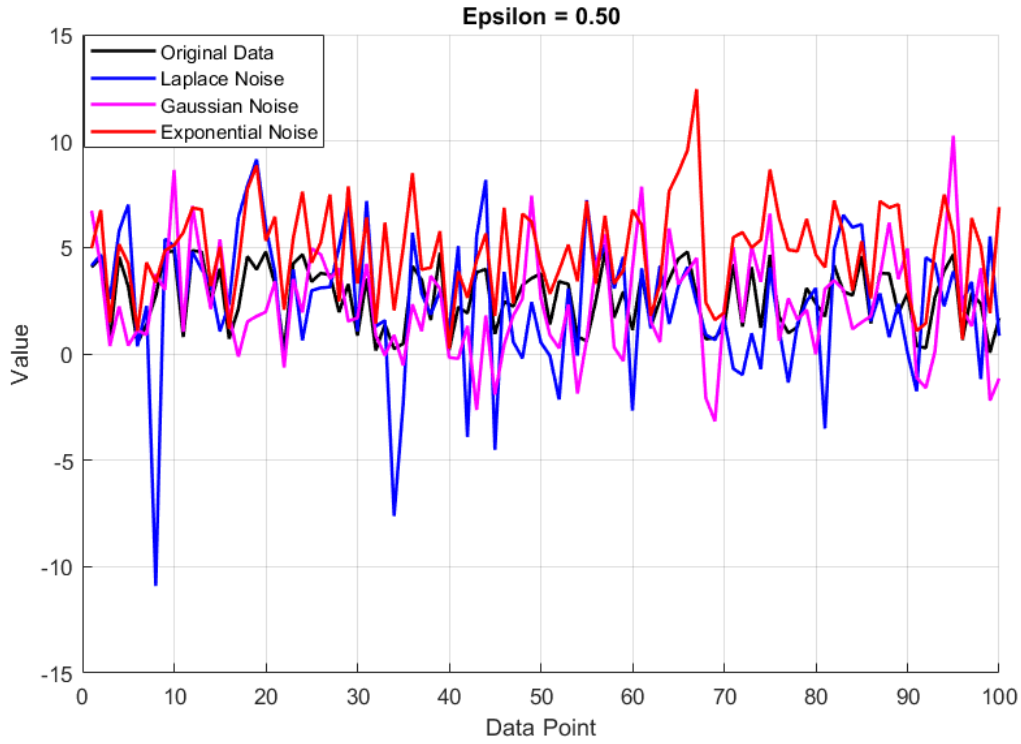

Figure 28: Impact of noise at epsilon=0.5- Medium Privacy Level

mathematical operations, such as the calculation of sensitivity values, noise addition, and data aggregation, to achieve the desired privacy guarantees. These computationally intensive tasks can place a significant load on the CPU and memory resources of the local machine, particularly when scaling the number of blockchain nodes and the volume of transactions. Improvements such as scaling up the local machine, using a dedicated server, and implementing distributed simulation, can help overcome the limitations and further improve the blockchain network's performance.

Foregoing, to evaluate the performance of the proposed framework in terms of throughput, Fig. 30, Fig. 31 and Fig. 32 represents the comparison of sequential mode of transmission and evaluate the performance of RAFT, IBFT and PoA consensus protocols in variation to different epsilon values or privcay levels for all the three kind of noise i-e Laplace, Gaussian and Exponential noise. In terms of throughput performance, PoA outperforms

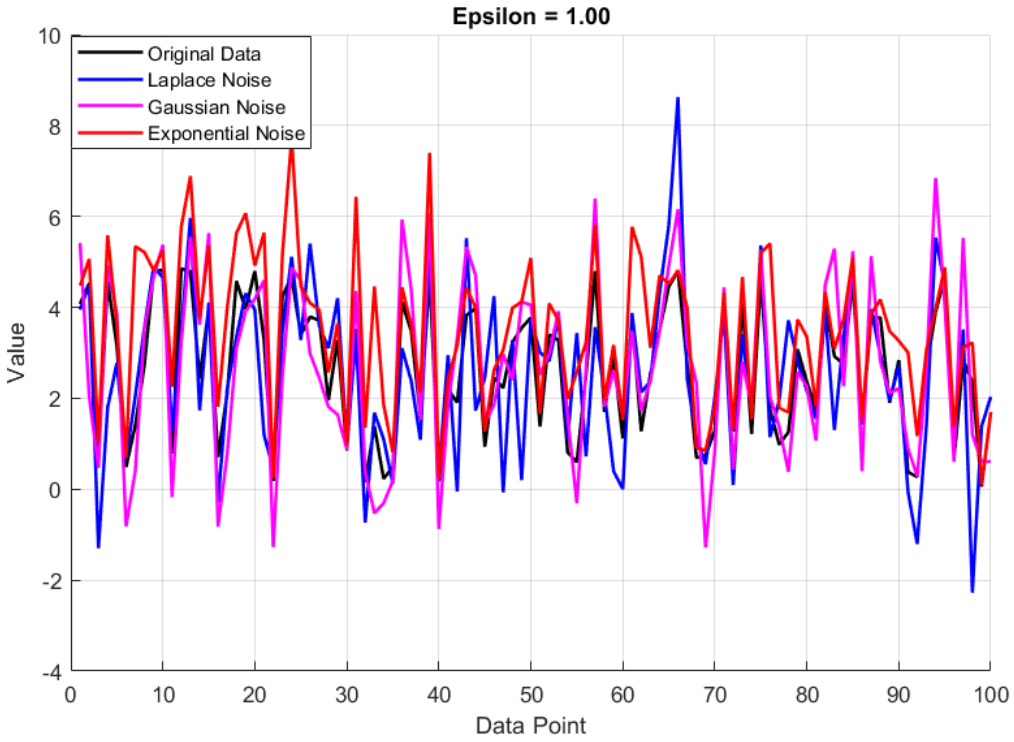

Figure 29: Impact of noise at epsilon=1- Low Privacy Level

IBFT and RAFT due to the fact that PoA relies on a limited number of pre-selected authorities or validators to validate transactions and create new blocks. Additionally, the simulation results iterate that Laplace noise provides higher throughput as compared to Gaussian as well as exponential noise for each consensus protocol that is implemented and it is due to the fact that both Gaussian noise and exponential noise tends to have a larger magnitude due to heavier tail. This means that probability of generating larger noise values is higher both in case of Gaussian and Exponential mechanism. Additionally, calculating a square root of the variance to determine the standard deviation of the distribution is also relatively an expensive operation in the Gaussian mechanism. All these factors favours Laplace mechanism to provide better throughput as compare to Gaussian and Exponential mechanism.

It is important to mention here that at low epsilon values i-e. at $\varepsilon = 0.05$, more noise is added as compare to higher epsilon values therefore the performance of blockchain in terms of throughput increases as we increase from $\varepsilon = 0.05$ to $\varepsilon = 1$. For instance when

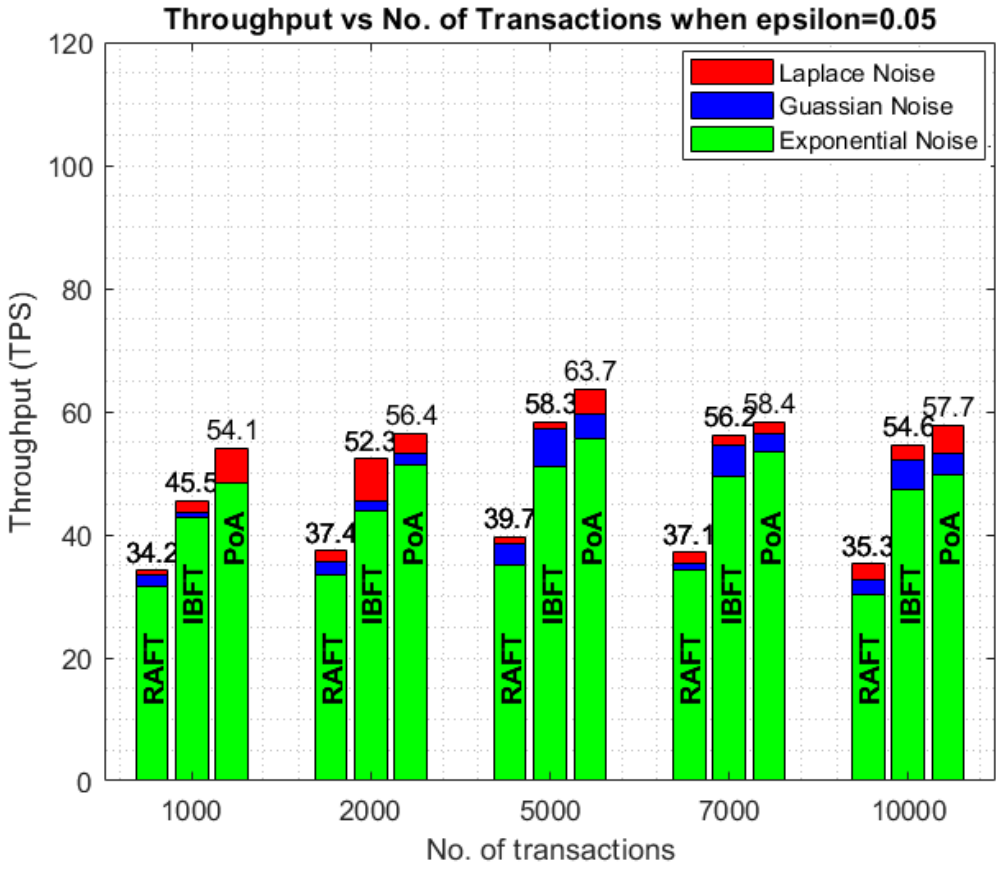

Figure 30: Sequential throughput at epsilon=0.05- High Privacy Level

processing 5000 transactions in sequential mode, PoA achieves the highest throughput of 67.5 TPS for $\varepsilon = 0.5$ among the implemented network as depicted in Fig. 31. Furthermore, it is also observed that as we increase the number of transactions, throughput decreases which is due to an increase in communication overhead and workload both in the case of RAFT and IBFT. Similarly evaluating the performance in terms of throughput for all the three consensus protocols at $\varepsilon = 1$, where comparatively less noise is generated as compared to low epsilon values, an enhanced throughput is observed as compared to $\varepsilon = 0.05$ and $\varepsilon = 0.5$. For example at 5000 transactions, PoA offers higher throughput of 70.5 TPS in the presence of Laplace noise when compared to IBFT and RAFT where throughput is limited to 65.7 and 48.3 TPS respectively as shown in Fig. 32. When comparing the

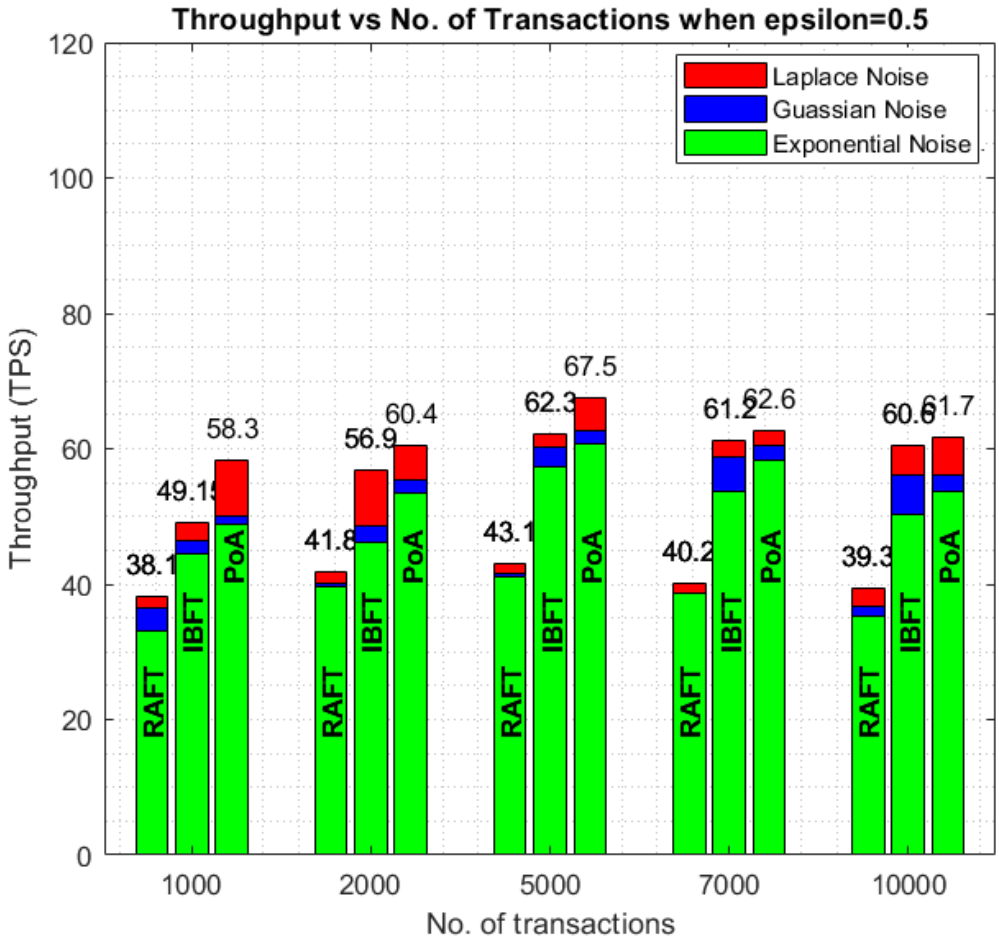

Figure 31: Sequential throughput at epsilon=0.5- Medium Privacy Level

performance of the sequential mode of operation with the multi-threaded mode, it is evident, as shown in Figure 33 that the multi-threaded mode achieves higher throughput. This can be attributed due to the parallel execution of operations, resulting in improved speed and enhanced processing. In order to fully evaluate the performance blockchain, multiple simulations are conducted using different epsilon values and analyze the performance of PoA, IBFT and RAFT for Laplace noise, Gaussian noise and Exponential noise. At low epsilon values i-e. at $\varepsilon = 0.5$ and $\varepsilon = 1$, an accelerated throughput is observed as compared to a sequential mode where PoA outperforms both IBFT and RAFT respectively. For instance as shown in Fig. 35 , for the 5000 transactions at $\varepsilon = 1$, PoA achieves 73.5 TPS as

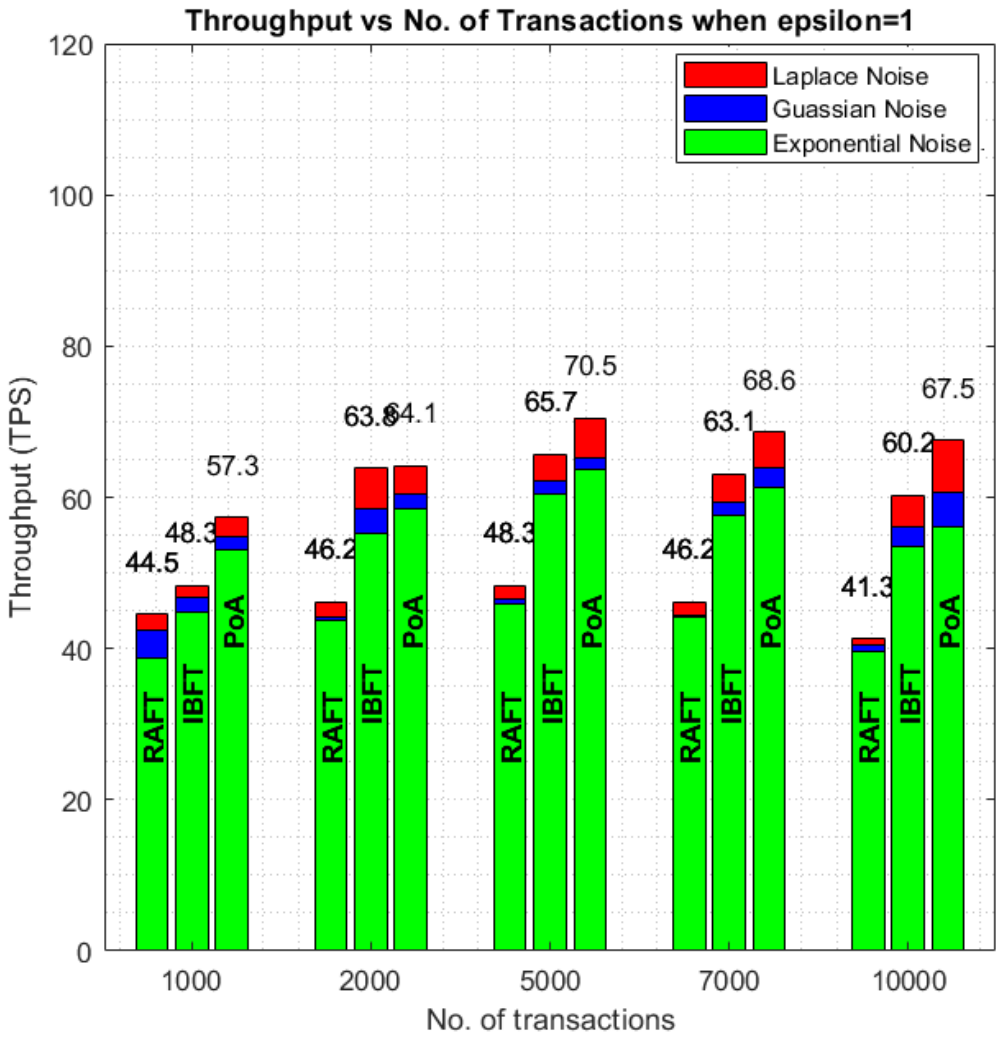

Figure 32: Sequential throughput at epsilon=1- Low Privacy Level

compared to IBFT and RAFT which are at 69.5 TPS and 46.8 TPS respectively. It is important to mention here that similar to the sequential mode, the throughput decreases as the number of transactions increases. This trend highlights that as the length of the blockchain increases, the throughput decreases.

Furthermore, to give more insight into the performance evaluation, overall transaction latency both for sequential mode and multi-threaded mode for Laplace, Gaussian and Exponential noise at different epsilon values are also plotted. As expected for Laplace noise,

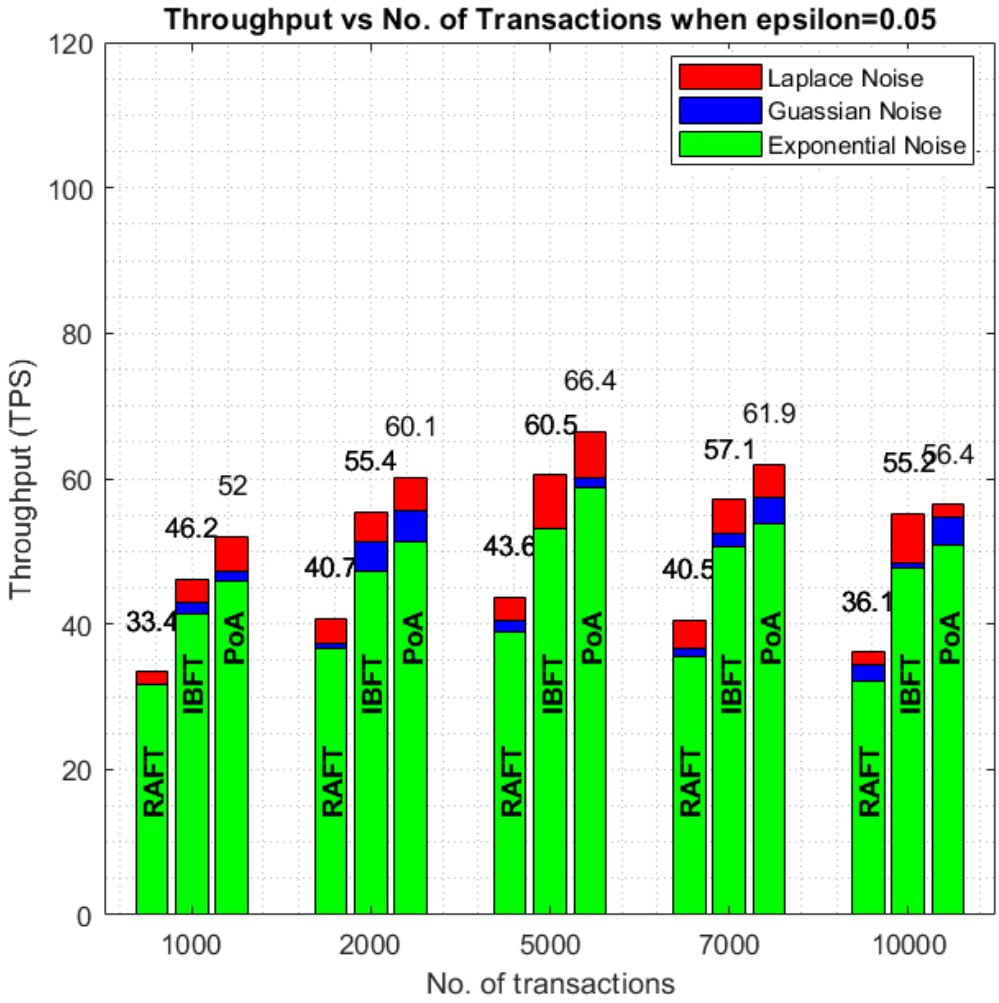

Figure 33: Multi threaded throughput at epsilon=0.05- High Privacy Level

PoA overall shows the lowest latency as compared to IBFT and RAFT. For instance for sequential mode of transmission at $\varepsilon = 0.05$ which is considered as high privacy level in our simulation as shown in Fig. 36, PoA achieves a delay of 78.49 sec, while IBFT and RAFT exhibits a delay of 85.76 sec and 125.94 sec respectively. Similarly for $\varepsilon = 1$ for sequential mode of transmission at 10,000 transactions as shown in Fig. 38, PoA has a delay of 148.14 sec as compared to IBFT and RAFT which have the convergence time of 166.11 sec and 242.13 sec respectively. The overall delay shows an increasing trend with an increase in number of transactions. As the number of transactions increases, it takes longer wait times

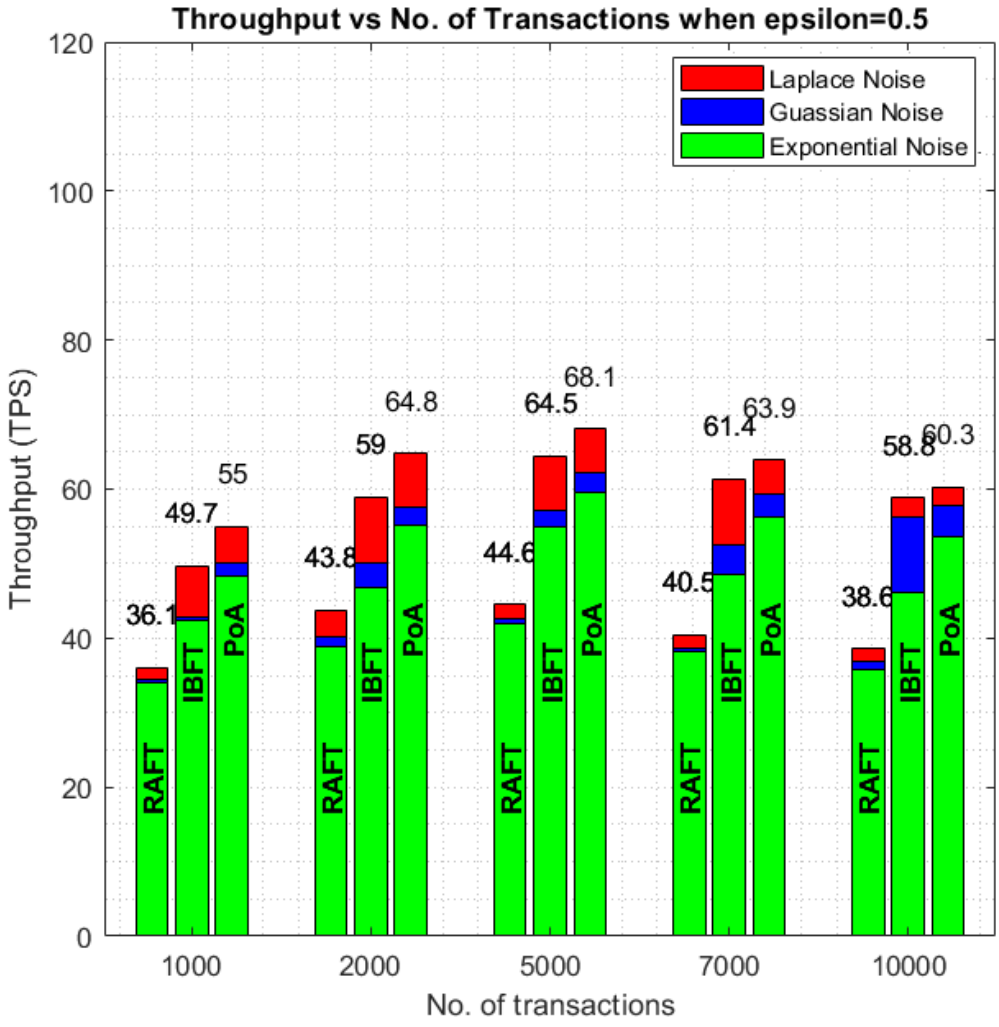

Figure 34: Multi threaded throughput at epsilon=0.5- Medium Privacy Level

for transactions to be confirmed and added to the blockchain, leading to increased delay. It is also evident from the simulation results that latency increases as the epsilon values decrease. This is because at low epsilon, higher magnitude of a noise is added leading to the increase in delay.

Similarly latency plot for multi-threaded environment is also plotted across multiple values of epsilon. At high epsilon values i-e.at $\varepsilon = 1$ and $\varepsilon = 0.5$, PoA encounters the lowest delay as compared to IBFT and RAFT. For example as shown in Fig. 41, PoA experiences a delay of 68.0 sec at $\varepsilon = 1$ for processing 5000 transactions, while IBFT has a

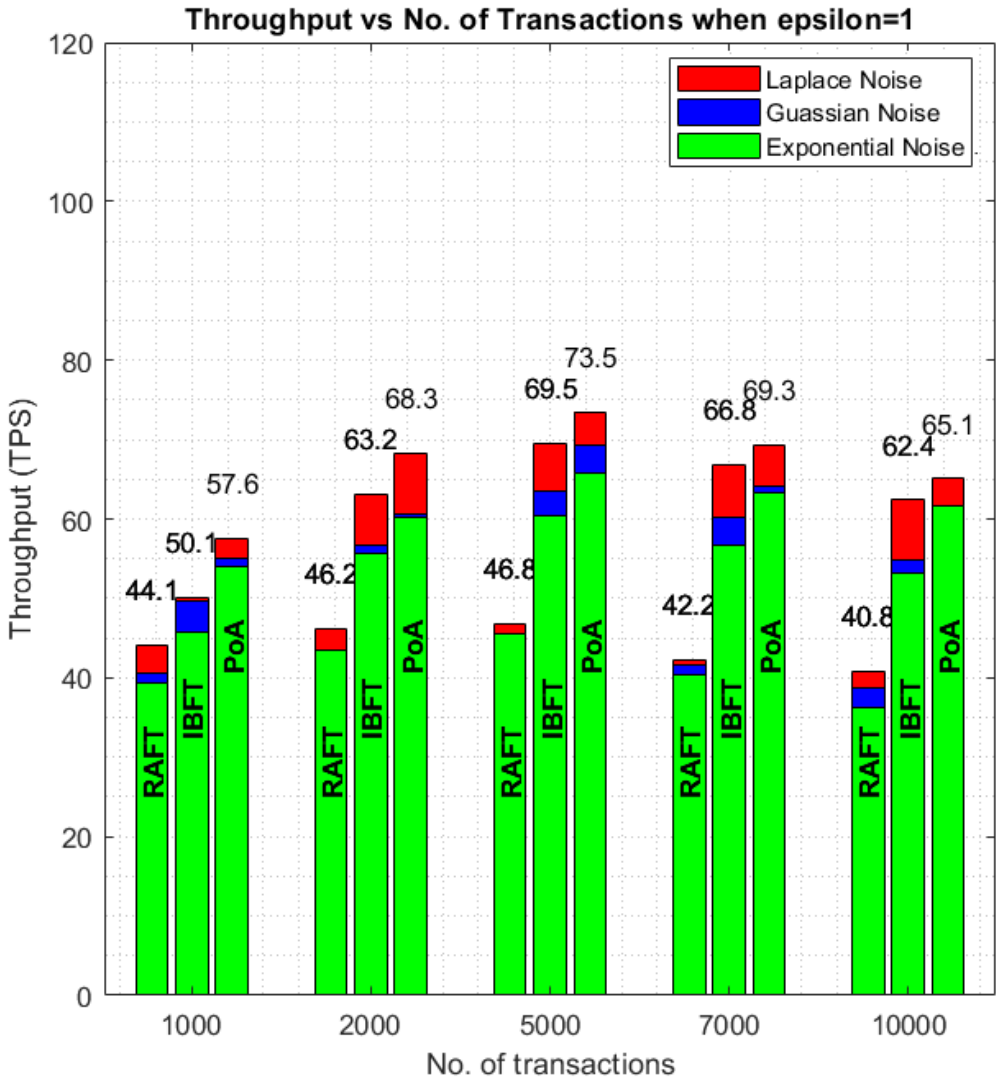

Figure 35: Multi threaded throughput at epsilon=1- Low Privacy Level

delay of 71.94 sec and a delay of 106.83 sec for RAFT respectively. When compared with Gaussian noise and Exponential noise, an increase in delay is experienced for all epsilon values due to the high computation involved while generating both the noises. Similarly, an increase in delay is also observed in multi-threaded environments as well with an increase in number of transactions due to the fact that large number of transactions need to wait for subsequent blocks to be mined. To conclude, Laplace noise along PoA proves itself to be a well adapted consensus algorithm and performs better in terms of throughput and latency

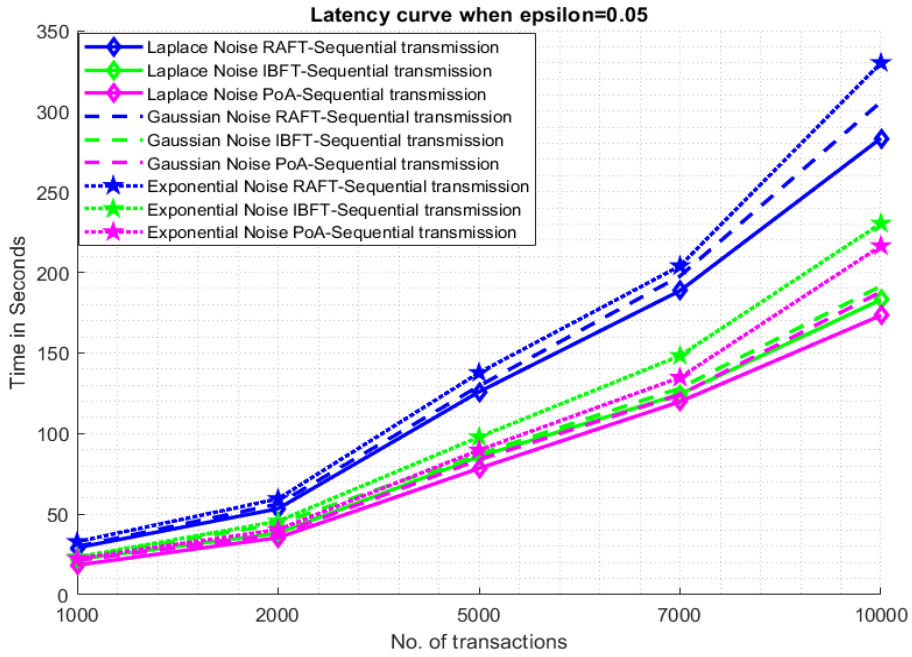

Figure 36: Sequential latency at epsilon=0.05 - High Privacy Level

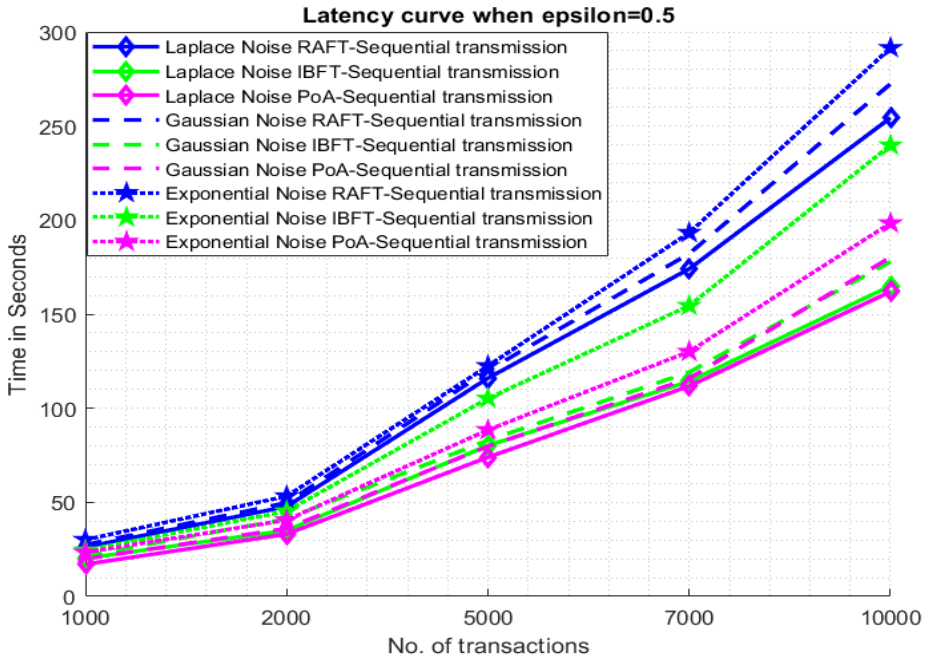

Figure 37: Sequential latency at epsilon=0.5- Medium Privacy Level

both for sequential and multi-threaded modes of transmission. In the context of differential privacy, PoA can add noise to the data with a smaller range or magnitude due to the limited

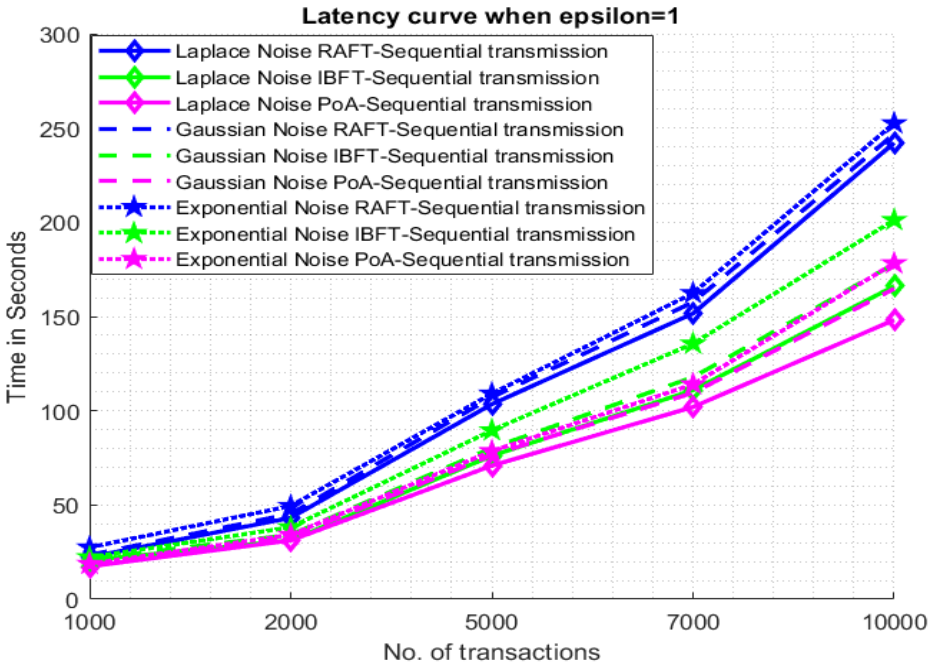

Figure 38: Sequential latency at epsilon=1- Low Privacy Level

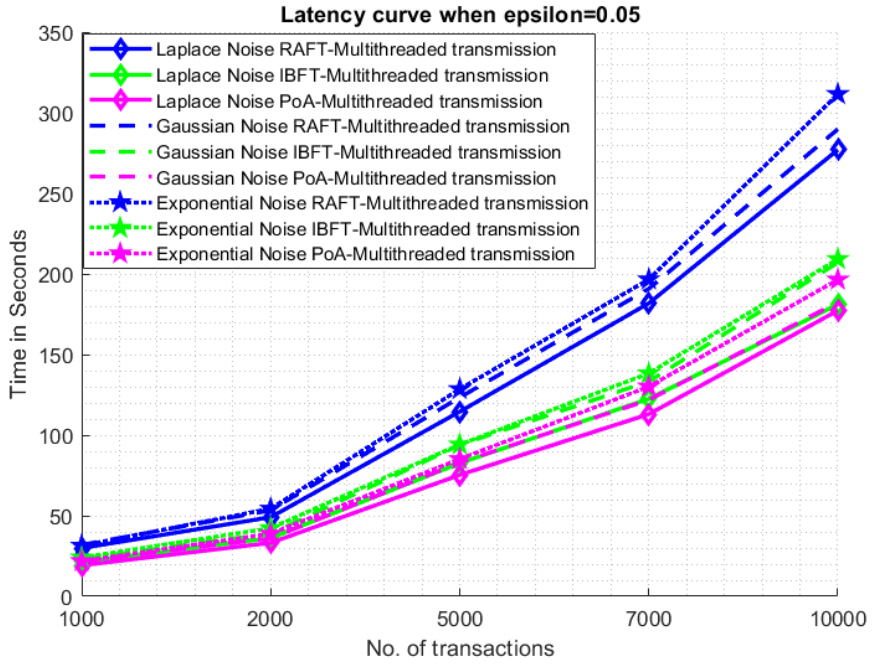

Figure 39: Multi threaded latency at epsilon=0.05- High Privacy Level

number of authorities. As a result, the added noise may have a lesser impact on the utility of the data, allowing PoA to provide better performance or accuracy in low privacy settings.

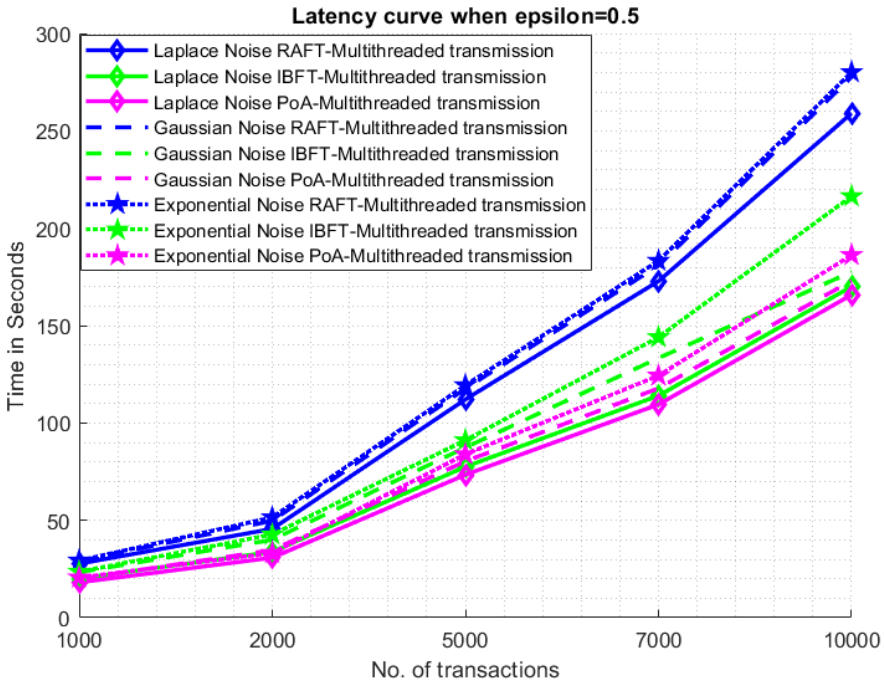

Figure 40: Multi threaded latency at epsilon=0.5- Medium Privacy Level

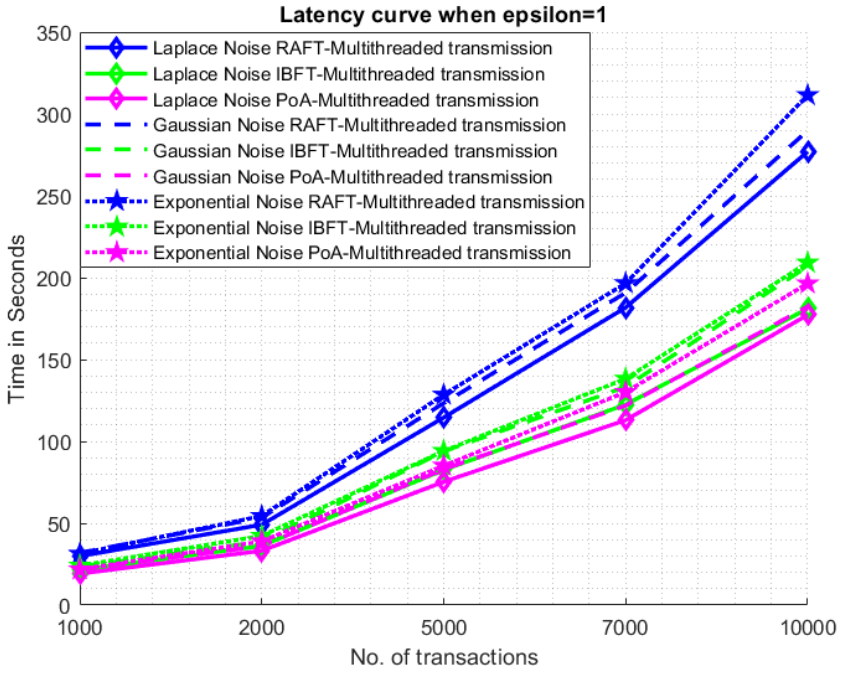

Figure 41: Multi threaded latency at epsilon=1- Low Privacy Level

These results can be considered as a first milestone for exploring blockchain in this domain and can pave the path for subsequent integrating with MIoT in blockchain networks using differential privacy mechanisms.

6.6 General Guideline for Adopting Differential Privacy in Healthcare Domain

The application of differential privacy techniques in the MIoT domain provides a promising approach to address the critical challenge of preserving individual privacy while enabling the beneficial use of medical data. The key takeaway from this research is that by carefully designing and implementing differential privacy mechanisms, MIoT systems can strike a balance between data utility and robust privacy protection. When applying differential privacy in practice, it is essential to consider the following guidelines:

- Understand the trade-off: Recognize that the use of differential privacy involves a trade-off between data utility and the level of privacy protection. Carefully evaluate the specific requirements and constraints of your MIoT application to find the optimal balance.

- Tailor the differential privacy mechanisms: Differential privacy techniques should be tailored to the unique characteristics and data requirements of the MIoT ecosystem. This may involve selecting appropriate privacy parameters, noise addition mechanisms, or other customization's to ensure effective privacy protection.

- Calibrate the noise carefully: The addition of noise is a critical component of differential privacy, and the level of noise must be carefully calibrated to strike the right balance between privacy protection and data utility.

- Ensure transparency and accountability: Implement transparent mechanisms like blockchain that allow users, regulators, and other stakeholders to understand and

validate the privacy-preserving measures employed. This can help build trust and facilitate the adoption of differential privacy-based MIoT solutions.

- Continuously monitor and adapt: Regularly review the performance and effectiveness of the differential privacy mechanisms in the MIoT environment. Adapt the approaches as necessary to address evolving privacy threats, technological advancements, and changing regulatory requirements.

  By following these guidelines, organizations and practitioners can leverage the power of differential privacy to unlock the benefits of MIoT while prioritizing the protection of sensitive medical data and ensuring the trust of patients and healthcare providers in a real world environment.

CHAPTER VII

SUMMARY AND CONCLUSION

In this thesis, we present a novel solution to address the privacy preservation issues while integrating Medical Internet of Things (MIoT) with traditional patient healthcare records (PHRs). Our two innovative frameworks, namely the Enhanced Privacy Preservation Based Blockchain Mechanism (EPIoT) and the Differential Privacy Preserving (DPP) framework leverages blockchain technology to ensure data integrity, transparency, and auditability in the PHR system. EPIoT framework employ service-oriented layers approach in which each layers operate independently of each other, providing a flexible architecture for the MIoT ecosystem. The service-oriented layer approach comprises of four key layers:registration layer, authentication layer, privacy enforcement layer, and transaction layer to provide a complete end-to-end framework specifically for the MIoT devices. Additionally, the framework will provide the functionality of setting the privacy preference by the data owner for each data stream generated by an IoT device and provide a decentralized privacy compliance check so that it can be auditable as well. The low complex consensus algorithm like RAFT, IBFT and, PoA and low computation cryptography mechanism adopted in our proposed system model to suit best for the MIoT devices.

To further surmount the privacy preservation issues in MIoT based blockchain network and to further enhance the privacy protection, we have proposed the DPP framework. DPP is a mathematical framework that ensures strong privacy guarantees. By implementing DPP at the stream level generated by IoT devices, it provides a rigorous mathematical framework that provides provable privacy guarantees, making it a more robust and reliable approach compared to the blockchain-based mechanism used in EPIoT. The DPP framework injects three different types of noises: Laplace noise, Gaussian noise, and Exponential

noise, which are applied strategically to achieve privacy preservation. We have introduced a novel concept of privacy levels, which are adjustable by data owners as low, medium, and high. This flexibility addresses the varying privacy requirements of different applications and empowers data owners to customize the level of privacy preservation according to their specific needs. The impact of different parameters on the effectiveness of the approach is analyzed, providing recommendations for tuning.

Both the proposed frameworks were evaluated through comprehensive simulations to assess their effectiveness in addressing security and privacy concerns in the patient health record system. In the EPIoT framework, the performance evaluation was conducted by deploying a quorum blockchain network. The performance of the proposed architecture was assessed in terms of throughput (transactions processed per second) latency and block generation time. For each type of transaction sent, the simulation is evaluated using two modes of transmission i-e., sequential mode of transmission and multi-threaded transmission, and evaluates the performance of each network in terms of throughput and latency. On the other hand, in the DPP framework, a benchmark study between privacy and utility was first conducted and implemented in Matlab. Our results demonstrate that increasing the privacy parameter, such as the amount of noise added, can increase the level of privacy but decrease the accuracy of the data, and similarly decreasing the privacy parameter will increase the utility. To support our argument, we plotted the privacy and utility curve for all three kinds of noises (Laplace, Gaussian, and Exponential). Further to simulate a blockchain network, a quorum-based blockchain network is created, and evaluated the performance in terms of throughput and latency by setting the privacy level as low, medium, and high. Simulations are repeated for both the sequential mode of transmission and the multi-threaded mode of transmission in the DPP framework. Simulations demonstrated the efficacy of both frameworks, showing high levels of privacy preservation while upholding data utility and blockchain consistency. Furthermore, to demonstrate the efficacy of the approach, a security analysis of the proposed framework was conducted using the AVISPA

tool, and the results confirmed that the framework attains the desired security goals.

The integration of MIoT with PHRs has the potential to significantly improve the quality of care by providing accurate diagnosis, real-time data, and improved data analysis for doctors. However, privacy concerns surrounding PHRs necessitate robust solutions such as the EPIoT and DPP frameworks to ensure the confidentiality and privacy of patients' sensitive health information.

The findings of this research contribute to the field of healthcare systems by providing practical and scalable solutions for secure and privacy-preserving PHR systems. The proposed frameworks can serve as a foundation for future research and development in secure and privacy-aware healthcare applications, fostering trust and enabling the responsible use of MIoT technologies in healthcare.

REFERENCES

[1] F. Daidone, B. Carminati, and E. Ferrari, "Blockchain-based privacy enforcement in the iot domain," *IEEE Transactions on Dependable and Secure Computing*, 2021.

[2] N. Ahmad, P. Laplante, and J. F. DeFranco, "Life, iot, and the pursuit of happiness," *IT Professional*, vol. 22, no. 6, pp. 4–7, 2020.

[3] X. Ding, D. Clifton, N. Ji, N. H. Lovell, P. Bonato, W. Chen, X. Yu, Z. Xue, T. Xiang, X. Long, K. Xu, X. Jiang, Q. Wang, B. Yin, G. Feng, and Y.-T. Zhang, "Wearable sensing and telehealth technology with potential applications in the coronavirus pandemic," *IEEE Reviews in Biomedical Engineering*, vol. 14, pp. 48–70, 2021.

[4] G. W. M. A. R. J. W. E. Luo, M. Z. A. Bhuiyan and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[5] C. Xu, N. Wang, L. Zhu, K. Sharif, and C. Zhang, "Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8345–8356, 2019.

[6] E. Aguiar, B. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys*, vol. 53, pp. 1–27, 03 2020.

[7] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[8] A. El Bekkali, M. Essaaidi, M. Boulmalf, and D. el Majdoubi, "Systematic literature review of internet of things (iot) security," *Advances in Dynamical Systems and Applications*, vol. 16, pp. 1671–1692, 01 2022.

[9] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in iot," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 4, p. 100158, 2023.

[10] M. Ogonji, G. Okeyo, and J. Wafula, "A survey on privacy and security of internet of things," *Computer Science Review*, vol. 38, p. 100312, 11 2020.

[11] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: Ongoing challenges and research opportunities," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pp. 230–234, 2014.

[12] N. Khan, A. Awang, and S. A. Abdul Karim, "Security in internet of things: A review," *IEEE Access*, vol. PP, pp. 1–1, 01 2022.

[13] C. Xu, N. Wang, L. Zhu, K. Sharif, and C. Zhang, "Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8345–8356, 2019.

[14] J. Huang, M. Sharaf, and C.-T. Huang, "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud," in *2012 41st International Conference on Parallel Processing Workshops*, pp. 279–287, 2012.

[15] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 131–143, Jan 2013.

[16] T. Munirathinam, S. Ganapathy, and A. Kannan, "Cloud and iot based privacy preserved e-healthcare system using secured storage algorithm and deep learning," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 3, pp. 3011–3023, 2020.

[17] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 5, pp. 37–42, 2015.

[18] L. Selvam and R. Arokia, "Secure data sharing of personal health records in cloud using fine-grained and enhanced attribute-based encryption," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, (Coimbatore, IN), pp. 1–6, IEEE, 2018.

[19] G. Aceto, V. Persico, and A. Pescapò, "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0," *Journal of Industrial Information Integration*, vol. 18, p. 100129, 2020.

[20] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, pp. 461–466, 2016.

[21] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 850–880, 2019.

[22] S. Shi, D. He, L. Li, N. Kumar, M. Khan, and K. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & Security*, vol. 97, p. 101966, 2020.

[23] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[24] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 850–880, 2019.

[25] N. Szabo, "Smart contracts: building blocks for digital markets," *EXTROPY: The Journal of Transhumanist Thought*, vol. 16, 1996.

[26] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[28] T. Dinh, R. Liu, M. Zhang, G. Chen, B. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[29] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[30] "Hyperledger." https://www.hyperledger.org, 2017.

[31] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

[32] ConsenSys, "Quorum whitepaper." https://github.com/ConsenSys/quorum-docs/blob/master/Quorum

[33] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," in *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[34] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proceedings of the 2014 USENIX Conference*, (Philadelphia, PA, USA), pp. 305–320, 2014.

[35] H. Moniz, "The istanbul bft consensus algorithm," *arXiv preprint arXiv:2002.03613*, 2020.

[36] P. Szil agyi, "Eip-225: Clique proof-of-authority consensus protocol." https://eips.ethereum.org/EIPS/eip-225, 2017.

[37] E. Brewer, "Towards robust distributed systems," in *Proceedings of the Nineteenth Annual ACM Symposium on Principles of Distributed Computing*, (Portland, OR, USA), pp. 343477–343502, 2000.

[38] L. Lamport, "The part-time parliament," *ACM Transactions on Computer Systems*, vol. 16, no. 2, pp. 133–169, 1998.

[39] M. Vukoli c, "The quest for scalable blockchain fabric: proof-of-work vs. bft replication," in *Open Problems in Network Security* (J. Camenisch and D. Kesdo gan, eds.), pp. 112–125, Springer, 2015.

[40] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[41] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[42] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," in *Proceedings of the 22nd International Conference on Data Engineering (ICDE)*, (Atlanta, GA, USA), p. 24, 2006.

[43] N. Li, T. Li, and S. Venkatasubramania, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proceedings of the IEEE 23rd International Conference*, pp. 106–115, 2007.

[44] C. Gentry, *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[45] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*, pp. 169–178, 2009.

[46] J. Rodriguez, D. Schreckling, and J. Posegga, "Addressing datacentric security requirements for iot-based systems," in *Proceedings of the International Workshop on Secure Internet of Things (SIoT)*, pp. 1–10, 2017.

[47] P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Generation Computer Systems*, vol. 76, pp. 540–549, 2017.

[48] Y. Huang, "Secure multi-party computation," in *Responsible Genomic Data Sharing* (X. Jiang and H. Tang, eds.), pp. 123–134, Academic Press, 2020.

[49] C. Wang, S. Wang, X. Cheng, Y. He, K. Xiao, and S. Fan, "A privacy and efficiency-oriented data sharing mechanism for iots," *IEEE Transactions on Big Data*, vol. 9, no. 1, pp. 174–185, 2023.

[50] Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, p. 1054, 2014.

[51] H. A. Eds and D. Hutchison, "A dynamic distributed architecture for preserving privacy of medical iot monitoring measurements," in *Proc. Int. Conf. Smart Homes Health Telemat.*, pp. 146–157, 2018.

[52] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for iot data analytics," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 20–25, 2018.

[53] M. Fernández, M. Kantarcioglu, and B. Thuraisingham, "A framework for secure data collection and management for internet of things," in *Proc. 2nd Annu. Ind. Control Syst. Security Workshop*, pp. 30–37, 2016.

[54] K. Jung and S. Park, "Grayscale access control: Applying differential privacy to access control for internet of thing environment," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, pp. 849–854, 2017.

[55] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, pp. 461–466, 2016.

[56] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 850–880, 2019.

[57] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[58] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, pp. 1–7, 2018.

[59] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, 2018.

[60] L. Cheng, J. Liu, C. Su, K. Liang, G. Xu, and W. Wang, "Polynomial-based modifiable blockchain structure for removing fraud transactions," *Future Generation Computer Systems*, vol. 99, pp. 154–163, 2019.

[61] J. Z. D. B. D. L. X. Liang, S. Shetty and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," *Springer*, vol. 10, no. 10, 2017.

[62] V. Costan and S. Devadas, "Intel sgx explained," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 86, 2016.

[63] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[64] M. S. F. G. X. T. H. Li, L. Zhu and S. Liu, "Blockchain-based data preservation system for medical data," *Jounral of Medical System*, vol. 42, pp. 1–13, 2018.

[65] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, p. 140, June 2018.

[66] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "Bpds: A blockchain based privacy-preserving data sharing for electronic medical records," 11 2018.

[67] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.

[68] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

[69] S. Pournaghi, M. Bayat, and Y. Farjami, "Medsba: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, 11 2020.

[70] D. J. M. L. X. Yue, H. Wang and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Jounral of Medical System*, vol. 40, pp. 1–8, 2016.

[71] E. Zaghloul, T. Li, and J. Ren, "Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts," *2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 375–379, 2019.

[72] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[73] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[74] P. Li, C. Xu, H. Jin, C. Hu, Y. Luo, Y. Cao, J. Mathew, and Y. Ma, "Chainsdi: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2042–2053, 2020.

[75] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2169–2176, 2020.

[76] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 69–79, 2018.

[77] L. H. . X. J. Qian, Z, "A differential privacy-preserving framework for smart contracts in blockchain," *IEEE Access*, vol. 8, pp. 186525– 186532, 2020.

[78] J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, and J.-P. Hubaux, "Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, pp. 1413–1426, 2018.

[79] A.-E. R. A.-E. A. . A.-G. A. Al Omar, R, "Privacy-preserving data aggregation in miot using blockchain and differential privacy," *IEEE Access*, vol. 7, pp. 5622–5634., 2019.

[80] A. A. H. A. N. B. . B. A. H. Fauzi, I., "Privacy preserving data collection and sharing framework for miot in healthcare using blockchain and differential privacy," *IEEE Access*, vol. 8, pp. 207515–207533., 2020.

[81] L. Vigano, "Automated security protocol analysis with the avispa tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.

[82] Y. Glouche and T. Genet, *SPAN - a Security Protocol ANimator for AVISPA - User Manual*. IRISA / Universit'e de Rennes 1, 2006. 20 pages.

[83] A. Krueger, "Github - drandreaskrueger/chainhammer: fire many transactions at ethereum node, then produce diagrams of tps, blocktime, gasused and gaslimit, and blocksize," 2019. Accessed: 2024-05-30.

VITA

Muhammad Kashif received his BE Electrical Engineering from the Department of Electrical Engineering, University of Engineering and Technology (U.E.T) Peshawar, Pakistan in 2009. He completed his M.S Electrical Engineering from the Department of Electrical Engineering, University of Engineering and Technology (U.E.T) Taxila,Pakistan, in 2014. He is pursuing his Ph.D. at the Department of Computer Science, Ozyegin University, Istanbul, Turkey under the supervision of Professor Kubra Kalkan. His research interests include network security, Internet of things, and Blockchain.