Designing Quantum-Safe Lattice-Based Multi-Authority CP-ABE Scheme for Blockchain-Enabled IoT-Based Consumer Healthcare Electronics

Prithwi Bagchi, Abhishek Bisht, Ashok Kumar Das, *Senior Member, IEEE*, Neetesh Saxena, M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*—Despite edge computing reducing communication delays associated with cloud computing, privacy concerns remain a significant challenge when sharing data from edge-based consumer electronics (CE) or Internet-of-Things (IoT) devices. Ciphertext policy attribute-based encryption (CP-ABE) is a cryptographic tool that facilitates intricate and refined access control. It can deliver more flexible, secure, compact, and effective access control policies for the cloud data. In the case of a conventional CP-ABE scheme, the keys can only be issued and disseminated by a trusted central authority (CA). However, if the CA is compromised, the entire system becomes more susceptible to assaults or failures, which leads to a single-point failure. In this article, we propose a Ring-Learning with Errors (Ring-LWE)-based MA-CP-ABE scheme that is effectively resolved by the multi-authority CP-ABE (MA-CP-ABE), and it ensures the security against quantum attacks. The threshold secret sharing by Shamir and the Lagrange interpolation formula are applied in the key-generation and decryption procedures of the proposed scheme, which make it easier to segment and restore the private keys. The proposed scheme is implemented in the CE-enabled IoT-based smart healthcare applications using the blockchain technology as a secure storage. A detailed comparative study, security analysis and experimental results with the existing relevant schemes shows that the proposed scheme exhibits superior security and better efficiency as compared to other schemes, demonstrating its feasibility in practical IoT-based healthcare applications.**

***Index Terms*—Consumer electronics, Edge devices, Internet of Things (IoT)-based smart healthcare, Post-quantum cryptography, Blockchain, Security.**

This work was supported by the Researchers Supporting Project number (RSP2024R32), Riyadh, Saudi Arabia. This work was also supported by the Information Security Education & Awareness (ISEA) Phase III Project, Ministry of Communication and Information Technology, Department of Electronics and Information Technology, Government of India. *(Corresponding authors: Ashok Kumar Das; M. Shamim Hossain).*

Prithwi Bagchi and Abhishek Bisht are with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: prithwi.bagchi@research.iiit.ac.in, abhishek.bisht@research.iiit.ac.in).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

Neetesh Saxena is with the School of Computer Science and Informatics, Cardiff University, Cardiff CF24 4AG, UK (e-mail: saxenan4@cardiff.ac.uk).

M. Shamim Hossain is with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 13273, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

I. Introduction

The advancement of network connectivity enhances the rapidity of the transfer of information and increasing the capacity of storage which in turn promotes the expansion of cloud computing. Cloud computing offers users the convenience of sharing their data, which mitigates expenses associated with local data management. In the context of daily existence, cloud storage is indispensable. Nevertheless, specific information, like healthcare data, can be extremely sensitive.

Consumer electronics encompass a wide range of devices intended for personal use, primarily focused on communication, entertainment, and convenience [1]. These products are typically designed with user-friendly interfaces, compact forms, and integration into digital ecosystems. Technological advancements have driven the growth of smart consumer electronics, leveraging artificial intelligence, cloud computing, and wireless technologies to offer personalized experiences and automation. These devices facilitate seamless communication, deliver engaging entertainment, and boost productivity, becoming an essential part of modern life and showcasing the fusion of innovation and everyday convenience.

Consumer electronics play a crucial role in smart IoT-based healthcare systems by facilitating advanced health monitoring and management through integration with connected platforms [2]. Wearable devices gather continuous health data and interact with IoT-enabled systems to process the information, identify irregularities, and deliver meaningful insights. Additionally, portable medical gadgets contribute to improved patient care by providing real-time diagnostics and enabling remote monitoring. This application of consumer electronics fosters efficient, personalized healthcare, improving patient outcomes and reducing reliance on traditional in-person consultations.

Edge computing introduces distinct security challenges, including the risk of unauthorized access and interception of sensor data from connected devices by hackers. Ensuring security in edge environments remains a persistent challenge due to the complexity and widespread nature of their network topologies. Additionally, IoT devices are particularly susceptible to hacking because of their constrained computing resources and low resistance to sustained attacks, particularly against quantum attacks [3].

Multiple encryption schemes have been devised to safeguard

the data stored in cloud storage. Using the concept of identity based encryption, an attribute based encryption (ABE) was proposed by Sahai *et al.* [4]. In the ABE scheme proposed in [5], every individual user contains a collection of attributes that can serve as a representation of their identity. A collection of attributes are used by data owner to produce the ciphertext labels, whereas users can acquire his/her own private keys from the "Key Generation Center (KGC)" according to his own attributes. A user may able to decode the encrypted ciphertext and obtain the plaintext data, if the attributes using in the access policy of the data user can satisfied by the attribute set of the data owner. Later, fine-grained access control is made possible by the ABE scheme. ABE is categorized into two different types: 1) "Key-Policy Attribute-Based Encryption (KP-ABE)" [6] and 2) "Ciphertext-Policy Attribute-Based Encryption (CP-ABE)" [7]. In a variety of applications, CP-ABE offers a robust framework for secure and flexible sharing of information, since the data owners have direct control over the access policies for their shared data.

With the proliferation of highly interconnected and data driven smart healthcare applications [8], it is crucial to safeguard sensitive, important and operational information. This is particularly true in case of an Internet of Things (IoT) environment, where the smart devices are in a state of continuous communication, necessitating the accurate authentication of their identities. Typically, ABE schemes are employed to implement smart healthcare applications [9]. At present, the majority of healthcare oriented ABE schemes [10] depend on the bilinear pairings, that rely on the hardness of the "Diffie-Hellman problem (discrete logarithm problem)". These ABE schemes are inefficient because of their high computation and communication latency, as well as their inability to withstand quantum attacks using the Shor's algorithm [11], which makes a threat on the sensitive medical data. The "post-quantum cryptographic (PQC)" techniques, such as the lattice-based CP-ABE scheme [12], performs exceptionally well in safeguarding the sensitive medical data from the adversaries. The hardness of the lattice structures guarantees the security of the lattice-based CP-ABE schemes against quantum attacks along with it reduces the computation and communication overhead of such CP-ABE schemes. The most of lattice-based CP-ABE schemes rely on "Ring-Learning With Errors (Ring-LWE)" [13] or "Learning With Errors (LWE)" [13] hard problems.

Ajtai *et al.* [14] were the pioneers in developing lattice-based encryption. The approach they took demonstrates that the time necessary to compromise the algorithm is equivalent to the time required to solve the "Shortest Vector Problem (SVP)" [15], thereby ensuring data security. Nevertheless, their approach was impractical, inefficient, and posed a risk of errors during decryption. Goldreich *et al.* [16] introduced a scheme, which involves the implementation of a trapdoor through lattices. Subsequently, numerous additional lattice-based encryption schemes implemented using this concept. The scheme [16] is highly efficient; however, but it lacks a rigorous security proof, and there is a possibility that the ciphertext could disclose certain information about the plaintext. In order to enhance the security, Micciancio suggested an another scheme [17]. Nevertheless, their scheme's efficiency is reduced as a result of the expensive storage cost. Gentry *et al.* [18] constructed and standardized the "trapdoor functions in lattice-based encryption" in accordance with the LWE problem. The straightforward expression of these trapdoor functions made them extensively used in lattice-based encryption schemes.

LWE is one of the usable average-case lattice problems. At the outset, numerous extant schemes are founded on LWE, which guarantee their security. An LWE based scheme, suggested by Regev [19] was capable to resist both the "chosen plaintext attack (CPA)" and the "chosen ciphertext attack (CCA)". The storage cost of LWE-based schemes is substantial, which suggests that they have an excessive computational complexity. So when take the smart IoT applications, that generates an immense amount of data, hence the most urgent issue is data storage. Then LWE based schemes ensures that they are typically ineffective for practical IoT-based application due to the high data storage. The most significant average-case lattice problem pertinent to the practical CP-ABE schemes [13] is Ring-LWE, which is designed to decrease the computational burden as well as to provide the high security. There is an immense volume of data being generated and transmitted in smart healthcare-based CP-ABE scheme. It is crucial to minimize the computational overhead and preserve the security of sensitive healthcare data. These huge amount of data issue might be resolved by transferring data to the cloud servers, which will be semi-trusted [20]. The bilinear pairing was employed to construct the majority of the current CP-ABE schemes [21], [22], but it is not sufficiently secure or efficient in the current context. To ensure the security, Chaudhary *et al.* [23] proposed a "lattice-based secure cryptosystem for smart healthcare in smart cities environment", where they employed a mutual authentication and a lightweight key exchange mechanism, which is employed to verify the queries between cloud storage and a variety of end users, including patients and doctors. Also, Gupta *et al.* [24] proposed a "lightweight lattice-based authentication and access control protocol" applied in smart IoT based health systems, which also prevents the quantum attacks. In a similar way, Haritha *et al.* [25] proposed a "lattice-based access control protocol", where the blockchain stores and accesses the patient's e-health information as immutable blocks. In the context of the CP-ABE scheme [26], the health records of patients, such as medical history and lab results, are stored in an encrypted format. Decryption and access to particular records are restricted to authorized personnel who possess the necessary qualifications. This guarantees that only those who require confidential information have access to it. Additionally, in [27], the attribute-based key distribution improves key administration in large healthcare institutions where the roles for users are regularly updated, because it also distributes decryption keys based on user attributes.

CP-ABE guarantees that access control policies can be effectively administered and maintained as the number of users and data increases [28]. Healthcare applications may reach an elevated level of safety, confidentiality, and regulatory conformance by implementing a CP-ABE method depends on the lattice structure. This ensures the protection of sensitive patient data and the facilitation of efficient and flexible access control from quantum threat. In order to achieve the aforementioned

benefits, it is imperative to establish a healthcare oriented blockchain based CP-ABE scheme using the Ring-LWE [13].

A. Motivation

The necessity of a centralized authority to manage and distribute the encryption keys is diminished by the CP-ABE schemes [13]. The "Multi-Authority CP-ABE (MA-CP-ABE)" scheme [29] is an improvement on the conventional CP-ABE scheme that incorporates multiple attribute authorities. Consequently, MA-CP-ABE schemes are intended to be immune to collusion attacks and the risk of the exposure of a single authority is mitigated by the dependence on multiple authorities [29]. In order to mitigate the substantial computational overhead and safeguard the conventional MA-CP-ABE schemes from the quantum threats, adoption of an efficient MA-CP-ABE method depends on the lattice-structure is very important [29]. Generally, in the smart healthcare applications, a vast quantity of sensitive data has been produced. So, it is necessary to reduce computational overhead and ensure the security of such private and confidential data. For this reason, in this article, we would like to build a more flexible, scalable and efficient blockchain based smart healthcare oriented lattice-based MA-CP-ABE scheme, which can simultaneously guarantee that the access policies remain hidden to those parties who are illegitimate and can provide desirable security of attributes.

B. Research Contributions

The key contributions of this paper are delineated as follows:

- We develop a "multi-authority CP-ABE scheme based on the lattice structure in a distributed environment for consumer electronics based IoT-enabled smart healthcare applications". Our scheme supports the trapdoor generation and Gaussian pre-image sampling techniques. Implementation of the trapdoor generation is substantially reduced the computational overhead associated with the keygen phase, and Gaussian pre-image sampling guarantees that the pre-images are statistically comparable to the discrete Gaussian distribution [30], ensuing 'integrity' security aspect.
- The proposed scheme that has been developed regards the numerous authorities as synchronized servers. During the encryption phase, a linear secret sharing scheme is implemented, while the Lagrange interpolation is utilized in the decryption phase to facilitate the recovery of the plaintext. The security proof of the proposed scheme ensures that the scheme is secure against "indistinguishable under selective chosen plaintext attack (IND-sCPA)" along with the hardness of Ring-LWE ensures the resistance of the scheme against quantum attacks. Informal security analysis shows that the scheme is secure against various attacks including the various quantum attacks.
- We implement the proposed scheme in the smart healthcare applications to guarantee the security and the confidentiality of the medical information. In an effort to mitigate the substantial storage expenses, the blockchain technology has been incorporated in this scheme. We utilize the Hyperledger Sawtooh framework in the blockchain simulation. Also to evaluate the computational time needed for the various phases in our scheme, we design a testbed experiment.

C. Outline

The paper is organized as follows. Section II provides a critical review of the existing schemes in the literature. The relevant mathematical preliminaries are then provided in Section III. The system models containing the network model and threat model are discussed in Section IV. In Section V, we discuss the existing algorithms relevant to the derived MA-CP-ABE method that is contingent upon lattice structure. Next, in Section VI we apply the proposed lattice-based MA-CP-ABE scheme in IoT-enabled smart healthcare applications. Section VII provides detail security analysis, including formal and informal security analysis. While Section VIII describes the testbed experiment along with the blockchain simulations, Section IX provides the comparative analysis with the current lattice-dependent CP-ABE/MA-CP-ABE schemes. Section X represents the conclusion of the proposed scheme.

II. Related Work

Fu *et al.* [31] presented an offline/online lattice-based CP-ABE framework, that splits the executions into offline and online stages, where their scheme works under the premise of Ring Learning with Errors (Ring-LWE). Their proposed scheme is single-authority based. Prior to the attributes being specified, the offline phase of the private key creation [31] generates an intermediate private key, and the online stage then constructs the corresponding private key depending on the attributes. In the encryption process of [31], the offline stage produces an intermediate ciphertext prior to defining of the plaintext message and access policy, handling the complex computations required for encryption. Subsequently, in their scheme, the final ciphertext is generated during the online phase. Their scheme also described a system architecture that is appropriate for mobile devices. Their method offers resilience against quantum attacks, and it drastically reducing the amount of time and space needed through Ring-LWE.

Utilizing the "Ring Learning With Errors (Ring-LWE) hardness", Sun *et al.* [29] presented a decentralized multi-authority CP-ABE scheme that enables flexible access policies, and leverages a new lattice trapdoor for G-lattices over rings to boost effectiveness. Several authorities are in charge of managing and distributing private keys in their system [29]. Their method [29] is well-suited for dispersed storage environments since it segments and reconstructs private keys during key generation and decryption using Shamir's threshold secret sharing and the Lagrange interpolation algorithm. Additionally, they proved that the scheme in [29] is selectively secure from chosen plaintext attacks.

Regarding cloud storage applications, Zhao *et al.* [28] suggest a reversible lattice-based CP-ABE method (RL-ABE). Their RL-ABE method is meant to withstand assaults from both collusion and quantum attacks. Their RL-ABE scheme [28] is generated by first building trapdoor functions that provide public/secret key pairs for attributes and secret values.

These key pairs are then integrated with the CP-ABE structure through the application of the Ring-LWE hardness. Their scheme [28] guarantees users' rights to fine-grained access control over shared data. Their scheme also facilitates attribute revocation, which makes it easy for users to renew their attributes and provide or remove access permissions.

Yang *et al.* [32] designed a "multi-authority and multi-valued attribute-supporting revocable and multi-authority CP-ABE (RM-CP-ABE) scheme for cloud computing based on the hardness of the Ring-LWE problem". Several authorities can take part in key distribution with this method, and this scheme has an attribute revocation function that lets users alter their attributes whenever necessary. Their method resists quantum attacks due to the Ring-LWE hardness.

Yao *et al.* [33] devised a technique, called multi-authority attribute-based encryption (MA-ABE) to ensure static security against arbitrary collusion in the random oracle model. [33] combines a two-stage lattice sampling technique, a monotonous linear secret sharing scheme (M-LSSS), and a global ID model. A disjunctive normal form (DNF) formula represents the scheme's access policy. Their method fine-tunes the settings based on Sample-pre by integrating the SampleLeft algorithm into the two-stage sampling procedure. The scheme's resilience against quantum attacks stems from its reliance on the Learning With Errors (LWE) assumption, although at the cost of more computing complexity. Their approach leads to reduced key sizes and shorter ciphertexts, which is an improvement over Datta *et al.* [34].

Finally, Table I provides the description and limitations of the existing lattice-based CP-ABE schemes.

III. Mathematical Background

This section contains the pertinent mathematical preliminaries required for the development of the proposed scheme.

1) Lattice and its Hard Assumptions: $\mathbb{N}$ represents the collection of natural numbers, and α is an element in $\mathbb{N}$, i.e. $\alpha \in \mathbb{N}$, such that $f = 2^{\alpha} \in \mathbb{N}$. Consider q to be a large prime for which $q \equiv 1 \pmod{2f}$ is satisfied. We shall now consider a finite field $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ along with the ideal $< x^f + 1 >$, which is produced by an irreducible polynomial $x^f + 1$. An expression $R = \mathbb{Z}[x]/ < x^f + 1 >$ that represents a ring, which can be written as follows: $R = \{\Psi(x) : \Psi(x) = \sum_{u=0}^{f-1} B_u x^u \ : \ \forall u \in \{0, 1, \cdots, f-1\}, B_u \in \mathbb{Z}\}$, with $\mathbb{Z}$ represents the set of all integers. An analogous a finite field $R_q = \mathbb{Z}_q[x]/ < x^f + 1 >= \{\Psi(x) : \Psi(x) = \sum_{u=0}^{f-1} D_u x^u : \forall u \in \{0, 1, \cdots, f-1\}, D_u \in \mathbb{Z}_q\}$ is established. A positive integer d is defined as $0 < d < \sqrt{q}$, under the condition that $d \leq (q-1)/2$. A subset of R_q is designated as $R_{q,d} = \{\Psi(x) : \Psi(x) = \sum_{u=0}^{f-1} D_u x^u : \forall u \in \{0, 1, \cdots, f-1\}, D_u \in [-d, d]\}$. The term $\overline{H}$ denote hash functions, which is described as $\overline{H} : \mathbb{Z}_q^f \rightarrow R_q$. For $m \geq 1$, R_q^m represents a column vector, which contains m number of polynomials selected from R_q, and $R_q^{1 \times m}$ is the row vector that contains m number of polynomials chosen from R_q. Sample u from R_q involves arbitrarily selecting a polynomial from R_q. Furthermore, N is the total number of authorities, the user attribute set is denoted by S_{uid} and $S_{uid,\theta} (\subseteq S_{uid})$ that incorporates attributes specific to the authority AA_{θ}. Additionally, W' symbolizes the user's access policy.

2) Ring Learning with Errors (Ring-LWE): Lattice based cryptosystem (LBC)'s security is significantly enhanced by the Ring-LWE [13], which is based on the principles of LWE. In modern times, the security of the preponderance of lattice-based schemes is also determined by the hardness of the Ring-LWE [35] hardness. The following is a description of the Ring-LWE. Select a polynomial $a \in R_q$ with a maximal degree of $f-1$ and another polynomial $s \in_R R_q$ with a degree that does not surpass $f-1$. Considering an error distribution χ defined over R, $D_{s,\chi}$ represents as the Ring-LWE distribution which produces the output as $(a, a.s + e \pmod{x^f + 1}) \in R_q \times R_q$, e denotes the error, and select uniformly at random from the error distribution χ. Now, let us presume that given $\{(a_i, e_i); i \in [m]; m \geq f\}$, where the e_i's are selected uniformly at random from χ, and $a_i \in R_q$, for $i \in [m]$. Extracting the secret s by utilizing m instances $\{(a_i, a_i.s + e_i \pmod{x^f + 1}); i \in [m]\}$ is very difficult, where s is sampled from the uniform distribution over R_q.

The details of other preliminaries like binary decomposition of R_q elements, discrete Gaussian, trapdoor generation, Gaussian pre-image sampling, Linear Secret Sharing Scheme (LSSS), generalized Multi-Authority Ciphertext Policy Attribute-based Encryption (MA-CP-ABE) scheme, and its security framework are provided in the supplementary material.

3) RingSamplePre Algorithm [36]: This algorithm takes a public matrix $A \in \mathbb{R}_q^{1 \times m}$ with an associated trapdoor basis T_A, a target vector $v \in \mathbb{R}_q$, and the Gaussian parameters $\sigma, \sigma_s > 0$, and then outputs a perturbation vector $l \in R_q^m$, and a short pre-image vector $M \in \mathbb{R}_q^m$ that satisfies the equation: $J^T.Y = v - A \cdot l$, where Y is generated from R_q^k. The following are the steps involved in this algorithm:

Step 1 (Generate disturbance vector l and a set of polynomials Y): Generate a collection of polynomials $l \in R_q^m$ from a discrete Gaussian distribution $l \sim D_{\Lambda,\sigma}$ using the trapdoor T_A, along with a set of polynomials $Y \in R_q^k$.

Step 2 (Computation): For $i = 0, 1, \cdots, m-1$:
if $i = 0$, then compute $M_0 = l_1 + e.Y$; if $i = 1$, then compute $M_1 = l_2 - r.Y$; if $2 \leq i \leq k+1$, then compute $M_i = l_{i+1} + Y[i-1]$; else compute $M_i = l_{i+1}$.

Step 3 (Verification): Verify if $A.M = v$. If it is valid, then return M; else, return error.

IV. System Model

In this section, we discuss both the network as well as threat models that are applied in the design of the proposed scheme.

A. Network Model

The network is made up of many healthcare applications, which is described in Fig. 2. Each IoT-based healthcare application domain containing the consumer electronics is composed of the authorized hospital authority, which is also known as the registration authority, their associated departments, along with the data owner acting on the edge devices, the data user, and the medical authority aligned with the

TABLE I
DESCRIPTION AND LIMITATIONS OF EXISTING LATTICE-BASED CP-ABE SCHEMES

Scheme	Description	Drawbacks/Limitations
Fu *et al.* [31] (2022)	It is based on computational Ring-LWE hardness. It is resistant to quantum attacks, while offline/online techniques enhance efficiency.	It depends on a single authority, making it vulnerable if compromised. Its centralized nature helps in reducing effectiveness.
Sun *et al.* [29] (2021)	In this scheme, Lagrange interpolation and Shamir's secret sharing split and reconstruct private keys in KeyGen and Decryption, which enable multi-authority support. Ring-LWE hardness also ensures quantum resistance.	No blockchain implementation or real-world IoT applications for this scheme is provided. This scheme also requires a large private key size.
Zhao *et al.* [28] (2022)	This scheme enables fine-grained access control by securely revoking and renewing user rights based on attributes. Ring-LWE hardness ensures resistance to quantum attacks for this scheme.	It lacks a blockchain implementation and has a large plaintext size.
Yang *et al.* [32] (2022)	This technique is suited for cloud computing, by supporting multiple authorities and attributes. Based on computational Ring-LWE assumption, it is safe against quantum and CPA attacks. It also provides a testbed experiment.	The expense of generating the ciphertext becomes substantial. There is no implementation of blockchain in this scheme.
Yao *et al.* [33] (2024)	The scheme is quantum secure. A testbed experiment is also included in their scheme.	Use of LWE causes a significant computational cost. Moreover, the scheme is inefficient for practical IoT-based applications.

hospital authority. The trusted hospital authority registers each individual authority in the existent departments within the hospitals along with the associated data owner, data user and the medical authority.

Each individual authority in the existing departments affiliated with a specific trusted hospital authority sends a set of attributes from their attribute set to the data user. Following this, data user generates their attribute sets using the received attribute sets from each individual authority. In conjunction with each individual authority generates a unique set of secret keys based on their attribute sets, which are then forwarded to the data user. Subsequently, the data user generates their secret key by utilizing the secret keys that have been provided by each individual authority associated with the specific hospital authority. The data owner chooses the medical data from their respective IoT-based healthcare consumer electronics devices and generates the plaintext message, over which they implement the lattice-based MA-CP-ABE mechanism to generate the ciphertext, and using this encrypted ciphertext, data owner produces a transaction. The transaction is then forwarded to the relevant medical authority by the data owner. The medical authority validates the transaction's freshness by verifying the timestamp mechanism once obtaining it from the associated data owner. If the timestamp mechanism is effectively validated for the received transaction, the medical authority will store it in their own database. After storing n_t number of successfully verified transactions, medical authority proceeds to generate a block, Block. Given that the medical authorities associated with the various application domains form a peer-to-peer (P2P)-CS network, the Block is incorporated into the blockchain centre through the consensus algorithm. This system is distinguished by its extensive computational capabilities and storage capacity.

B. Threat Model

By employing the public (insecure) channel, each individual authority affiliated with the hospital transmits a set of attributes along with secret keys to the data user. Subsequently, using the insecure medium, each individual authority associated with the hospital forwards the access structure to the data owner and the data owner transmitted the generated transaction to the relevant medical authority connected with the hospital through a public channel. Security is a substantial challenge due to the fact that all the information are communicated by a public channel. The proposed scheme takes into account the existing widely recognized threat models that comprises the "Dolev-Yao (DY)" [37], "Canetti and Krawczyk (CK)" [38], "Honest-But-Curious (HBC)" and "extended CK-adversary (eCK)" models [39], [40].

- The DY-threat model presupposes that an adversary, such as $\mathcal{A}$, is a prohibited entity that has the capacity to intercept/delete/modify the messages used for communication. Additionally, $\mathcal{A}$ possesses the capability to add forged messages into the communication channel.
- The adversary $\mathcal{A}$ shall be regarded as a passive adversary under the "Honest-but-Curious (HBC) adversary model". This implies that $\mathcal{A}$ is a legitimate entity and adheres to the established protocol. Nevertheless, $\mathcal{A}$ may be interested in obtaining knowledge regarding the data that is being transmitted among the network's entities.
- The basic requirement for the adversary $\mathcal{A}$ in the CK-adversary model is that it keeps to every one of the characteristics outlined in the DY-threat model. The CK-adversary paradigm provides $\mathcal{A}$ with the supplementary capacity to gain confidential information and session states by employing the "session hijacking attacks". The release of short (temporal) and long-term secrets can also be facilitated through the compromise of the session state.
- The eCK-adversary model is a variation of the CK-adversary model. As a result of its enhanced capabilities, $\mathcal{A}$ is more powerful than the adversary in the CK paradigm. It is conceivable that these supplementary capabilities could include the capacity to actively generate potential query sequences in order to maintain the session's freshness. Therefore, the eCK-adversary model offers $\mathcal{A}$ with improved functionalities that permits it to compromise or impede communication.

The data owner cannot be monitored continuously in 24×7 times due to the challenging circumstances of healthcare applications. As a result, the adversary $\mathcal{A}$ may commit quantum side-channel attacks, including power analysis attacks, to retrieve confidential medical data from the compromised, physically captured data owner's memory. Furthermore, $\mathcal{A}$ is authorized to launch a lattice-reduction attack in order to identify a short vector to recover the private keys. It is presume that the hospital authority, individual authority associated with each departments, medical authority will not be physically compromised, thereby enabling them to be protected with physical locking mechanisms. However, the hospital authority and departments are treated as the fully trusted entities, whereas medical authorities are considered as the semi-trusted entities.

V. Proposed Lattice-Based Multi-authority CP-ABE Scheme

An efficient "lattice-based multi-authority CP-ABE technique" is outlined in this section. The global setup phase is initially conducted by a trusted party, called KGC, to produce the public parameters pp, and unique identifiers for each authorized users and authorities. Each authority then proceeds with the AASetUp phase, during which their respective secret and public keys are generated. Every authority creates an access policy, which is then sent to the data owner. An access policy that the data owner creates by combining the access policies they have received. After that, the data owner collects a message and encrypt such message, i.e., producing the encrypted ciphertext during the encryption phase, which is then uploaded to the P2P-CS network. Then, the data user retrieve the encrypted ciphertext. In order to decrypt this encrypted ciphertext, the data user must submit a request to each authority to obtain an attribute set and the private key set. The ciphertext may only be decrypted by the data user only if their attribute satisfies the access policy requirements. Each phase is explained in detail below. Table II specifies the notations and their respective interpretations.

TABLE II
Notations and their meanings

Symbol	Description
KGC	Trusted key generation center (Control Room)
pp	Public parameters generated by KGC
f, m, q	Positive power of 2 which represents the degree of an irreducible polynomial; A positive integer have the following form $\lfloor \log_2 q + 1 \rfloor + 2$; Sizable prime number given that $q \equiv 1 \pmod{2f}$
bin_q	A binary decomposition function.
AA_θ, h_θ	The authority identified by θ; Total number of attributes corresponding to the authority AA_θ.
χ'_θ, S	The attribute set corresponding to the authority AA_θ; The entire amount of attributes set by the KGC in [28].
R_q	A finite field of the type: $\mathbb{Z}_q[x]/ < x^f + 1 >$, where $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$, and $q \equiv 1 \pmod{2f}$
N, $[N]$, J	Total number of authorities involving in this scheme.; A set $\{1, 2, \cdots, N\}$; A set represents the collection of attributes involving in the ciphertext in [28].
u, $S_{uid,\theta}$, S_{uid}	A polynomial chosen uniformly at random from R_q; Attribute set generated by the authority AA_θ for the data user uid; Attribute set of the user uid.
uid_i $S_{uid_i,\theta,B}$, $S_{uid_i,B}$	i^{th} data user associated with the B^{th} hospital; Attribute set produces by the authority AA_θ associated with the B^{th} hospital for the corresponding i^{th} data user uid_i; Attribute set generated by the i^{th} data user uid_i associated with the B^{th} hospital.
$y_{uid,\theta}$, SK_{uid}	The secret key, produces by the authority AA_θ for the user uid in the KeyGen phase; User, i.e. uid's secret key.
$SK_{uid_i,\theta,B}$, $SK_{uid_i,B}$	Secret key generated by the authority identified as θ associated with the B^{th} hospital for the i^{th} data user; Secret key generated by the i^{th} data user associated with the B^{th} hospital authority.
$RSamplePre$, $TrapGen$	Gaussian Preimage Sampling Algorithm; Trapdoor Generation Algorithm.
M_θ	Output produces by the Trapdoor generation algorithm.
F, W'_θ, W', ct	Share Generating Matrix; The access structure that is generated by the authority AA_θ using the attributes from χ'_θ; Access structure generated by the data owner; Encrypted ciphertext produces by the data owner.
$\lvert W' \rvert, W'_{\theta,B}, W'_B$	Total number of attributes in the access structure W'; Access structure generated by the authority identified as θ associated with B^{th} hospital, where it is composed by the attributes derived from $X'_{\theta,B}$; Access structure generated by the i^{th} data owner DO_i associated with B^{th} hospital.
$R_{q,d}$	Sub-field of R_q, where the interval $[-d, d]$ contains all the coefficients of every polynomial in this subfield, such that $d < \sqrt{q}$
APK'_θ, ASK'_θ	"Public and secret keys" of the authority AA_θ.
$APK'_{\theta,B}$, $ASK'_{\theta,B}$	"Public and secret keys" of the authority AA_θ associated with the B^{th} hospital.
$ID^B_{DO_i}$,	Unique identity of the i^{th} data owner DO_i associated with the B^{th} hospital;
ID^B_{MA}, $ID^B_{uid_i}$	Unique identity of the medical authority associated with the B^{th} application domain; Unique identity of the i^{th} data user associated with the B^{th} hospital.
MA_B , DO_i	Medical authority associated with the B^{th} application domain; i^{th} data owner associated with B^{th} hospital.
$L_i(x, y)$	An unique bi-variate polynomial of degree $f-1$ chosen by the B^{th} hospital.
ϕ	Plaintext message.
ϕ_B, TS_{ϕ_B}, CTS_{DO_i}	Sensing medical data selects by the i^{th} data owner DO_i associated with B^{th} hospital; Timestamp generated by the DO_i associated with B^{th} hospital when the sensing medical data ϕ_B is selected; Timestamp generated by the i^{th} data owner DO_i associated with B^{th} hospital for generating the transaction.
$Data_{\phi_B,DO_i}$, ct_{ϕ_B,DO_i}, TX_{ϕ_B,DO_i}	Plaintext message generated by the DO_i associated with the B^{th} hospital; Encrypted ciphertext generated by the DO_i associated with B^{th} hospital; Transaction generated by the i^{th} data owner DO_i associated with B^{th} hospital on ϕ_B.
η, n_a, n_v	A positive integer that satisfies the conditions $m = \eta.\lvert S \rvert$ in [28]; The number of attributes involving in the access structure in [32]; Represents the number of virtual attributes involving in [32].
n_u, n_τ	Number of attributes that the user possesses in [32]; The quantity of attributes that have been revoked in [32].
$\mathscr{A}, \mathscr{U}, U, y, t_{max}$	The terms are used in the scheme [33].
m_1, m_2	The positive integers are used in the scheme [33], where $m_2 > t_{max}.m_1.\log q + w(\log m_1) + \lambda$.
$\overline{H}(\cdot)$, G, $H(\cdot)$	A "collision-resistant" cryptographic one-way hash function which maps from R_q to R_q; Number of existing departments associated with B^{th} hospital; A "collision-resistant one-way hash function which maps from $\{0,1\}^*$ to $\{0,1\}^*$".

A. GlobalSetUp

The steps that the reliable key generation center (KGC) takes are listed below.

• First, KGC takes the security parameter λ as an input. The KGC choose a polynomial $u(x) = \sum_{j=0}^{f-1} u_j.x^j$ uniformly at random from R_q. After that, KGC produces the public parameters represented by $pp = (q,\ f,\ k,\ \sigma,\ \sigma_s, \overline{H}\ u)$. Here, q represents a sizable prime number, where $\sigma, \sigma_s \geq 0$ stands for the Gaussian parameters.

• It is assumed that there are N authorities in total, and the set of authorities are represented as $\{AA_1,\ AA_2,\ \cdots,\ AA_N\}$. While registering each authority AA_θ, KGC randomly selects a function $E(y)$, where $E(y) = u + \sum_{I=1}^{N-1} G_I y^I \pmod q$, where each G_I is selected randomly from R_q in a uniform manner, $G_I = \sum_{j=0}^{f-1} d_j^I.x^j \in_R R_q$, $\forall I \in [N-1]$. Ultimately, each AA_θ's polynomial value $E(\theta) \in R_q$ is calculated and transmitted to the relevant AA_θ.

B. AASetUp

The following protocols are employed by each authority AA_θ to execute this phase:

• AA_θ begins by running the Ring Trapdoor Generation algorithm, called $RTrapGen$ [41], which produces the outputs as a pair (A_θ, T_{A_θ}), where $A_\theta \in R_q^{1\times m}$, $T_{A_\theta} = (r_\theta,\ e_\theta)$, such that r_θ, and $e_\theta \in R_q^k$. Let $\chi'_\theta = \{x_1, x_2, \cdots, x_{h_\theta}\}$ represents the set of attribute corresponding to the authority AA_θ. For each attribute $x_i \in \chi'_\theta$, AA_θ selects $(b^+_{\theta,i}, b^-_{\theta,i}) \in_R R_q^{1\times m} \times R_q^{1\times m}$.

• Afterward, AA_θ randomly chooses $P_\theta \in R_q^m$, where $P_\theta = (P_{\theta,1},\ P_{\theta,2},\ \cdots,\ P_{\theta,m})^T$. For each $\Pi \in [m]$, AA_θ calculates $bin_q(P_{\theta,\Pi}) = bin_q(P_{\theta,\Pi,0}, P_{\theta,\Pi,1}, \cdots, P_{\theta,\Pi,f-1}) = (\sum_{i=0}^{f-1} P_{\theta,\Pi,i,0}.x^i,\ \sum_{i=0}^{f-1} P_{\theta,\Pi,i,1}.x^i, \cdots, \sum_{i=0}^{f-1} P_{\theta,\Pi,i,\lceil \log q \rceil - 1}.x^i)$.

• The public and secret keys for AA_θ are represented as $\{APK'_\theta\}$ and $\{ASK'_\theta\}$, where $APK'_\theta = \{A_\theta,\ (b^+_{\theta,i},\ b^-_{\theta,i})_{i\in[h_\theta]}\}$, and $ASK'_\theta = \{T_{A_\theta},\ (bin_q(P_{\theta,1}), bin_q(P_{\theta,2}), \cdots, bin_q(P_{\theta,m}))\}$.

C. KeyGen

Each authority AA_θ is responsible for carrying out this phase. Suppose $\theta \in [N]$, uid represents the identity of the user, while the user's attribute set is represented by the symbol $S_{uid} = \cup_{\theta\in[N]} S_{uid,\theta}$, where $S_{uid,\theta} \subseteq \chi'_\theta$. This phase includes the subsequent stages:

• The following operations are performed by AA_θ corresponding to the each attribute $x_i \in \chi'_\theta$, where $i \in [h_\theta]$:

(i). Select $(\zeta^i_{\theta,1},\ \zeta^i_{\theta,2},\ \cdots, \zeta^i_{\theta,m}) \in \mathbb{Z}_q^{m\lceil \log q \rceil}$.

(ii). Calculate $(bin_q(P_{\theta,1}).\zeta^i_{\theta,1},\ bin_q(P_{\theta,2}).\zeta^i_{\theta,2},\ \cdots,\ bin_q(P_{\theta,m}).\zeta^i_{\theta,m})$.

(iii). Compute $y_{\theta,i} = (\overline{H}(bin_q(P_{\theta,1}).\zeta^i_{\theta,1}), \overline{H}(bin_q(P_{\theta,2}).\zeta^i_{\theta,2}), \cdots, \overline{H}(bin_q(P_{\theta,m}).\zeta^i_{\theta,m}))^T$.
Let $y_{\theta,i} \in R_q^m$, for all $\theta \in [N]$, and $i \in [h_\theta]$. Then, corresponding to every one attribute $x_i \in \chi'_\theta$, AA_θ generates

$$n_{\theta,i} = \begin{cases} (b^+_{\theta,i}).y_{\theta,i}, & \text{if } x_i \in S_{uid,\theta} \\ (b^-_{\theta,i}).y_{\theta,i}, & \text{if } x_i \in \chi'_\theta \setminus S_{uid,\theta} \end{cases}$$

• Subsequently, AA_θ computes $\Delta_\theta = E(\theta) - \sum_{i=1}^{h_\theta} n_{\theta,i}$, then executes the Ring Gaussian pre-image sampling algorithm, known as $RSamplePre$ [42], i.e. $RSamplePre(A_\theta, T_{A_\theta}, \Delta_\theta, \sigma, \sigma_s)$ to produces the output represented as M_θ.

• The user's secret key is obtained as $SK_{uid} = \cup_{\theta\in[N]}\{SK_{uid,\theta}\} = \cup_{\theta\in[N]}\{y_{uid,\theta}\}$, where $y_{uid,\theta} = \{ y_{\theta,1}, \cdots, y_{\theta,h_\theta}, M_\theta\}$.

D. Encryption

This phase is conducted by the data owner, with the goal to produce the appropriate ciphertext ct on the plaintext message ϕ. This is achieved through the execution of the following steps, which are defined below:

• The inputs are $\{APK'_\theta\}_{\theta\in[N]}$, along with an "access structure $W' = \cup_{\theta\in[N]}W'_\theta = \cup_{\theta\in[N]}({W_\theta}^+ \cup {W_\theta}^-)$", where W'_θ is the access structure that is determined by the attributes that are assigned by AA_θ, and the plaintext: "$\phi = (\phi_i)_{i\in\{0,\cdots,f-1\}} \in \{0,1\}^f$, such that $\phi(x)$ is a polynomial in R_q". The data owner chooses a share generating matrix $F \in R_q^{h_\theta\times m}$ and a vector $\Sigma = (d,, r_2, \cdots, r_m)$, such that $d \in R_q$ stands for the secret that must be disclosed, for all $i \in [m] \setminus \{1\}$, and a uniform random selection of $r_2, r_3, \cdots, r_m$ are made from R_q.

• The data owner selects an $\tilde{e}$ uniformly at random from R for the subsequent stages:

$*$ Determine c_0 such that "$c_0 = 2.u.d+ \tilde{e}+ \phi\lfloor q/2\rfloor$".

$*$ Sample $e_{\theta,AA_\theta} \in R_q^{1\times m}$ and execute $c_{\theta,AA_\theta} = A_\theta.d + e_{\theta,AA_\theta}$.

$*$ If $x_i \in {W_\theta}^+$, select $e_{\theta,i,1} \in R_q^{1\times m}$ along with $e_{\theta,i,2} \in R_q$ to compute "$c_{\theta,i,1} = (b^+_{\theta,i}).d + e_{\theta,i,1}$, and $c_{\theta,i,2} = (F_{i,1}).u.d+ \sum_{j=2}^m F_{i,j}.r_j + e_{\theta,i,2}$".

$*$ If $x_i \in {W_\theta}^-$, sample $e_{\theta,i,1} \in R_q^{1\times m}$, and $e_{\theta,i,2} \in R_q$. Afterwards, execute "$c_{\theta,i,1} = (b^-_{\theta,i}).d+ e_{\theta,i,1}$ and $c_{\theta,i,2} = (F_{i,1}).u.d+ \sum_{j=2}^m F_{i,j}.r_j+ e_{\theta,i,2}$".

$*$ If $x_i \in \chi'_\theta \setminus W'_\theta$, choose $e^+_{\theta,i,1}$, $e^-_{\theta,i,1}R_q^{1\times m}$, and $e_{\theta,i,2} \in R_q$, and then evaluate "$c^+_{\theta,i,1} = (b^+_{\theta,i}).d + e^+_{\theta,i,1}$, $c^-_{\theta,i,1} = (b^-_{\theta,i}).d + e^-_{\theta,i,1}$, and $c_{\theta,i,2} = (F_{i,1}).u.d + \sum_{j=2}^m F_{i,j}.r_j + e_{\theta,i,2}$".

• Subsequently, the ciphertext is generated as $ct = \{c_0, \{c_{\theta,i,1}, c_{\theta,i,2}\}_{x_i\in W'_\theta,\theta\in[N]}, \{c^+_{\theta,i,1}, c^-_{\theta,i,1}, c_{\theta,i,2}\}_{x_i\in\chi'_\theta\setminus W'_\theta,\theta\in[N]}, \{c_{\theta,AA_\theta}\}_{\theta\in[N]}, W'\}$ by data owner.

• Finally, the data owner forwards (ct, F) to data user.

E. Decryption

This phase involves the following stages to decrypt the encrypted ciphertext ct to recover the original plaintext message ϕ by the data user:

• Given the ciphertext ct, together with the shared generating matrix F associated with the Linear Secret Sharing Scheme (LSSS) scheme [34], and the "set of secret keys $SK_{uid} = \{SK_{uid,\theta}; \theta \in [N]\}$", where $SK_{uid,\theta}$ is the set of secret keys generated by the authority AA_θ corresponding to the attribute sets χ'_θ for the data user, the data user attempts to decrypt ct. The decryption will be unsuccessful, if $(1, 0, \cdots, 0)$ is not present in $Span < F_i; i \in [h_\theta] >$. Otherwise, the data user takes $\{g_i \in \{0,1\}; i \in [h_\theta]\}$, a collection of scalars for which $\sum_{i=1}^{h_\theta} g_i.F_i = (1, 0, \cdots, 0)$, where F_i represents the i^{th} row of F.

• Data user determines $\Lambda_{\theta,0} = (c_{\theta,AA_\theta})M_\theta$ for each authority $AA_\theta(\theta \in [N])$. Subsequently, for each $x_i \in \chi'_\theta$, the data user executes $\Lambda_{\theta,i,1}$, $\Lambda_{\theta,i,2} \in R_q$ by the following way:

1) Data user performs the computation of $\Lambda_{\theta,i,1} = (c_{\theta,i,1}).y_{\theta,i}$ and $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$ for each $x_i \in W'_\theta$. The data user then executes $\Lambda_{\theta,i,1} = (c_{\theta,i,1}{}^+).y_{\theta,i}$ and $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$ for other $x_i \in S_{uid,\theta}$.
2) Now, for $x_i \in \chi'_\theta \setminus \{W'_\theta \cup S_{uid,\theta}\}$, the data user executes $\Lambda_{\theta,i,1} = (c_{\theta,i,1}{}^-).y_{\theta,i}$, $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$, $\Lambda_\theta = \Lambda_{\theta,0} + \sum_{i=1}^{h_\theta}[\Lambda_{\theta,i,1} + \Lambda_{\theta,i,2}] \in R_q$.

• Subsequently, $\phi' = (\phi'_0, \phi'_1, \cdots, \phi'_{f-1}) = c_0 - \sum_{\theta\in[N]} \mathcal{L}_\theta\ \Lambda_\theta$ is computed by the data user, where $\mathcal{L}_\theta$ represents the Lagrangian polynomial [29].

• Following this, corresponding to each $i \in \{0\} \cup [f-1]$, the output becomes $\phi_i = 0$ when $|\phi'_i| < \frac{q}{4}$; otherwise, $\phi_i = 1$.

As indicated by the aforementioned steps, the values corresponding to $\phi' = (\phi'_0, \phi'_1, \cdots, \phi'_{f-1})$ can be used to recover the original message ϕ. It is vital to recognize that the message is regarded as $\phi = (\phi_i)_{i\in\{0,\cdots,f-1\}} \in \{0,1\}^f$, such that $\phi(x) \in R_q$. As a result, the plaintext ϕ is determined by using the coefficients of ϕ'.

Fig. 1 finally illustrates how the suggested architecture operates overall.

Remark 1. *If Learning With Errors (LWE) is used instead of Ring-LWE (RLWE), the security of the proposed scheme remains unchanged since LWE is as difficult as worst-case lattice problems. However, the computational complexity increases significantly. RLWE offers several advantages that enhance performance compared to LWE, such as 1) Compact representation: RLWE expresses errors and secrets as polynomials rather than high-dimensional vectors, leading to smaller key sizes, which reduces storage and communication overhead, making it more practical for real-world applications; 2) Efficient cryptographic operations: Many cryptographic protocols depend on trapdoor sampling and key-switching operations, which are more efficient in RLWE due to its structured representation; 3) Computational efficiency: Unlike LWE, which requires computationally expensive matrix-vector multiplications, RLWE enables efficient polynomial arithmetic using the Fast Fourier Transform (FFT); and 4) Suitability for constrained environments: RLWE's efficiency makes it well-suited for resource-limited devices, such as IoT and embedded systems.*

VI. Implementation of the Proposed Scheme in IoT-Enabled Healthcare Applications

We describe an IoT-enabled smart healthcare application using the "blockchain technology for secure storage" by using

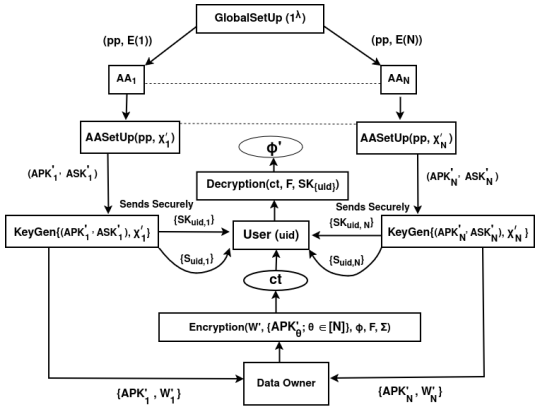


Fig. 1. Overall Working of the Proposed Scheme

our proposed scheme as discussed in Section V.

In IoT-based smart healthcare, patient data privacy is crucial. Such a system must operate in real time to ensure timely monitoring and responses, as delays can be life-threatening. It also needs to integrate various medical devices, which demands seamless interoperability.

Blockchain technology assists marketers in maintaining a comprehensive overview of the medical products in use. Consequently, the healthcare and pharmaceutical industries can leverage blockchain to eliminate counterfeit medications by enabling the tracking of all drugs, thereby identifying the source of falsification. Counterfeit medicines not only pose serious risks to public health but also lead to revenue losses for legitimate manufacturers [43]. Furthermore, blockchain technology enhances the security of patient records in hospitals. Once a medical history is created, blockchain can securely store it, ensuring that patient records remain unaltered [44].

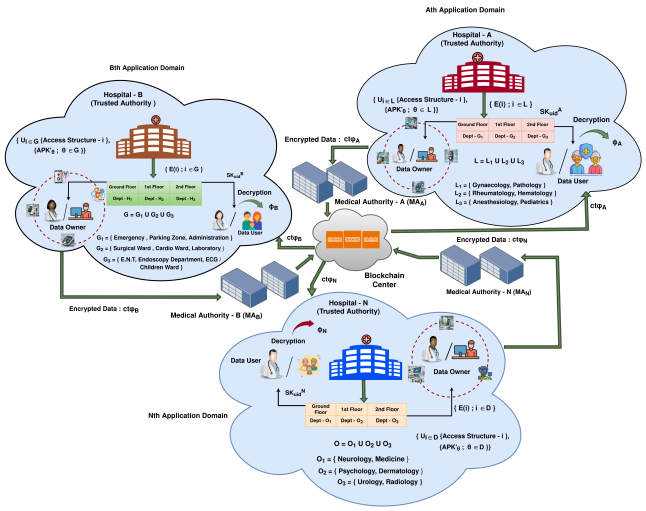


Fig. 2. Applying Lattice-based MA-CP-ABE in Healthcare application

The application of the proposed scheme (MA-CP-ABE) in blockchain-based IoT-enabled smart healthcare section shown in Fig. 2, which contains five phases, namely a) "registration phase", b) "user authentication phase", c) "data encryption phase", d) "block formation and addition phase", and e) "data decryption phase". The entities involved in the network are hospital authorities, medical authorities associated with the hospital authorities, data owners, data users, participating authorities connect to each hospital. The details of the various phases are as follows.

A. Registration Phase

Throughout the registration process, each hospital authority is classified as a registration authority (considered as a trusted entity). We contemplate an IoT-enabled healthcare application domain using the consumer electronics devices, say B^{th}-application, in which each individual authority associated with the existing departments in the affiliate hospital (B^{th} Hospital) has duly registered by the trusted B^{th} hospital authority. Also, the B^{th} hospital authority registered the associated data owner acting on the edge devices, medical authority along with the data user. To register each individual authority in the existing departments, the B^{th} hospital authority chooses a $(N-1)^{th}$ degree polynomial, called $E(y)$. Subsequently, utilizing this polynomial $E(y)$, the B^{th} hospital authority determine and allocate the value $E(\theta)$ to the individual authority identified as the θ in the existing departments of the B^{th} hospital, where $\theta \in [N_B]$. Now, B^{th} hospital authority selects the identity ID^B_{MA} for the respective medical authority MA_B associated with the B^{th} application domain and stored ID^B_{MA} into the MA_B's memory. After that, for each data owner, B^{th} hospital authority selects a unique bi-variate polynomial $L_i(x,y)$ of degree $f-1$ for the i^{th} data owner DO_i, and the unique identity $ID^B_{DO_i}$, then B^{th} hospital authority computes the uni-variate polynomials in y of degree $f-1$, i.e., $L_i(ID^B_{DO_i}, y)$ and $L_i(ID^B_{MA}, y)$ and stores $L_i(ID^B_{DO_i}, y)$ and $ID^B_{DO_i}$ publicly into the DO_i's memory and $L_i(ID^B_{MA}, y)$ publicly into the MA_B's memory before their deployment in the B^{th} application domain, and $L_i(x,y)$ kept secret for each i. Also, B^{th} hospital selects the identity $ID^B_{uid_i}$ for the i^{th} data user uid_i and transmits $ID^B_{uid_i}$ publicly to the uid_i. Upon completing the registration process, each individual authority in the existing departments associated with B^{th} hospital, identified as θ, executes the AASetup phase (described in Section V-B), and generates a unique pair of secret and public keys $(ASK'_{\theta,B}, APK'_{\theta,B})$, and this is hold for each individual authority connected with the existing departments associated with the B^{th}-Hospital.

B. User Authentication Phase

This phase is carried out by each individual authority in the existing departments associated with the B^{th} hospital. The individual authority, identified as θ, has a collection of attributes, represented by $\chi'_{\theta,B}$. Subsequently, each individual authority identified as θ, sends a set of attributes $S_{uid,\theta,B}$ to the i^{th} data user, uid_i, where $S_{uid_i,\theta,B} \subseteq \chi'_{\theta,B}$. Following this, the uid_i generates his/her own attribute sets their corresponding attribute set $S_{uid_i,B}$ by taking the union of each $S_{uid_i,\theta,B}$, where $\theta \in [N_B]$. Each individual authority AA_θ connected with the B^{th} hospital produces a unique set of secret keys, $y_{uid_i,\theta,B}$, based on his/her attribute set $\chi'_{\theta,B}$, after generating the KeyGen phase (described in Section V-C). Each individual

authority, identified as θ, transmits their secret keys $y_{uid_i,\theta,B}$ to the corresponding uid_i. Upon receiving each $y_{uid_i,\theta,B}$, for $\theta \in [N_B]$, the i^{th} data user, uid_i, creates their own secret key, i.e. $SK_{uid_i,B} = \cup_{\theta\in[N_B]}\{SK_{uid_i,\theta,B}\} = \cup_{\theta\in[N_B]}\{y_{uid_i,\theta,B}\}$. The data user is regarded as either a healthcare professional like doctors or nurses associated with the B^{th}-Hospital or the authority of the B^{th}-Hospital.

C. Data Encryption Phase

This phase is performed by the i^{th} data owner (DO_i) associated with the B^{th} hospital. First of all, the DO_i needs to securely collect the medical sensitive data from the respective IoT-enabled healthcare application domain using the deployed consumer electronics devices. Later, the DO_i takes the collected medical data, ϕ_B, and then creates the plaintext message $Data_{\phi_B,DO_i} = (\phi_B, TS_{\phi_B}, ID^B_{DO_i})$, where TS_{ϕ_B} represents the timestamp when the message is selected, $ID^B_{DO_i}$ implies the identity of the associated i^{th} data owner DO_i, then received the collection of public keys represented as $\{APK'_{\theta,B}; \theta \in [N_B]\}$ of every individual authority identified as θ in the existing departments associated with the B^{th} hospital. At this phase, the individual authority, identified as θ connected with the B^{th} hospital, establishes an access structure referred to as $W'_{\theta,B}$, which is composed of attributes derived from $X'_{\theta,B}$, and subsequently $W'_{\theta,B}$ is then transmitted to the i^{th} data owner DO_i. The data owner DO_i constructs an access structure, W'_B, formed by the union of each $W'_{\theta,B}$ associated with the B^{th} hospital, where $\theta \in [N_B]$. Following this, data owner implements the proposed lattice-based multi-authority CP-ABE method described in Section V-D to encrypt the sensing medical data $Data_{\phi_B,DO_i}$ of the patients, and produces the ciphertext as ct_{ϕ_B,DO_i}. Also MA_B forwarded ID^B_{MA} to the DO_i. Subsequently, the i^{th} data owner DO_i produces a current timestamp, represented as CTS_{DO_i}, then computes $L(ID^B_{DO_i}, ID^B_{MA})$ and generates a transaction, referred to as $TX_{\phi_B,DO_i} = \{(ct_{\phi_B,DO_i}, F), CTS_{DO_i}, H(CTS_{DO_i}, ct_{\phi_B,DO_i}, (L(ID^B_{DO_i}, ID^B_{MA}))), ID^B_{DO_i}\}$. This TX_{ϕ_B,DO_i} is subsequently transmitted to the medical authority MA_B associated with the B^{th} application domain.

Block Header	
Block Version	$BVer$
Previous Block Hash	PBH
Merkle Tree Root	MTR
Timestamp	TS_{BLOCK}
Owner of Block	MA_B
Block Payload	
List of n_t Encrypted Transactions	$\{TX_{\phi_B,DO}\|i = 1, 2, \cdots, n_t\}$
Current Block Hash	$CBHash$

Fig. 3. Structure of a block

D. Block Formation and Addition Phase

Once the medical authority MA_B, related with the B^{th} application domain, receives the transaction TX_{ϕ_B,DO_i}, MA_B is extracting the timestamp CTS_{DO_i}, the identity ID_{DO_i} of the i^{th} data owner DO_i, and the encrypted ciphertext ct_{ϕ_B,DO_i} from this transaction TX_{ϕ_B,DO_i}. Following that, this transaction TX_{ϕ_B,DO_i} is validated by MA_B through the computations of $(L(ID^B_{MA}, ID^B_{DO_i})$ and $H(CTS_{DO_i}, ct_{\phi_B,DO_i}, (L(ID^B_{MA}, ID^B_{DO_i})))$ and checks whether this computed hash value is equal or not with the received hash value in the TX_{ϕ_B,DO_i}. The transaction TX_{ϕ_B,DO_i} is declined by the medical authority MA_B if the above hash values are not equal. On the contrary, if the condition be satisfied, MA_B then approved the transaction TX_{ϕ_B,DO_i}. In this scenario, all the medical authorities linked with the different hospitals established a P2P-CS network. Let, MA_B designates the in-charge of this P2P-CS network. Once, MA_B obtains a collection of n_t valid transactions $\{TX_{\phi_B,DO_1}, TX_{\phi_B,DO_2}, \cdots, TX_{\phi_B,DO_{n_t}}\}$ from the respective data owners associated with the B^{th} hospital. The following procedures are subsequently executed:

Fig. 3 illustrates that MA_B constructs a block, say $BLOCK$. The block comprises of several components: a set of n_t transactions denoted by $\{TX_{\phi_B,DO_1}, TX_{\phi_B,DO_2}, \cdots, TX_{\phi_B,DO_{n_t}}\}$, a unique block version, $BVer$, the previous block hash, PBH, the merkle tree root, MTR, the timestamp of block creation, TS_{BLOCK}, the current block hash, CBH, owner of the block i.e., medical authority MA_B. The secure hash algorithm, i.e., SHA-256 is employed in our system, mapping any arbitrary string to a 256-bit hash output. The Merkle tree root is determined by evaluating over the n_t transactions $\{TX_{\phi_B,DO_1}, TX_{\phi_B,DO_2}, \cdots, TX_{\phi_B,DO_{n_t}}\}$ that are included in the $BLOCK$. The current block hash is generated through the process of hashing every element in the $BLOCK$. This is represented as $CBHash$ = $Hash$(Block Header||Block Payload), where $Hash(,)$ symbolises the SHA-256 hash function. Subsequently, in order to select a leader, the medical authority associated with the B^{th}-Hospital initiates a leader selection algorithm among the existing n_{cs} number of medical authorities associated with the Hospitals in this P2P-CS network. After being elected the leader among these n_{cs} medical authorities, such medical authority, called L, develops a "voting based consensus algorithm for verifying and mining of the block, $BLOCK$ in the blockchain centre". In order to accomplish this objective, the "Practical Byzantine Fault Tolerance $(PBFT)$ algorithm" [45] is executed.

E. Data Decryption Phase

This stage is carried out by the data user. During this phase, the i^{th} data user uid_i associated with the B^{th} hospital, downloads the $BLOCK$ from the blockchain center, and then retrieves the transactions TX_{ϕ_B,DO_i}, from which retrieves the encrypted sensing information ct_{ϕ_B,DO_i}, which was generated by data owner DO_i associated with the B^{th} hospital. Subsequently, the data user, uid_i, employs their personal secret keys $SK_{uid_i,B}$ to decrypt the accumulated encrypted medical data ct_{ϕ_B,DO_i} of the patient's (described in Section V-E), thereby acquiring the patient's initial sensory medical information ϕ_B if the decryption will be successful.

VII. Security Analysis

In this section, we first provide a proof of the correctness of our proposed lattice-based MA-CP-ABE scheme. Next,

we provide the formal security analysis of the proposed scheme followed by the heuristic (informal) security analysis to show the robustness of our proposed scheme against various traditional attacks including quantum attacks.

A. Formal Security Analysis

Theorem 1 emphasizes that the suggested scheme exhibits selective security against the Chosen Plaintext Attack (sCPA), taking into account the decisional Ring-LWE problem's difficulty.

Theorem 1. *The security of the proposed lattice-based MA-CP-ABE scheme is IND-sCPA secure, relying on the hardness presented by the decisional Ring-LWE assumption. More specifically, if a "probabilistic polynomial time adversary (PPT) adversary", represented as $\mathcal{A}$ is capable of wining the IND-sCPA game having the success probability $\epsilon > 0$, where ϵ is a non-negligible number, then there exist an adversary $\mathcal{B}$ who is able to solve the Ring-LWE problem such an advantage ϵ.*

Proof: The proof of this theorem is provided in the supplementary material.

B. Informal Security Analysis

In this section, through the propositions 1–6, we show that our proposed lattice-based multi-authority CP-ABE scheme is able to resist the following important attacks, including quantum attacks. The detailed proofs of these propositions are provided in the supplementary material.

Proposition 1. *The proposed scheme resists replay attacks.*

Proposition 2. *The proposed scheme resists the man-in-the middle attack.*

Proposition 3. *The proposed scheme is secure against impersonation attacks.*

Proposition 4. *The proposed scheme resists quantum attacks through the Grover's algorithm.*

Proposition 5. *The proposed scheme resists quantum hidden subgroup problem.*

Proposition 6. *The proposed scheme is robust against quantum lattice reduction algorithms.*

VIII. Results and Discussions

A. Testbed Experiment

In this section, we design a testbed experiment to evaluate the computational time needed for the KeyGen, Encryption and Decryption phase related to the proposed scheme.

We used the "Python 3.10 on Ubuntu 22.04 LTS platform on a hardware with an Intel Core i7-9750H CPU @ 2.60GHz processor, with 6 cores and 12 threads, 16 GB of RAM and a 256 GB of SSD". For polynomial operations, we used the *numpy.polynomial* library in Python.

The experimental results for the KeyGen phase of the proposed scheme with respect to a varying number of attributes are shown in Fig. 4(a). It is worth noticing that the computational time in seconds required for this phase linearly increases when the number of attributes are increased. Even if, the number of attributes is reasonably more, the computational time is not very high. This means that the proposed scheme is practically applicable for the real-world scenario. Similarly, the experimental results for the encryption and decryption phases of the proposed scheme with respect to a varying number of attributes are also shown in Figures 4(b) and 4(c). From these figures, it is worth noticing that the similar trend happens as it was the case for the KeyGen phase. However, the time needed for the decryption phase is reasonably low as compared to that for the encryption phase of the proposed scheme, even when the number of attributes is more.

B. Blockchain Simulation

The Hyperledger Sawtooth framework has been utilized for our blockchain simulation, because it has the modular architecture and it support parallel transaction execution, and it provides a range of consensus techniques. It was developed and maintained by the Linux foundation. Each node in the Sawtooth network comprises "*Validator*, *REST API*, *Consensus Engine*, and *Transaction Processors*".

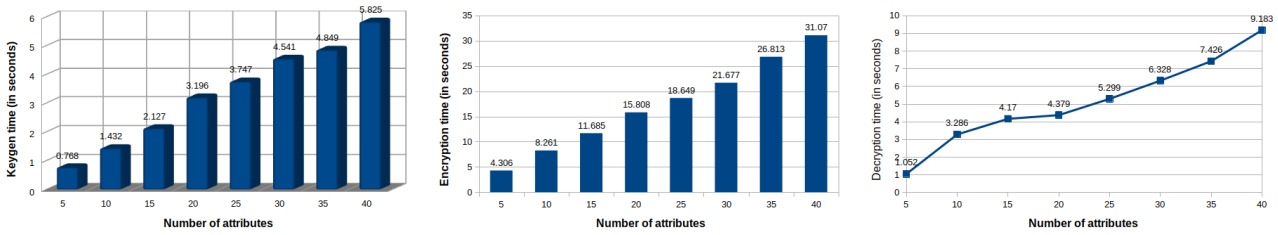
The REST API facilitates communication with the user, transaction submission, and determining the system's state. The validator's role is to verify transactions and add them as new blocks to the chain, following instructions from the Consensus engine on when to add a new block. Upon receiving a transaction, the validator forwards it to a registered transaction processor suitable for that transaction type. This module is developed by the programmer according to the application's requirements. The Sawtooth framework is highly modular, allowing the consensus algorithm to be changed in real-time without restarting the system.

We now present our simulation results obtained by using the transaction processor that we programmed for our scheme. We used a machine running "Ubuntu 22.04 LTS with an Intel Core i7-9750H CPU @ 2.60GHz processor, featuring 6 cores and 12 threads, 16 GB of RAM as primary memory, and a 256 GB solid-state drive as secondary memory", for our simulation. The consensus algorithm used for the blockchain was the "Practical Byzantine Fault Tolerance (PBFT)" algorithm.

In our blockchain simulation, we considered two cases:

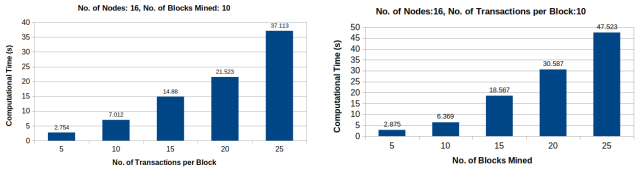
Case-1: Similar to Case-1, we also considered the total number of nodes in the blockchain network as 16, whereas the number of blocks mined in the network is fixed at 10. Fig. 5(a) shows the results for the blockchain simulation for this case. When we increased the number of transactions inserted into the block, the computational time needed for the consensus process described in Section VI-D also increased linearly, which is a similar trend as in Case-1.

Case-2: In this case, we considered the total number of nodes in the blockchain network as 16, whereas the number of transactions per block is fixed at 10. Fig. 5(b) shows the results for the blockchain simulation. When we increased the number of blocks mined in the blockchain network, we observed that the computational time needed for the consensus process described in Section VI-D increased linearly.



(a) (b) (c)

Fig. 4. Experimental results with a varying number of attributes for (a) KeyGen phase (b) encryption phase (c) decryption phase



(a) (b)

Fig. 5. Blockchain performance for (a) Case-1 (b) Case-2

TABLE III
COMPARATIVE ANALYSIS BASED ON LATTICE STRUCTURE

Scheme	Public Key	Private Key	Ciphertext	Plaintext
[31]	$(2mh + 1 + m)f\lceil \log q \rceil$	$h.mf\lceil \log q \rceil$	$(2h - \|W'\| + 1)mf\lceil \log q \rceil$	f
[33]	$2m_1m_2\|\mathscr{U}\|.\lceil \log q \rceil$	$m_2.U.\lceil \log_2(\|\sigma\|) \rceil + m_2.U.\lceil \log_2(\|\sigma\| + \|\delta\|) \rceil$	$yt_{max}\lceil \log_2 3 \rceil + 3m_2\bar{y}\lceil \log_2 q \rceil$	1
[28]	$mf\lceil \log q \rceil \|S\| + \eta f\lceil \log q \rceil$	$2n_kmf\lceil \log q \rceil$	$2\|J\|mf\lceil \log q \rceil$	ηf
[29]	$(2mh + mN + 1)f\lceil \log q \rceil$	$n_kmf\lceil \log q \rceil$	$(2h - \|W'\| + N)mf\lceil \log q \rceil$	f
[32]	$(2mh + mN + 1)f\lceil \log q \rceil$	$2(2n_u + 2n_v - n_r)mf\lceil \log q \rceil$	$\{2(n_a+n_v-n_k+1)m+ m+1\}f\lceil \log q \rceil$	f
Proposed	$(2mh + mN + 1)f\lceil \log q \rceil$	n_kmfd	$(2h - \|W'\| + N)(m + 1)f\lceil \log q \rceil$	f

IX. PERFORMANCE ANALYSIS

In this section, we now provide a detailed comparative study based on some related components between the proposed method and the existing CP-ABE/MA-CP-ABE methods, like Fu *et al.* [31], Yao *et al.* [33], Zhao *et al.* [28], Sun *et al.* [29], and Yang *et al.* [32]. The symbols specified in Table II are also employed for this comparative study. According to Table III, we see that our scheme has a smaller secret key size with respect to the other compared schemes. Additionally, the proposed scheme's plaintext size is smaller with respect to Zhao *et al.*'s scheme [28].

TABLE IV
PERFORMANCE COMPARISON

Scheme	Authority	Architecture	Security	Implementation in real-life IoT applications	Blockchain Implementation	Efficiency
[31]	Single	Centralized	Quantum Secure	N/A	No	Low
[29]	Multi	Decentralized	Quantum Secure	N/A	No	Low
[28]	Multi	Decentralized	Quantum Secure	N/A	No	High
[32]	Multi	Decentralized	Quantum Secure	N/A	No	Low
[33]	Multi	Decentralized	Quantum Secure	N/A	No	Moderate
Proposed	Multi	Decentralized	Quantum Secure	Yes	Yes	High

The efficacy level of the scheme designed by Fu *et al.* [31] is low due to the application of a central (single) authority, as indicated through the performance analysis comparison in Table IV. Table IV demonstrates that all of the schemes aside from the suggested scheme have no blockchain implementations and no useful real-world applications. Consequently, all the proposed schemes [31], [29], [28], [32], [33] including the proposed scheme provides quantum resistant privacy protection. Despite the fact that the multi-authority CP-ABE is employed by the proposed scheme and the remaining schemes suggested by Fu *et al.* [31], Sun *et al.* [29], Yang *et al.* [32],and Yao *et.al* [33], the proposed scheme achieves blockchain implementations, practical IoT applications, a robust privacy and security safeguards.

X. CONCLUSION

We developed a blockchain based efficient MA-CP-ABE method depends on the lattice structure. In order to protect against quantum attacks and enable less computationally demanding communications in smart healthcare, this scheme is especially designed for IoT-based smart healthcare applications. where the severity of the Ring-LWE assumption is a determining factor in the development of this method. The several authorities are regarded as decentralized distributed servers in this work, which suggests that the proposed scheme is compatible with a distributed computing environment. As the proposed scheme has been integrated into a smart healthcare application that is based on IoT, the lattice structure guarantees that the computational complexity is minimized. The implementation of blockchain technology in the IoT-based healthcare system ensures the security and tamper-proof storage of sensitive healthcare data, safeguarding it from illicit access and cyber threats. This scheme is designed to ensure robust security by limiting access to the services to authorized parties with legitimate access policies, which are managed by multiple authorities. The performance analysis, testbed experiments, blockchain simulation and security analysis indicate that the proposed scheme is more effective and robust than other existing lattice-based schemes that are currently in use. In future, we would like to add traceability and revocation features, as well as key escrow feature with the blockchain in the proposed scheme.

REFERENCES

[1] G. K. Garge, C. Balakrishna, and S. K. Datta, "Consumer Health Care: Current Trends in Consumer Health Monitoring," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 38–46, 2018.

[2] S. Datta and S. Namasudra, "Blockchain-Based Smart Contract Model for Securing Healthcare Transactions by Using Consumer Electronics and Mobile-Edge Computing," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4026–4036, 2024.

[3] P. R. Babu, S. A. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Computer Science Review*, vol. 54, p. 100676, 2024.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2005*, Aarhus, Denmark, 2005, pp. 457–473.

[5] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2011*, Tallinn, Estonia, 2011, pp. 568–588.

[6] J. Kim, W. Susilo, F. Guo, M. H. Au, and S. Nepal, "An efficient KP-ABE with short ciphertexts in prime ordergroups under standard assumption," in *ACM Asia Conference on Computer and Communications Security*, Abu Dhabi, United Arab Emirates, 2017, pp. 823–834.

[7] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, 2014.

[8] H.-T. Wu and C.-W. Tsai, "Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, 2018.

[9] K. Sowjanya and M. Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC," *Journal of Information Security and Applications*, vol. 54, p. 102559, 2020.

[10] Y. Wang, B. Chen, L. Li, Q. Ma, H. Li, and D. He, "Efficient and secure ciphertext-policy attribute-based encryption without pairing for cloud-assisted smart grid," *IEEE Access*, vol. 8, pp. 40 704–40 713, 2020.

[11] A. G. Fowler and L. C. L. Hollenberg, "Scalability of Shor's algorithm with a limited set of rotation gates," *Phys. Rev. A*, vol. 70, Sep 2004.

[12] P. Bagchi, B. Bera, R. Maheshwari, A. K. Das, D. K. Y. Yau, and B. Sikdar, "An Efficient and Secure Post-Quantum Multi-Authority Ciphertext-Policy Attribute-Based Encryption Method Using Lattice," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Hoboken, NJ, USA, 2023, pp. 1–6.

[13] P. Bagchi, R. Maheshwari, B. Bera, A. K. Das, Y. Park, P. Lorenz, and D. K. Y. Yau, "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," *IEEE Transactions on Vehicular Technology*, pp. 1–16, 2023.

[14] M. Ajtai, "Generating Hard Instances of Lattice Problems (Extended Abstract)," in *Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, Pennsylvania, USA, 1996, pp. 99–108.

[15] M. Yasuda, "A survey of solving SVP algorithms and recent strategies for solving the SVP challenge," in *International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019*, Singapore, 2021, pp. 189–207.

[16] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Advances in Cryptology — CRYPTO '97*, Santa Barbara, California, USA, 1997, pp. 112–131.

[17] D. Micciancio, "Improving Lattice Based Cryptosystems Using the Hermite Normal Form," in *Cryptography and Lattices*. Providence, RI, USA: Springer Berlin Heidelberg, 2001, pp. 126–145.

[18] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, Victoria British Columbia, Canada, 2008, pp. 197–206.

[19] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, pp. 84–93, 2005.

[20] D. Dharminder, U. Kumar, A. K. Das, B. Bera, D. Giri, S. S. Jamal, and J. J. P. C. Rodrigues, "Secure cloud-based data storage scheme using postquantum integer lattices-based signcryption for IoT applications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 9, p. e4540, 2022.

[21] F. Zhang, R. Safavi-Naini, and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," in *Public Key Cryptography – PKC 2004*, Singapore, 2004, pp. 277–290.

[22] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with Partially Hidden Access Structures," in *7th ACM Symposium on Information, Computer and Communications Security*, New York, NY, USA, 2012, pp. 18–19.

[23] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 24–32, 2018.

[24] D. S. Gupta, S. H. Islam, M. S. Obaidat, A. Karati, and B. Sadoun, "LAAC: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3620–3627, 2021.

[25] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System," *IEEE Access*, vol. 11, pp. 114 322–114 340, 2023.

[26] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute Based Encryption," in *Automata, Languages and Programming*, Reykjavik, Iceland, 2008, pp. 579–591.

[27] W. Dai, Y. Doröz, Y. Polyakov, K. Rohloff, H. Sajjadpour, E. Savaş, and B. Sunar, "Implementation and evaluation of a lattice-based key-policy ABE scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1169–1184, 2017.

[28] S. Zhao, R. Jiang, and B. Bhargava, "RL-ABE: A Revocable Lattice Attribute Based Encryption Scheme Based on R-LWE Problem in Cloud Storage," *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 1026–1035, 2022.

[29] J. Sun, Y. Qiao, Z. Liu, Y. Chen, and Y. Yang, "Practical Multi-Authority Ciphertext Policy Attribute-Based Encryption from R-LWE," in *IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*, New York City, NY, USA, 2021, pp. 1435–1443.

[30] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography," *IEEE Transactions on Computers*, no. 3, pp. 322–334, 2018.

[31] X. Fu, Y. Wang, L. You, J. Ning, Z. Hu, and F. Li, "Offline/Online lattice-based ciphertext policy attribute-based encryption," *Journal of Systems Architecture*, vol. 130, p. 102684, 2022.

[32] Y. Yang, J. Sun, Z. Liu, and Y. Qiao, "Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing," *Journal of Information Security and Applications*, vol. 65, pp. 103–108, 2022.

[33] Y.-F. Yao, H.-Y. Chen, Y. Gao, K. Wang, and H.-Y. Yu, "A decentralized multi-authority CP-ABE scheme from LWE," *Journal of Information Security and Applications*, vol. 82, p. 103752, 2024.

[34] P. Datta, I. Komargodski, and B. Waters, "Decentralized Multi-authority ABE for DNFs from LWE," in *Advances in Cryptology - EUROCRYPT 2021*, Zagreb, Croatia, 2021, pp. 177–209.

[35] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in *Annual Cryptology Conference (CRYPTO)*, Santa Barbara, CA, USA, 2011, pp. 505–524.

[36] Q. Yuan, H. Yuan, J. Zhao, M. Zhou, Y. Shao, Y. Wang, and S. Zhao, "Distributed Identity Authentication with Lenstra-Lenstra-Lovasz AlgorithmâCiphertext Policy Attribute-Based Encryption from Lattices: An Efficient Approach Based on Ring Learning with Errors Problem," *Entropy*, vol. 26, no. 9, 2024.

[37] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[38] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[39] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023.

[40] R. M. Daniel, A. Thomas, E. B. Rajsingh, and S. Silas, "A strengthened eCK secure identity based authenticated key agreement protocol based on the standard CDH assumption," *Information and Computation*, vol. 294, p. 105067, 2023.

[41] R. El Bansarkhani and J. Buchmann, "Improvement and Efficient Implementation of a Lattice-Based Signature Scheme," in *Selected Areas in Cryptography – SAC 2013*, Burnaby, BC, Canada, 2014, pp. 48–67.

[42] P. Bert, G. Eberhart, L. Prabel, A. Roux-Langlois, and M. Sabt, "Implementation of Lattice Trapdoors on Modules and Applications," in *Post-Quantum Cryptography*, 2021, pp. 195–214.

[43] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1634–1646, 2017.

[44] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.

[45] 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.