Ring Learning With Error-Based Encryption Scheme for the Privacy of Electronic Health Records Management

Umar Abdulkadir[1,*], Victor Onomza Waziri[2], John Kolo Alhassan[3], and Idris Ismaila[4]
[1,2,3,4]Federal University of Technology, Minna, Nigeria
*Contact: umargud@gmail.com

2022 5th Information Technology for Education and Development (ITED) | 978-1-6654-9370-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITED56637.2022.10051260

Abstract— **The electronic health (e-health) systems support a range of electronic devices, wireless links, transmission and storage of data. E-health systems allows communication through a gateway (or central point) in the cloud. Health professionals and teams utilize e-health systems to perform virtual consultations to patients, remote treatment or diagnosis. The success story of e-health systems is often met with problems including: insecure channels of communication, eavesdropping of messages across channels by adversary, profound insider attacks on private information on servers, and healthcare services disruptions. Cryptography or encryption algorithms have been considered as capable of overcoming the privacy and security problems of electronic medical records management. However, certain issues persist with cryptographic-based schemes such as slow processing speed, weak security mechanisms, high computational overheads, and weak public-private keys. In this paper, a lattice-based cryptography, Ring Learning With Error (RLWE) encryption is used to propose a privacy scheme for EMR in cloud environment. The choice of RLWE is due to its provable hardness among conventional lattice problem. The outcomes revealed that, the proposed encryption scheme outperformed comparable asymmetric schemes in terms of elapsed time (0.04sec) against ECDSA (1.11sec), ECC (16.62sec), and RSA (37.95sec). Again, the public key size was better for RLWE (32-bits) only after ECDSA (10-bits), against ECC (97-bits), and RSA (191-bits). Similarly, the private key size for ECC (9-bits) was only better than RLWE (10-bits), against ECDSA (58-bits), and RSA (687-bits) respectively. The proposed encryption scheme is time and memory-efficient; and holds promise for EMRs privacy.**

I. INTRODUCTION

Cloud based platforms offer several benefits to organizations especially in areas of security and privacy [1]. The cloud has provided a veritable platform for synchronizing healthcare data collected from diverse service providers [2]. Recently, electronic health records have proven to effectively compliment healthcare delivery and services through seamless patient records sharing among various service points [3]. Though, information disclosure, that is, sensitive user data by illicit and unauthorized users remains a top challenge for the cloud-based applications such as electronic health records storages. Consequently, encryption approaches have been suggested to safeguard the sensitive information and to give data access rights only to approved users. Th[1]ese can be achieved through outsourcing of encryption and decryption computations to proxy server to attain privacy and flexible access control of big data in cloud [4] [5].

A typical electronic health system manages diverse data concerning patients (such as physiology) sent to one pointed hospital, which stores the data, and make them available to the user or third party (or doctors) for health purposes and analysis [6]. Often, there is monopoly of medical data, data are vulnerable to accidental losses due to single point storage. There is commercial exploitation of the private health data of patients by health records administrators leading to privacy issues [7]. Considering the adoption of electronic health records in the healthcare industry the most imperative barrier to entry is the high security of the information, which leads to the need of a medical software that can protect personal medical data and the privacy of the patients [8].

Modern biobanks permit large-scale analysis for individuation of specific diseases biomarkers starting from biological or digital material (that is, bioimages) with well-annotated clinical and biological data. These features are essential for improving personalized medical approaches, where effective biomarker identification is a critical step for disease diagnosis and prognosis [9].

Majority of data encryption approaches are used to protect the confidentiality rather integrity of health data [10]. Another potent solution was proposed by [11] in which a trusted third-party service as a permission service provider enable patients to set permissions for all related data in a particular location in the cloud such as Public Blockchain/Distributed Ledger Technologies [12]. In effect, there is an integration ease while patients decide data sharing arrangements [13]. In particular, electronic health records started to be implemented on Blockchains as at year 2017. Blockchain Technology replies on the strengths of public key cryptography, which are vulnerable to collision attacks, and privacy of user information is not guaranteed [14].

978-1-6654-9370-3/22/$31.00 ©2022 IEEE

2022 5th Information Technology for Education and Development (ITED)

However, majority of encryption approaches are ineffective and susceptible to attacks due to weak ciphers/keys, large storage requirements, and extended encryption/decryption processes [15]. This research work attempts to develop ring learning with error-based encryption scheme for the privacy of health records administration in cloud environment.

II. Related Studies

The EHRs are further driving the volume of data as patients' files, x-rays, lab results, and other sensitive medical records are transmitted across the network. Presently, nearly one-third of healthcare providers utilize mobile devices to access EHRs in cloud environments. The healthcare industry is bracing for a new reality in which healthcare applications are steadily impacting the mobility and security of how caregivers and hospitals are authorized to access vital information. To this end, privacy-preserving EHR system using ciphertext-multi authority attribute-based encryption (CPMA-ABE) was advanced by [16]. In this system, patients can encrypt their EHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive EHR contexts. Meanwhile patients maintain full control over access to their EHR files, by assigning fine-grained, attribute-based access privileges to selected data users, while different users can have access to different parts of their EHR.

Blockchain technology can be leveraged in the healthcare domain to achieve the delicate balance between privacy and accessibility of electronic health records. Therefore, [17] proposed a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. The smart contracts in an Ethereum-based blockchain were used to heightened access control and obfuscation of data, and employs advanced cryptographic techniques for further security [17].

The prospects of realizing the authentication scheme of EHRs system based on blockchain was identified by [18]. There is need to formally specify the EHRs system model in the setting of consortium blockchain. Also, new design considerations based on an identity-based signature scheme with multiple authorities for the blockchain-based EHRs system are evolving. New EHRs scheme can utilize more efficient signing and verification algorithms.

The new paradigm of EHRs raises fresh perspective about data privacy and network security for e-health systems, and ways of reliably sharing EHRs within mobile users while guaranteeing high-security levels in the mobile cloud is a challenging issue [19]. In addition, blockchain enabled solution is a step towards efficient management of e-health records on mobile clouds, which is promising in many healthcare applications [20].

It was noted in [21] that, there exists well-defined secured record management of patient's PHR; thereby revealing highly confidential personal information such as what happened, when, and who has access to such information. It further noted that, new framework must offer protection for sensitive patient's PHR data items in order guarantee time efficiency, and privacy, accessibility, and granular access control management.

Lattice-based cryptography became hot research in the last decade following the introduction of the Learning-With-Errors (LWE) problem in 2009 [22] and its more efficient ring variant, the ring-LWE problem in 2010 (Lyubashevsky et al. [23]). Prior 2012 almost all of the literature considered the theoretical aspects of LWE and ring-LWE-based cryptography. The implementation feasibilities and performance aspects of these schemes are relatively scanty. This serves as the motivation for this paper, which is to investigate implementation aspects of ring-LWE-based public-key cryptography for privacy of EMRs [23].

III. The Proposed Scheme

A. Problem Definition

1) *Definition 1*: Learning with error problem (LWE) can be represented as by Gaussian distribution D_z in Eqn. 1:

$$c(x) \cong \exp(-\pi \frac{(x-c)}{S^2}) \quad (1)$$

where, *S* and *C* are standard deviation and the Gaussian mean. Integral Gaussian Distribution: m = number of samples, the goals can be to find *S*, and right-hand side is not uniform (and independent of left-hand side). The choice of the discreet continuous Gaussian used ($\boldsymbol{\chi}$) (replace) $\mathbb{Z}_q$ in RHS by R(q$\mathbb{Z}$) is to simply explain with integer. The Continuous Gaussian works (replace) $\mathbb{Z}_q$ in RHS R|qR. The continuous Ring rather than U(-5aq, +5aq) provides hardness proof for LWE that heavily relies on Gaussian. If a = 0, LWE is easy (no error noise): Linear system mod q. If a≈ 1, LWE becomes trivially impossible as sample contains almost no information $\vec{s}$ (noise s- covers encrypting) as represented by Eqn. 2:

$$D_{Z,S,C}(X) = \frac{\exp(-\pi(x-c)^2|s^2)}{\sum_{c\in Z} exp[-\pi(x-c)^2]s^2} \quad (2)$$

Not all (once) properties of the continuous case hold for the integral 1s, but may do when S ≥ 1.

2) Definition 2: *Learning with Error*

Let $n \geq 1, q \geq 2, a \in \{0,1\}$and $\vec{s} \in (Z_q)^n$ we define the distribution $D_{n\in 0,1,a}(S)$ over $(Z_q)^n X Z_q$ by sample $a \leftarrow U(Z_q^n)$ sample e← $D_{Z,a,q,0}(error\ term)$ return $(\vec{a}, (\vec{a}, \vec{s}) + \overrightarrow{e})$ the linear product of $\vec{a}$ with $\vec{s}$ + sample error noise $e \in Z$ reduced mod q.

Search LWE: Let $\vec{s} \in Z_q^n$ arbitrary. Given arbitrary many sample from requirement and b ∈ {0,1}, if with non-negliable probability over $\vec{s}$ (proportionally ≥ $\frac{1}{n^2}$ for some constant c > 0), which can be depicted by Eqn. 3.

$$Adv(A) = \Pr|A \xrightarrow{D(S)} 1| - \Pr|A \xrightarrow{U} 1| \geq \frac{1}{n^2} \text{ for some c} > 0. \quad (3)$$

Assume that, $A \leftarrow Z_q^n,\ s \leftarrow Z_q^n,\ e \leftarrow \chi^n,\ r_1, r_2 \leftarrow Z_q^n$. Then, LWE can be defined by Eqn. 4:

$$(a, < a, s > + e) \approx r_1, r_2 \quad (4)$$

Being-LWE, a polynomial ring applied in stage represented by Eqn. 4 provides the outcomes presented in Eqn. 5:

$$Z_q^n \rightarrow Z_q[\chi]\Phi_m(x): n = \Phi(m) \quad (5)$$

$\forall\, m \in Z^+$ defines $\Phi_m(x)$, *P*: prime number in integer *r*, $Z_{P^r}[x]$ polynomial ring *r*, then, standard deviation of the discrete Gaussian distribution of the cipher text space parameter is represented by Eqn. 6:

$$q = q\,(m, p, r, r, k) \quad \leftarrow \quad \text{security parameters} \quad (6)$$

Message space: polynomial quotient ring as represent in Eqn. 6:

$$R_q \coloneqq Z_q[x]/\Phi_m(x): q \geq p \quad (7)$$

Key Generation: The operations are presented in Eqn. 8:

$$s \leftarrow X^n; a \leftarrow R_{q;}\, e \leftarrow X^n \text{ that is, } n = \Phi_m$$
$$q = -(a, s + e.p) \quad (8)$$

Secrete key $s_k := s$, Public key, $P_k \coloneqq (a_0, a_1)$

According to Li et al. [25], homomorphic encryption can be impractical to break. Therefore, basic encryption scheme operations include: Encrypted Message denoted by Eqn. 9:

$$M \in R_p;\ P_k = (a_0, a_1), U, f, g \leftarrow X^n$$
$$c + x \coloneqq (c_0 \colon a_0 u + gp + M) \quad (9)$$

Thereafter, the addition, and multiplication over polynomial rings can be represented as: $(c_0 \colon a_0 u + fp)$

While, the basic decryption can be represented as Eqn. 10:

$$C + x \coloneqq (c_0, c_1, \ldots \ldots c_k)\ Sk = s$$
$$M \coloneqq \sum_{c=0} c_i s\ mod(P, \Phi_m(x)) \quad (10)$$

B. RLWE Signature Generation Algorithm

The signature generation (*SignGen*) is concerned with forging of all the relevant keys Q, which is used to sign the medical records S by Algorithm 1.

Algorithm 1 *SignGen(Q, S, q, M, p, b, N)*	
Input:	The private key *Q*; medical records *S*; EMR content *S*; *SignGen*; Random function b; length of private key N.
Output	The complete result of signature; x.
	Choose a random key length q within the uniform vectors' keys *M*; calculate the ring polynomial *x.* which is given by $q \in M_{Q-1}$, $x = SignGen(G^s(mod\ N))$ **for** each $j \in [1, 9]$ do $p_j \leftarrow R(S, Q, p, r)$ **end for** **for** each $j, p_j \in$ [1,9] **do** $x_j \leftarrow (p_j, -b.q_2).(G^{s-1}(mod\ (N-1)))$ **return** $x \leftarrow q(p_1, p_2, p_3, \ldots, p_j)$ **terminate** *SignGen* operation.

After the completion of the signature generation in Algorithm 3.1, $(x \in Q)$ is used to encrypt the content of EMR S and generates the public or private keys respectively.

C. Experimental Settings

The initial experimental settings composed of hardware and software requirements for validating of the proposed RLWE scheme are contained in Table 1

TABLE I
THE MINIMAL EXPERIMENTAL PARAMETERS

Parameters	**Value**
Processor	AMD E1-1200 APU, Radeon™ HD Graphics 1.40 GHz
RAM	4.00 GB
Hard Disk Drive	282 GB
System Type	64-bit OS, x64-based processor
Operating System	Windows 8 Single Language
Application programming	Visual Studio Code
Cryptographic schemes	RLWE, ECDSA, ECC and RSA
Key generation mode	Asymmetric algorithm key exchange-based Diffie and Hellman

D. Performance Evaluation Parameters

This paper uses the standard metrics for measuring the performance of the proposed model including: key and encryption speed [12] [19] [24].

IV. RESULTS AND DISCUSSION

This section presents the validation outcomes of proposed RLWE key generation procedure with comparable cryptographic schemes such as ECC, ECDSA and RSA. The performances were analyzed on the basis of elapsed time for key generation, public key size and private key size as discussed in the subsequent sections.

A. Key Generation

The performance of the various key infrastructure generation strategies offered by RLWE (the proposed approach), ECDSA, ECC and RSA which all belong to the family of asymmetric algorithm are presented in Table 2.

TABLE III
THE ASYMMETRIC ALGORITHM-BASED KEY GENERATION PERFORMANCES

Cryptographic scheme	**Elapsed time (sec)**	**Public key size (bit)**	**Private key size (bit)**
RLWE (proposed)	0.038329	32	10
ECDSA	1.111095	10	58
ECC	16.622608	97	9
RSA	37.948438	191	687

From Table I, the time taken to generate keys with the proposed RLWE cryptography significantly outperformed comparable asymmetric schemes, that is, ECDSA, ECC and RSA respectively. The implications of the results include: the size of key generated as proportional to the elapsed time during the encryption process of the cryptographic schemes [3]. Electronic health records are time-sensitive applications that require faster encryption schemes such as RLWE for patient data sharing or storage [2]. The graphical representation of key generation of the various asymmetric algorithms are depicted in Fig. 1.

Also, the public key size realized from the proposed RLWE cryptography was second smallest after ECDSA, and better than comparable asymmetric schemes (ECC and RSA). The graphical representation of the sizes of public key generated based on the various asymmetric algorithms are depicted in Fig. 2.

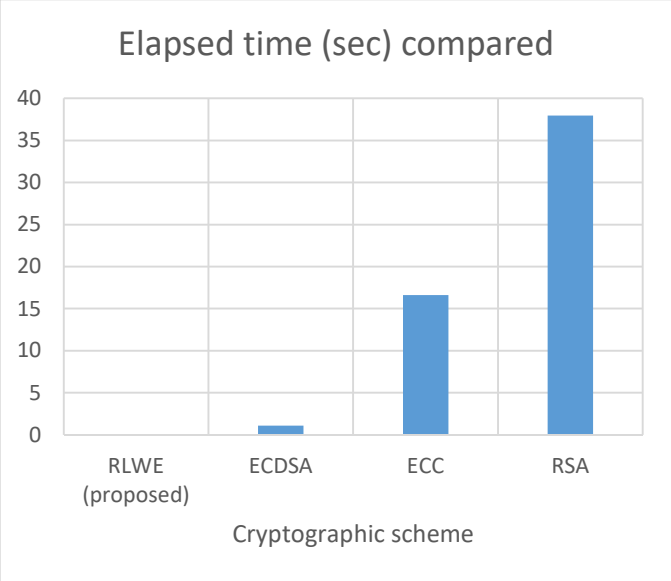

Fig. 1 The key generation elapsed time of asymmetric algorithms compared.

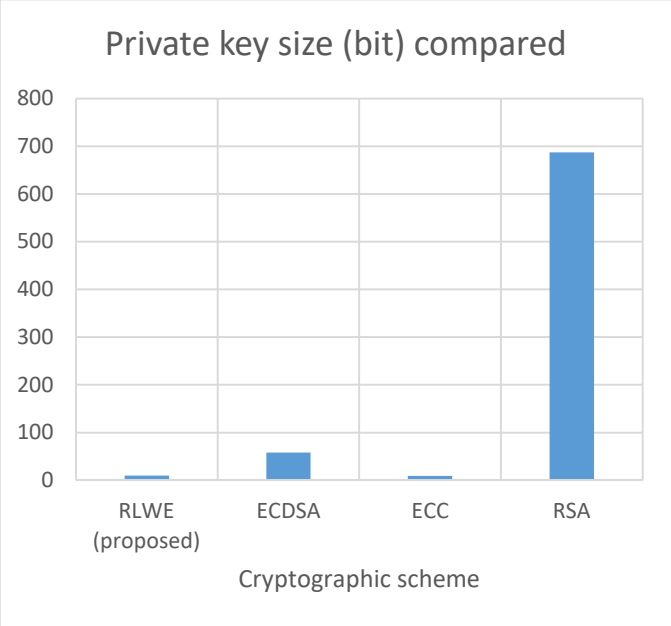

Fig. 2 The public key sizes generated with various asymmetric algorithms compared

More so, the private key size realized from the proposed RLWE cryptography was relatively shorter only behind ECC but, outperformed ECDSA and RSA asymmetric algorithms. The graphical illustration of the sizes of private key generated using the different asymmetric algorithms are shown in Fig. 3.

More so, the private key size realized from the proposed RLWE cryptography was relatively shorter only behind ECC but, outperformed ECDSA and RSA asymmetric algorithms. The graphical illustration of the sizes of private key generated using the different asymmetric algorithms are shown in Fig. 3.

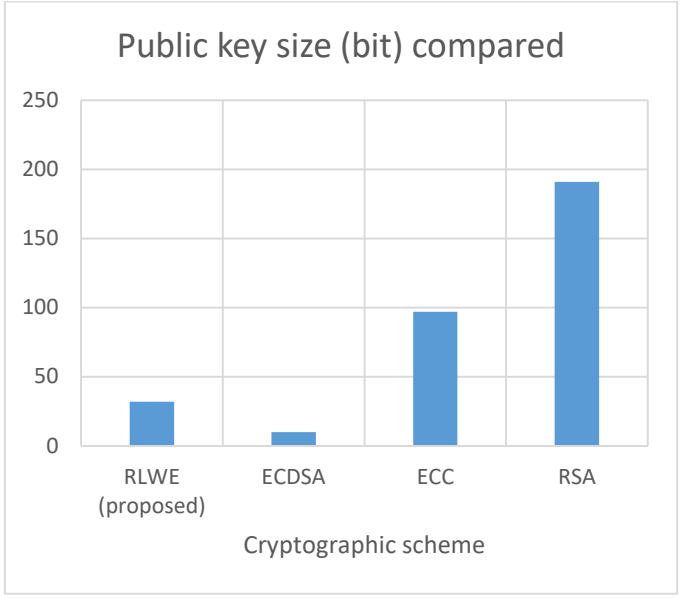

Fig. 3 The public key sizes of the various asymmetric algorithms compared

In term of memory, security, and speed of public infrastructure keys generation procedures, the proposed RLWE was better than ECDSA, ECC and RSA when deployed for authorization, signing and verification applications in protecting privacy of patient information available on digital and decentralized platforms of health information management systems. The implications include low memory usages for the storing the pubic-private keys generated by the RLWE. The overheads incurred during the forging the ciphers based on the public-private keys are highly minimised [3].

B. Forms of Public-Private Key Infrastructure

The ciphertext forms of private and public key generated using the distinct cryptographic schemes against the proposed RLWE are presented in Table 3.

TABLE IIIII
FORMATS OF THE PUBLIC KEY INFRASTRUCTURE COMPARED

Cryptographic scheme	**Private key ciphertext**	**Public key ciphertext**
RLWE (proposed)	B@3dd4a6fa	-1, -64, 62, -48, -33, -44, -39, -83, 87, 30, 102, 42, 36, 79, -39, 103, 43, 47, -14, 32, 41, -126, 42, -18, -15, 105, 98, -42, -27, 34, 98, -25
ECDSA	3642591252839664 8533604891329833 9392349598687282 8327240755	@2752f6e2
ECC	@ffffe8c5	6999243552131957491 3161573774065210491 8942620462, 5069434837475653665 9613357977190345620 10462986930
RSA	3082015502010030 0D06092A864886F 70D0101010500048 2013F3082013B020	305C300D06092A8648 86F70D010101050003 4B0030480241008F23 6FC124A035A71E7BF

	1000241008F236F C124A035A71E7B F62E9BF1C995AC B06E2B0D15CB9A ACBCF39D343109 A0DA9F9FE0BA … A4A0C6E428A522 569AF9D3A1	62E9BF1C995ACB06 E2B0D15CB9AACBC F39D343109A0DA9F9 FE0BA3B0BF…EF020 3010001

From Table 3, the simplest form of public and private keys are the generated by RLWE after ECC. RLWE offered the best form of privacy or protection for EMRs because of relative hardness problems in ciphertext derivations against those of ECDSA and RSA. The contribution of the paper is the relatively shortness in length of both public-private keys without reducing the level of security which contrary to the traditional cryptographic schemes such as RSA, whose strength depends on the relative largeness of their keys/ciphertexts.

V. Conclusion

Recently, the healthcare data concerning patients are sensitive, and susceptible to malicious attacks leading to serious risks caused largely by unauthorized access and tampering. Consequently, there are increasing considerations for privacy and security for the sensitive healthcare information. To this end, this paper takes advantage of lattice-based cryptography (that is, RLWE encryption scheme) to generate private and public keys for privacy of EMRs in the cloud.

Again, the security of RLWE encryption is due to multiple encryption processes and simpler memory capacity [3]. This targets health professionals, third party users such as researchers and regulatory authorities for secure and enhanced administration EMRs.

The outcomes showed that, the RLWE (0.04sec) is better in terms of elapsed time than ECDSA (1.11sec), ECC (16.62sec), and RSA (37.95sec). On the public key size, RLWE outperformed ECC (97-bits), and RSA (191-bits). More so, in private key size, the RLWE (10-bits) was more effective than ECDSA (58-bits), and RSA (687-bits) respectively. Therefore, it recommended that, RLWE can be used for key and hash value generation for better performance of digital ledger technology (Blockchain technology) and privacy of EMRs [14]. In future works, the privacy of medical data can be improved with strong access control schemes based on RLWE encryption schemes.

References

[1] M. Olowu, C. Yinka-banjo, and S. Misra, "A Secured Private-Cloud Computing System A Secured Private-Cloud Computing System," in *ICAI 2019, CCIS*, 2019, vol. 1051, pp. 373–384.

[2] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," *Concurr. Comput. Pract. Exp.*, vol. 33, pp. 1–10, 2021.

[3] I. Boumezbeur and K. Zarour, "Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology," *Acta Inform. Pragensia*, vol. 11, no. 1, pp. 105–122, 2022.

[4] P. K. Premkamal, S. K. Pasupuleti, and P. J. A. Alphonse, "A new verifiable outsourced ciphertext - policy attribute based encryption for big data privacy and access control in cloud," *J. Ambient Intell. Humaniz. Comput.*, pp. 1–15, 2018.

[5] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126. Academic Press, pp. 45–58, 15-Jan-2019.

[6] C. Singh, D. Chauhan, S. A. Deshmukh, S. S. Vishnu, and R. Walia, "Medi-Block record: Secure data sharing using block chain technology," *Informatics Med. Unlocked*, vol. 24, p. 100624, 2021.

[7] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys," in *2017 IEEE 13th International Symposium on Autonomous Decentralized Systems*, 2017, pp. 229–234.

[8] G. Assenza, C. Fioravanti, S. Guarino, and V. Petrassi, "New Perspectives on Wearable Devices and Electronic Health Record Systems," pp. 740–745, 2020.

[9] L. Coppola *et al.*, "Biobanking in health care : evolution and future directions," *J. Transl. Med.*, pp. 1–18, 2019.

[10] W. Bekri, R. Jmal, and L. Chaari Fourati, "Internet of Things Management Based on Software Defined Networking: A Survey," *Int. J. Wirel. Inf. Networks*, vol. 27, no. 3, pp. 385–410, 2020.

[11] V. Echeverr, L. M. Liebrock, and D. Shin, "Permission Management System : Permission as a Service in Cloud Computing," in *2010 34th Annual IEEE Computer Software and Applications Conference Workshops Permission*, 2010, pp. 371–375.

[12] R. E. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," *JBBA*, vol. 2, no. 1, p. 7679, 2019.

[13] E. M. Abou-nassar, A. M. Iliyasu, P. M. El-kafrawy, A. L. I. K. Bashir, and A. A. A. B. D. El-latif, "DITrust Chain: Towards Blockchain-based Trust Models for Sustainable Healthcare IoT Systems," *IEEE Access*, vol. 4, pp. 1–17, 2020.

[14] A. Al Mamun, S. Azam, and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," *IEEE Access*, vol. 10, pp. 5768–5789, 2022.

[15] D. El Majdoubi, H. El Bakkali, S. Sadki, Z. Maqour, and A. Leghmid, "The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment," *Secur. Commun. Networks*, vol. 2022, no. 5642026, pp. 1–26, 2022.

[16] L. W. Warren and H. Chi, "Securing EHRs via CPMA attribute-based encryption on cloud systems," in *Proceedings of the 2014 ACM Southeast Regional Conference, ACM SE 2014*, 2014.

[17] 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," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[18] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019.

[19] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratine, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.

[20] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[21] A. R. Rajput, Q. Li, M. Taleby, and A. Student, "EACMS : Emergency Access Control Management System for Personal Health Record based on Blockchain," *IEEE Access*, vol. pp, p. 1, 2019.

[22] D. Micciancio and O. Regev, *Lattice-based Cryptography*. Springer, Berlin, Heidelberg, 2009.

[23] S. S. Roy and I. Verbauwhede, *Lattice-Based Cryptography in Hardware*. United Kingdom: Springer Nature Singapore Pte Ltd. 2020, 2020.

[24] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight Three-Factor Authentication , Access Control and Ownership Transfer Scheme for E-Health Systems in IoT," *Futur. Gener. Comput. Syst.*, vol. 96, pp. 410–424, 2019.

[25] J. Li, Z. Qiao, K. Zhang, and C. Cui, "A Lattice-Based Homomorphic Proxy Re-Encryption Scheme with Strong Anti-Collusion for Cloud Computing," *Sensors*, vol. 21, no. 288, pp. 1–20, 2021.