Study of COVID-19 Monitoring System Based on Block Chain and Anonymity Techniques

[1]CHENGLIAN LIU, [2]SONIA C-I CHEN
[1]School of Computing, Neusoft Institute of Guangdong, Foshan 528225, CHINA
[2]School of Economics, Qingdao University, Qingdao 266061, CHINA

Abstract: Since the COVID-19 epidemic has been raging around the world, it has a great impact on people's life and work; in addition to monitoring and controlling the epidemic situation, government departments are also facing the impact of economic downturn. The investigation of epidemic situation and the privacy of personal information often contradict each other. It is a headache for countries all over the world how to make both sides perfect. This study uses blockchain technology, combined with cryptography theory, proposes a set of epidemic monitoring information system, which has the function of anonymity. When hospitals or doctors release patient information, they do not need to worry about personal information leakage.

Keywords: ElGamal Algorithm, Anonymity, Double-Blind Mechanism
Received: July 25, 2021. Revised: June 27, 2022. Accepted: August 8, 2022. Published: September 14, 2022.

1. Introduction

When COVID-19 outbreak, the epidemic swept the world, the impact can not be estimated. In particular, this new coronavirus is different from the coronavirus in the past. When people face this situation for the f rst time, they are helpless. It's not just the slow development and diff culty of vaccine production; the existing medical information system is also limited effect. If an additional information system is developed and designed for the new coronavirus epidemic, it will be time-consuming, labor-intensive, and ineff cient. Based on this viewpoint, our study intends to propose a simple and eff cient new coronavirus epidemic monitoring information system, the system uses cryptography and blockchain technology, and has anonymity function. Digital health is an interdisciplinary subject integrating medical treatment, information technology and medical service administration. The major medical units in the world are actively studying how to improve the system function and service eff ciency. At present, the technology is mainly used in mobile medicine, telemedicine, and health analytics. The application of digital health care can be combined with the business model of health care, and the real-time supervision mechanism of COVID-19 is urgent. The anonymity system needs to have a high degree of security, supervision and operability design. The identity of patients is anonymous to the hospital and the health bureau. To a certain extent, the identity is prevented from being leaked in this link; the health bureau has the function of supervision and inspection for the hospitals or doctors, and to prevent fraud between patients-doctors or doctors-hospitals dealers. If the transaction content is verif ed to be untrue, the system center has the right to decode the patient's identity and hold it accountable. Our research uses this as the design framework, combined with the ElGamal [1] and RSA [2] algorithm as the cores, introduces digital signature technology, and adjusts the algorithm to enhance the overall security. The algorithm includes 8 stages, namely: registration stage, account issuance stage, order placement stage, order conf rmation stage, transaction return stage, report business stage, data inquiry and supervision and inspection stage. The last 7 stages are the main content of discussion. , This solution meets the requirements of computational security and theoretical security.

2. Literature Review

In 2013, Chiang [3] began to study the medical research and personal data protection issues related to Japanese epidemiology. In 2016, Bouslimi and Coatrieux [4] proposed a medical image research with cryptography digital watermarking system, which has the characteristics of reliability and traceability. Abdmouleh et al. [5] discussed the encryption of medical images using JPEG algorithm in 2017. Anand and Singh [6] proposed an improved DWT-SVD secure watermarking algorithm in 2020. In 2021, Zermi et al. [7] also proposed a DWT-SVD based robust watermarking algorithm for medical image security in the Forensic Science International. On April of the same year, Fares et al. [8] also proposed a medical information security watermarking scheme by on DCT and DWT. Chen et al. [9] used mobile phone positioning signal to track the whereabouts of passengers on the Diamond Princess Cruise, Park et al. [10] also used information technology tracking technology to detect the epidemic of cowid-19 in South Korea, Liu et al. [11] proposed a tripartite anonymous information system for patients-doctors-hospitals to reduce the leakage risk of personal data privacy. For the research on the application of blockchain technology in medical treatment and health, please refer to [12]–[29]. In this paper, the author lists some literatures which discuss the application of other f elds in health or medicine , such as blockchain, image processing, watermarking, information security and so on. Due to limited conditions, this study lists parts of good contributions, but is a little different then what is discussed in this article, please see Table 1.

Table 1. RELATED LITERATURES

Year	Blockchain	Image	Watermarking	Others
2013				Chiang [3]
2014				
2015				
2016		Bouslimi & Coatrieux [4]	Bouslimi & Coatrieux [4]	
2016	Yue et al. [12]			
2017		Abdmouleh et al. [5]		
2017	Linn & Koo [13]			
2017	Kuo et al. [14]			
2018	Bayle et al. [15]			
2018	Dasaklis et al. [16]			
2018	Sadiku et al. [17]			
2019	Dimitrov [18]			
2019	Manset et al. [19]			
2019	Agbo et al. [20]			
2019	Khezr et al. [21]			
2019	McGhin et al. [22]			
2020	Fang et al. [23]			
2020				Liu et al. [11]
2020	Capece & Lorenzi [24]			
2020				Park et al. [10]
2020				Chen et al. [9]
2020			Anand & Singh [6]	
2020	Farouk et al. [25]			
2020	Hasselgren et al. [26]			
2020	Bell et al. [27]			
2021	Miyachi & Mackey [28]			
2021		Zermi et al. [7]	Zermi et al. [7]	
2021	Hussien et al. [29]			
2021			Fares et al. [8]	

3. Our Research Methodology

This paper extends the concept of information security technology and management, specifically introducing cryptography and information security mechanisms into the COVID-19 monitoring system, combining the two cryptographic algorithms of ElGamal [1] and RSA [2] to meet the requirements of the digitalization process of electronic medical records. In the process of patients using the medical insurance card, the information center can set the identity of the person who knows or does not know (double blind mechanism). Based on this design concept, the medical staff passively know or does not know the patient's identity. In this paper, we propose a conditional anonymity scheme. In the process of submission, patients and the system center have registered and issued account numbers, and patients, hospitals, doctors and the health insurance bureau are anonymous. In the process of the system, the patient has no direct contact with the health insurance bureau, so the health insurance bureau can not know the real identity of the patient at the initial stage; the role of the health insurance bureau has the right to supervise and inspect the doctor's visit content and inquire about the hospital information; the hospital has the responsibility to report the business to the health insurance bureau; the doctor has to report the visit situation to the hospital. This scheme of the algorithm consists of eight phases: registering phase, account issuing phase, medical treatment phase, diagnosis phase, data verification phase, data update phase, data response and final result return phase.

Step 1. Patient opens an account and register to hospital's system center.
Step 2. The system center issues an accounts to patient who applied an ID previously.
Step 3. Patient goes to hospital or clinic to meet a doctor when he feel ill.
Step 4. The doctor diagnoses patient and sent the diagnostic record to system center.
Step 5. The system center received the record from doctor before returned the verification.
Step 6. The doctor updates record with health bureau.
Step 7. The health bureau responds the updating action to doctor.
Step 8. The doctor feeds back the result to patient.

The detailed information flow is shown in Figure 1.
Notation and **Significant**:
p_i: denote a large prime of RSA.
q_i: denote a large prime of RSA.
n_i denote a modulo number of RSA.
e_i denote the public key of RSA.
d_i denote the secret key of RSA.
p_1: denote an other prime number of ElGamal, it different with p_i.
g: is the primitive root of prime number p_1.
x_i: is a private key in ElGamal like algorithm.
y_i: is a public key in ElGamal like algorithm.
m: digitized message.
Health Bureau: The Health Bureau (HB) means Ministry of Health and Welfare (MHL) or National Health Insurance Administration (NHI) in Taiwan. The names of medical institutions in different countries, it may be varieties.
Hospital: We usually means the hospital (or clinic) information system center. Here, we use abbreviation 'hospital' or 'system center'.
Doctor: We denote the staff who works in hospital. There are including nurse and doctor. We preferred mean to doctor who is qualified in medicine and treats people.
Patient: A common person or user who is ill.

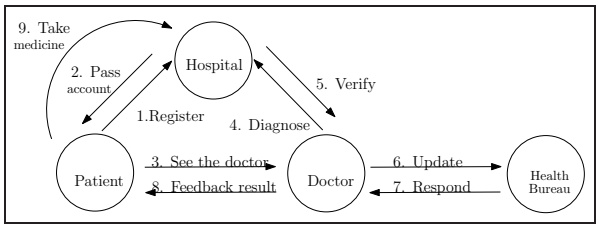

Figure 1. The concept of this system.

3.1. Initializing System Phase

3.1 In the system initialization phase, all users such as patients, doctors, system center and health bureau set their own account numbers and passwords, and share primitive parameters g and a large prime numbers p_1 through the system. The patient randomly selects a number x_a, as its private key and satisfies $\gcd(x_a, p-1)$, then calculates his public key

$$y_a \equiv g^{x_a} \pmod{p} \quad (1)$$

The hospital (or system center) randomly selects its own private key x_b to calculates its own public key y_b, and then announces

$$y_b \equiv g^{x_b} \pmod{p} \quad (2)$$

The doctor randomly selects its own private key x_c to calculates its own public key y_c, and publishes it

$$y_c \equiv g^{x_c} \pmod{p} \quad (3)$$

The health bureau will randomly select its own private key x_d to calculate his public key y_d, and then publishes

$$y_d \equiv g^{x_d} \pmod{p}. \tag{4}$$

Please see Figure 2. Every Users (Patients) randomly

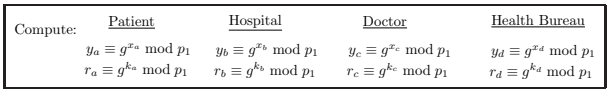

Figure 2. The System Initializing Phase.

select two primes p_i and q_i to find:

$$n_i = p_i \cdot q_i, \tag{5}$$

since

$$\phi(n) = (p_1 - 1) \cdot (q_q - 1). \tag{6}$$

Compute the public key e_i where it satisfied

$$\gcd(e_i, n_i) = 1 \tag{7}$$

and

$$e_i \cdot d_i \equiv 1 \pmod{n_i}. \tag{8}$$

The public key pairs are (e_i, n_i), although the secret key is d_i; we have destroyed some parameters such as (p_i, q_i and $\phi(n_i)$) based on security issue. From Equation (5) to (8), it is well-known RSA algorithm [2].

3.2. Registering Phase

3.2 The Patient uses his ElGamal private key x_a and the RSA secret key d_a to calculate a temporary account from Equation (9) to (11),

$$y_a \equiv g^{x_a} \pmod{p_1}, \tag{9}$$

$$r_a \equiv g^{k_a} \pmod{p_1}, \tag{10}$$

$$R_a \equiv (y_a \cdot r_a)^{d_a} \pmod{n_a}, \tag{11}$$

and register this account to system center (hospital), see Figure 3.

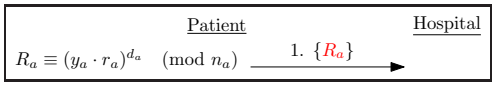

Figure 3. The Registration Phase.

3.3. Issuing Account Phase

3.3 When the hospital receives R_a from patient, hospital approved and returned P_a since

$$P_a \equiv (R_a)^{e_a x_b} \cdot y_c^{x_b} \pmod{n_a}, \tag{12}$$

see Figure 4.

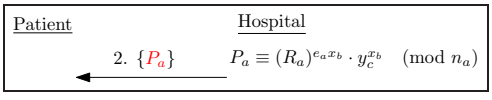

Figure 4. The Account Issuing Phase.

3.4. Meeting Doctor Phase

3.4 The patient obtains a valid account and he then uses W_a and m before he went to hospital to meet a doctor. This operation has an anonymous feature:

$$W_a \equiv (P_a \cdot m)^{d_a} \pmod{n_a}, \tag{13}$$

see Figure 5.

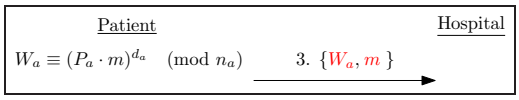

Figure 5. The Watch Doctor Phase.

3.5. Filling Record Phase

3.5 When the doctor receives the patient's requirement, he will diagnose patient and sent the diagnostic record to system center for processing. The process is shown in Equation (14) and Figure 6.

$$C_a \equiv y_c^{W_a} \cdot W_a^{x_c} \pmod{p_1}. \tag{14}$$

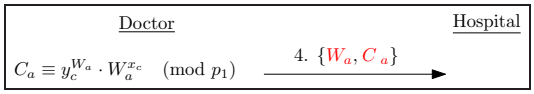

Figure 6. The Fill Record Phase.

3.6. Returning Transaction Phase

3.6 The hospital received the diagnostics record by a doctor, he would check this identifier W_a firstly; if it is hold, and then verified this message before returned to doctor. See Equation (15)-(16) and Figure 7.

$$W_a^{e_a} \stackrel{?}{\equiv} (P_a \cdot m) \pmod{n_a}. \tag{15}$$

If holds, to calculate the Equation (16).

$$V_a \equiv C_a^{x_b} \cdot (W_a^{x_c})^{-x_b} \pmod{p_1}. \tag{16}$$

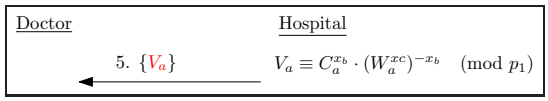

Figure 7. The Transaction Return Phase.

3.7. Reporting Business Phase

3.7 The doctor updates diagnostic record such as calculation Equation (17), and the results to the health bureau, see Figure 8.

$$U_a \equiv (V_a) \cdot y_d^{k_c} \pmod{p_1}, \tag{17}$$

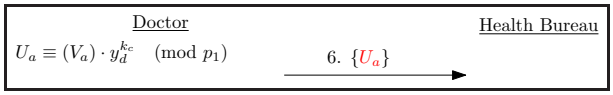

Figure 8. The Report Business Phase.

3.8. Inquiring Data Phase

3.8 When the health bureau received the doctor of updating with diagnostic, he can compute Equation (18) and (19), see Figure 9. The health bureau calculates

$$Ap_0 \equiv (U_a) \cdot r_c^{-x_d} \pmod{p_1}, \tag{18}$$

and

$$Ap_a \equiv (Ap_0) \cdot y_c^{x_d} \cdot m' \pmod{p_1}. \tag{19}$$

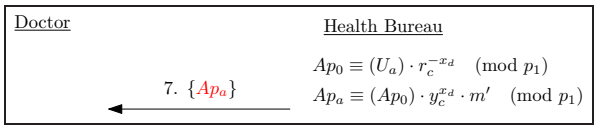

Figure 9. The Information Inquiry Phase.

3.9. Supervising and Inspecting Phase

3.9 In addition to supervising and inquiring the contents of the reports of the stock exchange, the SFC can also supervise and inspect securities companies, see Equation (14) and Figure 10.

$$F_a \equiv (Ap_a) \cdot y_d^{-x_c} \cdot m^{-1} \cdot y_b^{-x_c \cdot W_a} \pmod{p_1}. \tag{20}$$

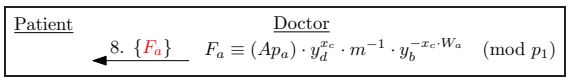

Figure 10. The Supervision and Inspection Phase.

Proof.

$$\begin{aligned} m' &\overset{?}{\equiv} F_a \cdot m \pmod{p_1} \\ &\equiv (Ap_a) \cdot y_d^{-x_c} \cdot m^{-1} \cdot y_b^{-x_c \cdot W_a} \cdot m \pmod{p_1} \\ &\equiv m^{-1} \cdot m' \cdot m \pmod{p_1} \\ &\equiv m' \pmod{p_1} \end{aligned} \tag{21}$$

□

123243

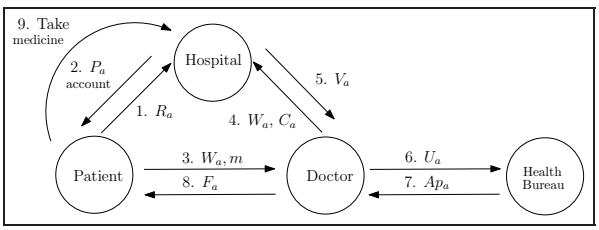

Figure 11. The protocol of this scheme.

4. Security Analysis

1312321

Def nition 1. *Discrete Logarithm Problem (DLP)*
As known parameters $\{p,\ g,\ y_i\}$ *where the formula* $y_i \equiv g^{x_i} \pmod{p}$*, it is very hard to f nd the private key* x_i *while prime approaching inf nite. Based on this assumption of computation and condition, it is called solving the discrete logarithm problem (Solving Discrete Logarithm Problem) [30]. The current public key cryptosystem based on discrete logarithm has value parameters that are greater than* 1024 *bit length or* 2048 *bit length.*

Def nition 2. *Computation Diff e-Hellman Problem (CDHP)*
The Computation Diff e-Hellman Problem [31]is derived on the Diff e-Hellman key exchange principle (Diff e Hellman Key Exchange) [32]. The main ideas are described as follows: Given $\{g,\ g^x,\ g^y\}$ *to f nd* g^{xy}*. Here,* g *is known parameter, the* x *and* y *are unknown parameters.*

Def nition 3. *Decisional Diff e-Hellman Problem (DDHP)*
The Decisional Diff e-Hellman Problem [33] is a variant of the Diff e-Hellman computation problem. Given $\{g,\ g^x,\ g^y,\ g^z\}$*, to f nd the* $\mathbb{Z}_p$ *is satisf ed* $z = xy$*. Given* $\{g,\ g^x,\ g^y\}$*, to f nd* g^{xy}*. Here the parameter* g *is known, and the parameters* $\{x,\ y,\ z\}$ *are all unknown.*

4.1. Theoretical Security Level Analysis

Theoretical Security Level Analysis Analysis security of theoretical level

Lemma 1. *If patient is honest, then the Equation (6) holds, that is, the hospital verif ed the patient.*

Proof. The patient registers R_a through the system center by Equation (5). The system system center uses its RSA's public key e_a to check $W_a^{e_a} \overset{?}{\equiv} (P_a \cdot m) \pmod{n_a}$, if it does not equal, it is determined that the patient deception. Otherwise, patient honestly use his private key x_a in Equation (1), the patient naturally can not deny his behavior, the program has a "user-repudiation" in this scheme. □

Lemma 2. *If doctor is honest, the Equation (7) holds, that is to say, the system center and doctor verif ed each other.*

Proof. As known from Equation (13), doctor sent two parameters C_a and W_a to system center. System center calculates Equation (15) by Equation (14); in this mean time, if system center honestly use his private key x_b to compute V_a before he returned to doctor. The doctor can verify this Equation (22) if it holds. Otherwise, it is not equal, the system center cheated doctor.

$$V_a \overset{?}{\equiv} y_b^{w_a \cdot x_c} \pmod{p_1}. \tag{22}$$

If doctor cheated in Equation (13), namely diagnosing phase, it produced a wrong parameter C_a and then transmitted to system center, the system center naturally can not f nd the correct value V_a. Wrong input, of course get wrong output. The V_a was computed by system center

who can self-checking if doctor honest or not, namely Equation (23)

$$V_a \stackrel{?}{\equiv} y_c^{w_a \cdot x_b} \pmod{p_1}, \tag{23}$$

we rewrite Equation (22) and (23), get

$$V_a \stackrel{?}{\equiv} y_b^{w_a \cdot x_c} \stackrel{?}{\equiv} y_c^{w_a \cdot x_b} \pmod{p_1}. \tag{24}$$

Till now, it means "the system center and doctor verif ed each other". □

Lemma 3. *If doctor and Health Bureau are both interaction honestly, the Equation (16) and (17) holds, the doctor and health bureau can verify each other.*

Proof. As known the health bureau received U_a from doctor, the health bureau honestly use his private key x_d to calculate Ap_0 with Ap_a by Equation (18) and (19), and then returned Ap_a to doctor, the doctor recoveries the message through Equation (19). If doctor want to decode m', he should calculate Equation (25)

$$m' \equiv Ap_a \cdot V_a^{-1} \cdot y_d^{-x_c} \pmod{p_1}. \tag{25}$$

Since doctor obtained V_a by system center, and get the Ap_a from health bureau. We rewrite the Equation (25) into

$$\begin{aligned} m' &\stackrel{?}{\equiv} Ap_a \cdot V_a^{-1} \cdot y_c^{-x_d} \pmod{p_1} \\ &\equiv y_c^{W_a \cdot x_b} \cdot y_c^{x_d} \cdot m' \cdot V_a^{-1} \cdot y_d^{-x_c} \pmod{p_1} \\ &\equiv m' \pmod{p_1}. \end{aligned} \tag{26}$$

□

4.2. Analysis of practical safety levels

Analysis security of practical levels

Doubts about cracking RSA and ElGamal cryptosystems: If the attacker intends to disguise the identity of the patient, the attacker must have the patient's key da to be able to calculate the corresponding pairing public key ea. In addition to being unable to disguise the patient, the attacker cannot disguise the system center, unless the attacker can crack the RSA cryptosystem. Obviously cracking the RSA cryptosystem is not realistic at the moment [34].

Key Compromise Impersonation attacks: The patient, system center, doctor and Health Bureau keep their own keys. Although their public keys are published, the hackers can not calculate the corresponding key through known public parameters. The discrete logarithm problem of the Def nition 1 is def ned and fully described. This study does not consider this assumption unless any party who owns the key divulges the key.

5. Conclusion

This research is mainly about the four-party supervision and management plan of patients, hospitals, doctors, and the National Health Bureau. The improved ElGamal and RSA algorithm are used in the application of the COVID-19 monitoring system. This information system is anonymous and the identity of any patient is strictly controlled. Keep it secret. If the hospital (system) is invaded, hackers cannot obtain patient health record or content through the hospital. If the hacker colludes with any of the regulatory agencies to deceive, he still does not have to worry about identity exposure. If the patient has breached the contract, the doctor and the system center can track the anonymous identity under certain conditions, and f nally restore the anonymous identity to the real-name user identity. In this way, the patient's security can be protected. The identity is protected from exposure, and on the other hand, it can deter patient from maliciously defaulting on transactions. This program has the best of both sides. This research plan puts forward 3 lemmas, 3 def nitions and 26 equations to run through the full text, provide a strong theoretical support for the thesis, and f nally put this idea into reality. This idea shows a patient-hospital monitoring system with anonymity, non-modif cation, security, and double-blind mechanism to achieve a combination of theory and practice.

Acknowledgments

The authors would like to thank the anonymous reviewers for their useful comments.

References

[1] T. ElGAMAL, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] C.-M. F. Chiang, "Medical research and personal-data protection–take Japanese epidemiology research as the basis," *Technology Law Review*, vol. 10, no. 1, pp. 61–113, 2013.

[4] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Processing: Image Communication*, vol. 47, pp. 160–169, September 2016.

[5] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm," *Procedia Computer Science*, vol. 112, pp. 369–376, 2017.

[6] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, February 2020.

[7] N. Zermi, A. Khaldi, K. Redouane, K. Fares, and E. Salah, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Science International*, vol. 320, p. 110691, 2021.

[8] K. Fares, A. Khaldi, K. Redouane, and E. Salah, "DCT and DWT based watermarking scheme for medical information security," *Biomedical Signal Processing and Control*, vol. 66, p. 102403, 2021.

[9] C.-M. Chen, H.-W. Jyan, S.-C. Chien, H.-H. Jen, C.-Y. Hsu, P.-C. Lee, C.-F. Lee, Y.-T. Yang, M.-Y. Chen, L.-S. Chen, H.-H. Chen, and C.-C. Chan, "Containing COVID-19 among 627,386 persons in contact with the diamond princess cruise ship passengers who disembarked in Taiwan: Big data analytics," *Journal of Medical Internet Research*, vol. 22, no. 5, p. e19540, May 2020.

[10] S. Park, G. J. Choi, and H. Ko, "Information technology-based tracing strategy in response to COVID-19 in South Korea-privacy controversies," *JAMA*, vol. 323, no. 21, pp. 2129–2130, June 2020.

[11] C. Liu, J. Fang, S. C.-I. Chen, and D. Gardne, "Study of anonymous complaint system based on patient-doctor and hospital tripartite scheme," *Basic and Clinical Pharmacology and Toxicology*, vol. 126, no. S5, pp. 11–12, April 2020.

[12] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218:1–8, October 2016.

[13] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," https://www.healthit.gov/sites/default/f les/11-74-ablockchainforhealthcare.pdf, 2016.

[14] T.-T. Kuo, C.-N. Hsu, and L. Ohno-Machado, "Modelchain: decentralized privacy-preserving health care predictive modeling framework on private blockchain networks," http://pscanner.ucsd.edu/sites/pscanner.ucsd.edu/f les/uploads/1415\%20Kuo_0.pdf, 2016.

[15] A. Bayle, M. Koscina, D. Manset, and O. Perez-Kempner, "When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry," in *IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, Santiago, Chile, December 2018, pp. 788–792.

[16] T. K. Dasaklis, F. Casino, and C. Patsakis, "Blockchain meets smart health: Towards next generation healthcare services," in *2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA)*, Zakynthos, Greece, July 2018, pp. 1–8.

[17] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, "Block chain technology in healthcare," *International Journal of Advances in Scientif c Research and Engineering*, vol. 4, no. 5, pp. 154–159, May 2018.

[18] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Informatics Research*, vol. 25, no. 1, pp. 51–56, 2019.

[19] M. K. David Manset, Laura Berna and O. P. Kempner, "Blockchain and GDPR compliance for the healthcare industry," *Health Management*, vol. 19, no. 1, pp. 41–44, 2019.

[20] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[21] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, 2019.

[22] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[23] J. Fang, C. Liu, and S. C.-I. Chen, "Toward security and conf dentiality in personal health records via blockchain technology," *Basic and Clinical Pharmacology and Toxicology*, vol. 126, no. S5, p. 10, April 2020.

[24] G. Capece and F. Lorenzi, "Blockchain and healthcare: Opportunities and prospects for the EHR," *Sustainability*, vol. 12, no. 22, p. 9693, 2020.

[25] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Computer Communications*, vol. 154, pp. 223–235, March 2020.

[26] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences–a scoping review," *International Journal of Medical Informatics*, vol. 134, p. 104040, 2020.

[27] L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, "Applications of blockchain within healthcare," *Blockchain in Healthcare Today*, pp. 1–7, August 2020.

[28] K. Miyachi and T. K. Mackey, "hocbs: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Information Processing and Management*, vol. 58, no. 3, 2021.

[29] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *Journal of Industrial Information Integration*, vol. 22, p. 100217, June 2021.

[30] Wikipedia, "Discrete logarithm," https://en.wikipedia.org/wiki/Discrete_logarithm.

[31] ——, "Computational Diff e-Hellman assumption," https://en.wikipedia.org/wiki/Computational_Diff e-Hellman_assumption.

[32] ——, "Diff e-Hellman key exchange," https://en.wikipedia.org/wiki/Diff e_Hellman_key_exchange.

[33] ——, "Decisional Diff e-Hellman assumption," https://en.wikipedia.org/wiki/Decisional_Diff e-Hellman_assumption.

[34] ——, "RSA factoring challenge," https://en.wikipedia.org/wiki/RSA_Factoring_Challenge.