PMRSS: Medical Record Searching Methods in Cloud Computing Techniques

SK. Anjaneyulu Babu [1], Kodimela Bhaskar Rao [2]

[1] Associate Professor, Department of MCA at QISCET(Autonomous), Vengamukkapalem, Prakasam (D.T)

[2] PG Scholar in the Department of MCA at QISCET(Autonomous), Vengamukkapalem, Prakasam (D.T)

ABSTRACT_

Previous patients' cases are exceedingly private in the medical industry, but they are extremely helpful to current disease diagnosis. As a result, how to make maximum use of valuable cases while not compromising patients' privacy is a leading and promising study, particularly in the future privacy-preserving intelligent medical period. We examine how to securely invoke patients records from previous case-databases while respecting the privacy of both the present diagnosed patient and the case database in this work, and we builda privacy-preserving medical record searching technique based on ElGamal Blind Signature. In our system, by blinding the patient's healthy data and the intelligent doctor's database, the patient can securely perform self-help medical diagnoses by invoking previous case- databases and securely comparing the blinded abstracts of current data and previous records. Furthermore, instead of acquiring it after matching, the patient can obtain target searching information intelligently while also knowing whether the abstracts match or not. It significantly improves information acquisition timeliness and meets high-speed information sharing requirements, particularly in the 5G future. Furthermore, our suggested system provides bilateral security, which means that whether the abstracts match or not, both the privacy of the case-database and the present patient's private information are well safeguarded. Furthermore, it resists various levels of violent ergodic attacks by altering the number of zeros in a bit string to meet various security requirements

.

1.INTRODUCTION

WITH the advocacy of sensor innovation and Entomb net of Things medical services, numerous home clinical prepare ment, for example, infrared thermometer, pulse screen, and pulse screen are now very normal in individuals' regular routine and have been utilized to quantify fundamental body param eters, for example, pulse, internal heat level, and so on. Thusly, in IoT medical care situation, patients can make self-helped clinical finding by transferring actual sound information got from IoT clinical gadgets to iDoctor, which is a sort of self-helped administration clinical

framework, to get proficient medical services counsel [1]. Besides, these sort of self-helped administration clinical gadgets are turning out to be more versatile, exact, and individuate with the fast improvement of data innovation [2]-[4]. For this situation, smart clinical finding is an overwhelming and promising pattern in future clinical region. Like Web based business, it will be

very helpful for patients to get customized and professionalized analytic report whenever and anyplace, particularly with the well known of IoT medical services. In any case, the high prerequisite in security of patients' information frustrates iDoctor from giving sound and exact clinical benefits. As of late, clinical data spillage happened whenever inferable from the security weakness of medical care data framework, since malware is increasingly more hard to recognize and oppose [5]-[7]. Accordingly, related medical services information are in risk [8],[9]. For instance, Song of devotion organization, the second biggest U.S. health care coverage supplier, was once gone after by programmers and lead to 78 million bits of client data exposure including patients' singular data, solid information, and another delicate information. In this manner, how to safeguard the security of both flow analyzed patients' data and the information base of the iDoctor other than getting solid and precise clinical outcome brilliantly is the most troublesome issue in the application and improvement of savvy clinical determination, which makes safely looking through related conclusion report from the case-data set of the iDoctor be a promising pattern in future keen clinicalfinding.

2.LITERATURE SURVEY

2.1 K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against covid-19: A blockchain-based approach," IEEE Consum. Electron. Mag., vol. 10, no. 2, pp. 111–120, 1 Mar. 2021.

Abstract:COVID-19 is a major global public health challenge and difficult to control in a short time completely. To prevent the COVID-19 epidemic from continuing to worsen, global scientific research institutions have actively carried out studies on COVID-19, thereby effectively improving the prevention, monitoring, tracking, control, and treatment of the epidemic. However, the COVID-19 electronic medical records (CEMRs) among hospitals worldwide are managed independently. With privacy consideration, CEMRs cannot be made public or shared, which is not conducive to in-depth and extensive research on COVID-19 by medical research institutions. In addition, even if new research results are developed, the disclosure and sharing process is slow. To address this issue, we propose a blockchain-based medical research support platform, which can provide efficient and privacy-preserving data sharing against COVID-19. First, hospitals and medical research institutions are treated as nodes on the alliance chain, so consensus and data sharing among the nodes is achieved. Then, COVID-19 patients, doctors, and researchers need to be authenticated in various institutes. Moreover, doctors and researchers need to be registered with the Fabric certificate authority. The CEMRs for COVID-19 patients uses the blockchain's pseudonym mechanism to protect privacy. After that, doctors upload CEMRs on the alliance chain, and researchers can obtain CEMRs from the alliance chain for research.

Finally, the research results will be published on the blockchain for doctors to use. The experimental results show that the read and write performance and security

performance on the alliance chain meet the requirements, which can promote the wide application of scientific research results against COVID-19.

2.2 K. P. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchainenhanced data sharing with traceable and direct revocation in IIoT," IEEE Trans. Ind. Informat., to be published, oi: 10.1109/TII.2021.3049141.

Abstract:
The industrial Internet of Things (IIoT) supports recent developments in data management and information services, as well as services for smart factories. Nowadays, many mature IIoT cloud platforms are available to serve smart factories. However, due to the semicredibility nature of the IIoT cloud platforms, how to achieve secure storage, access control, information update and deletion for smart factory data, as well as the tracking and revocation of malicious users has become an urgent problem. To solve these problems, in this article, a blockchain-enhanced security access control scheme that supports traceability and revocability has been proposed in IIoT for smart factories. The blockchain first performs unified identity authentication, and stores all public keys, user attribute sets, and revocation list. The system administrator then generates system parameters and issues private keys to users. The domain administrator is responsible for formulating domain security and privacy-protection policies, and performing encryption operations. If the attributes meet the access policies and the user's ID is not in the revocation list, they can obtain the intermediate decryption parameters from the edge/cloud servers. Malicious users can be tracked and revoked during all stages if needed, which ensures the system security under the Decisional Bilinear Diffie-Hellman (DBDH) assumption and can resist multiple attacks. The evaluation has shownthat the size of the public/private keys is smaller compared to other schemes, andthe overhead time is less for public key generation, data encryption, and data decryption stages.

2.3. P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure IoT-based modern healthcare system with fault- tolerant decision making process," IEEE J. Biomed. Health Informat., vol. 25, no. 3, pp. 862–873, Mar. 2021.

Abstract—The advent of Internet of Things (IoT) has escalated the information sharing among various smart devices by many folds, irrespective of their geographical locations. Recently, applications like e-healthcare monitoring has attracted wide attention from the research community, where both the security and the effectiveness of the system are greatly imperative. However, to the best of our knowledge none of the existing literature can accomplish both these objectives (e.g., existing systems are not secure against physical attacks). This paper addresses the shortcomings in existing IoT-based healthcare system. We propose an enhanced system by introducing a Physical Unclonable Function (PUF)-based authentication scheme and a data driven fault-tolerant decision-making scheme for designing an IoT-based modern healthcare system. Analyses show that our proposed scheme is more secure and efficient than existing

systems. Hence, it will be useful in designing

an advanced IoT-basedhealthcare system.

3.PROPOSED SYSTEM

In this work, we focus on this issue and propose an ELGamal blind signature-based safe and practical medical record searching strategy (PMRSS). When compared to earlier systems, our solution has fouradvantages.

1) PMRSS privately realises intelligent self-helped medical diagnosis using IoMT data. There is no need for actual doctors or centres to participate.
2) PMRSS has a short latency. Instead of acquiring after matching, the patient obtains the diagnosis report at the sametime he knows if the encrypted abstracts match or not. In comparison to previous information searching solutions, the proposed scheme eliminates the two extra steps, Feedback and Resend, to obtain the target information after matching, increasing the timeliness of information acquisition and meeting high-speed information sharing requirements, particularly in future 5G D2D communication.
3) Bilateral security is possible. Regardless of whether the abstracts match or not, we can protect the security of both current diagnosed patients' information and the iDoctor database.
4) The amount of zeros in a bit string, represented by the parameter l, can be changed to withstand various levels of violent ergodic attacks according on thesecurity needs.

3.1 IMPLEMENTATION

Cloud Server

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as Login, View and Authorize Doctors, View and Authorize Patients, Add Hospital, View All Attackers, Recover Data, View Attacked and Data Recovered Results, View Patient's Disease Results.

3.1. 2 Doctor

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, View Profile, View Patient Details, View Patient's Indirect and Privacy Details, View Patient Indirect Information, Direct Information Searching

3.1.3 Patient

In this module, there are n numbers ofusers are present. Patient user shouldregister with group option before doingsome operations. After registrationsuccessful he has to wait for admin toauthorize him and after admin authorized him. He can login by using authorizeduser name and password. Loginsuccessful he will do some operationslike Register and Login, Add Patient,Search Patients by Disease.

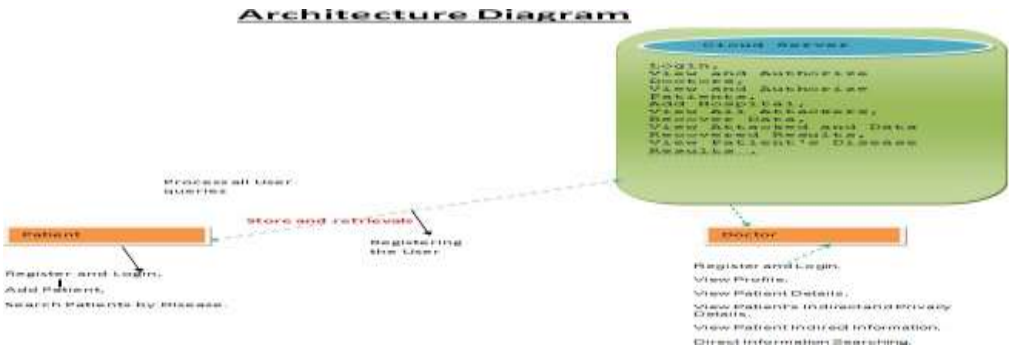

Fig.No:1 System Architecture

4.RESULTS AND DISCUSSION

SCHEME	DESIRABLE PROPERTY							
	DP1	DP2	DP3	DP4	DP5	DP6	DP7	DP8
Medisn-2010 [10]	-	-	-	-	-	-	-	-
Healthedge-2017 [11]	-	-	-	-	-	-	-	-
PHY-2017 [12]	√	-	-	-	√	-	-	-
SSAC-2019 [13]	-	-	-	-	√	√	-	-
LSAS-2019 [14]	√	-	-	√	√	-	-	-
AGE-2019 [15]	√	-	-	√	√	√	-	-
SMAP-2020 [16]	√	-	-	√	√	-	-	-
ECC-2020 [17]	√	-	-	√	√	-	-	-
SHS-2020 [18]	√	-	√	√	√	√	√	-
OUR PMRSS	√	√	√	√	√	√	√	√

Table 1: COMPARISON IN TERMS OF DESIRABLE PROPERTIES

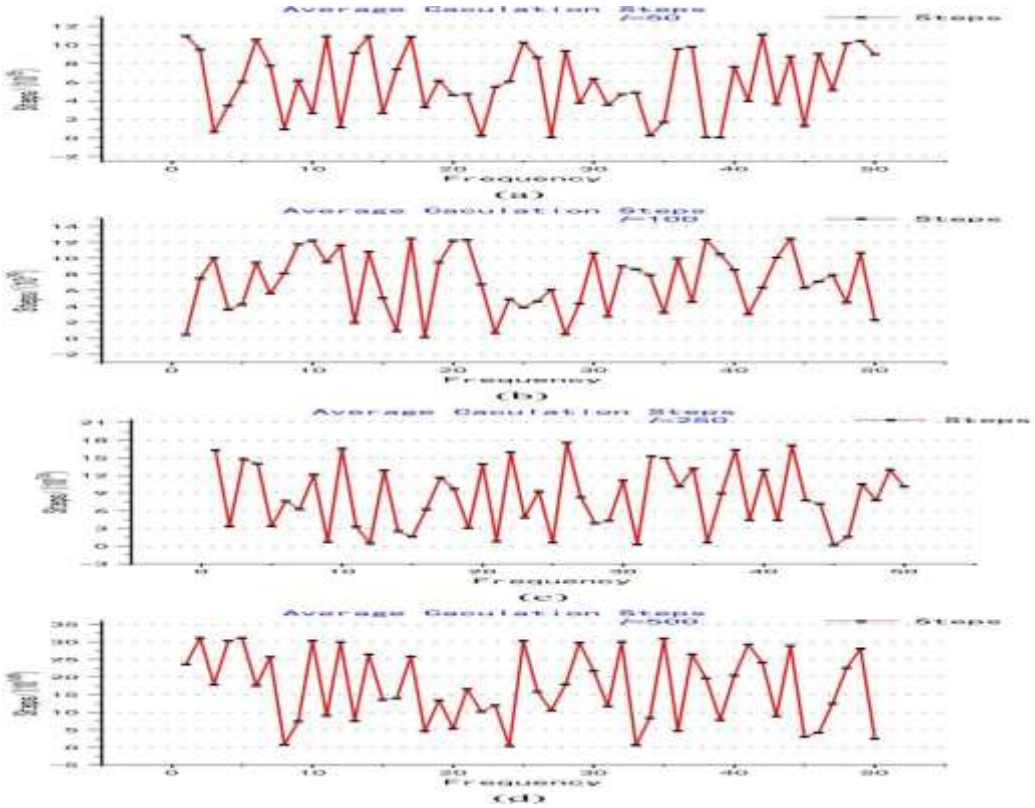

Fig. 2. Average Calculation Steps. (a) Average calculation steps in length 50. (b) Average calculate on steps in length 100. (c) Average calculation steps in length 250. (d) Average calculation steps in length 500.

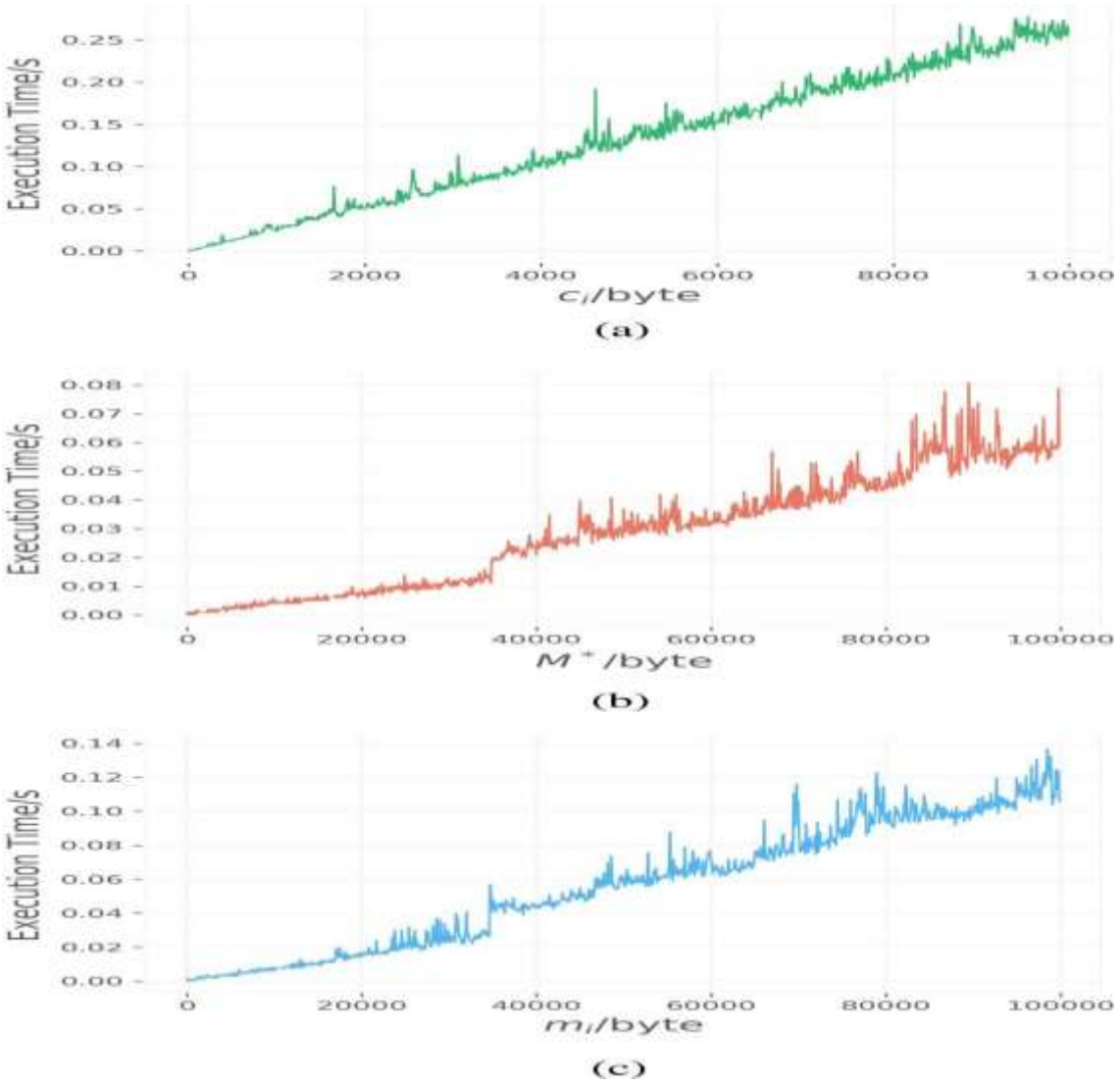

Fig. 3. Execution time. (a) Execution time with c_i. (b) Execution time with M^*. (c) Execution time with m_i.

5. CONCLUSION

In this study, we explore the topic of securely searching an iDoctor medical diagnosis report in IoT healthcare while respecting the privacy of both present patients and iDD that consists of prior patients' instances. We suggested a privacy-preserving medical record searching strategy, PMRSS, that uses ELGamal Digital Signature to securely search the diagnosis report in only two rounds of contacts without exposing any additional information about the two parties. Furthermore, we have a complete security study to demonstrate that PMRSS achieves the security goals. In the future, the most promising areas to concentrate on are how to compress and optimise the iDoctor's datab ase and standardise patient requirements.

REFERENCES

[1] Y. Zhang, R. Gravina, H. Lu, M. Villari, andG.Fortino,"Pea:Parallelelectrocardiogra m-based authentication for smart healthcare systems,"Journalof Network and Computer Applications, vol. 117, pp. 10–16,2018.

[2] Y. Zhang, M. Chen, D. Huang, D. Wu, and Y. Li, "idoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization," Future Generation Computer Systems, vol.66, pp. 30–35,2017.

[3] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against covid-19: A blockchain-based approach," IEEE Consumer Electronics Magazine, 2020.

[4] K. P. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchainenhanced data sharing with traceable and direct revocation in iiot," IEEETransactions on Industrial Informatics, 2021.

[5] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, "Mthael:Cross-architecture iot malware detection based on neural network advanced ensemble learning," IEEE Transactions on Computers, 2020.

[6] S. Sriram, R. Vinayakumar, V. Sowmya, M. Alazab, and K. Soman,"Multi-scalelearning based malware variant detection usingspatialpyramid pooling network," in IEEE INFOCOM 2020-IEEE Conference onComputer Communications Workshops

(INFOCOM WKSHPS). IEEE,2020, pp.740–745.

[7] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, "Network flowbased iot botnet attack detection using deep learning," in IEEE INFOCOM 2020-IEEE Conference on Computer CommunicationsWorkshops(INFOCOM WKSHPS). IEEE, 2020, pp. 189–194.

[8] P. Schwartz and J. R. Reidenberg, Data privacy law: a study of UnitedStates data protection. LEXIS law, 1996.

[9] H. Nissenbaum, Privacy in context: Technology, policy, and the integrityof social life. Stanford University Press, 2009.

[10] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson,T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "Medisn: Medical emergency detection in sensor networks," ACM Transactions on EmbeddedComputing Systems (TECS), vol. 10, no. 1, pp. 1–29, 2010.

[11] P. Hao and X. Wang, "A phy-aided secure iot healthcare systemwith collaboration of social networks," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall). IEEE, 2017, pp.1–6.

[12] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preservingsmart iot-based healthcare big data storage and self-adaptive accesscontrol system," Information Sciences, vol. 479, pp. 567– 592, 2019.

[13] M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and secure

threefactor authentication scheme for remote patient monitoring using onbody wireless networks," Security and Communication Networks, vol.2019, 2019.

[14] T. Kumar, A. Braeken, A. D. Jurcut,
M. Liyanage, and M. Ylianttila,"Age: authentication in gadget-free healthcare environments," Information Technologyand Management, pp. 1–20, 2019.

[15] S. Binu, M. Misbahuddin, and J.Paulose,"Asignaturebasedmutualauthentic ation protocol for remote healthmonitoring," SN ComputerScience, vol. 1,no. 1, pp. 1–14, 2020.

[16] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptographybased enhanced anonymous authentication protocol for wearable healthmonitoring systems," International Journal of Information Security,vol. 19, no. 1, pp. 129–146, 2020.

AUTHOR PROFILE

Mr.SK.ANJANEYULU BABU, Associate Professor in thedepartment of MCA atQIS College Engineering andTechnology (Autonomous). He is esearch publications. His area of interest is Machine learning &Data mining.

K. Bhaskar Rao PGScholar in the department of MCA at

QIS College Engineering andTechnology (Autonomous), Vengamukkapalem, Prakasam (D.T) His areas of Intrests Networking and Cloud Computing.