International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (online): 2347-5552, Volume-11, Issue-3, May 2023
https://doi.org/10.55524/ijircst.2023.11.3.17
Article ID IJIRD-1255, Pages 90-93
www.ijircst.org

Effective Stochastic Decoding Method for Electronic Medical Information Sharing

Janardhan Reddy D[1], GiriBabu Sadineni[2], Telikapalli Sai Krishna Gayathri[3], Gollamudi Venkata Sai Suchithra[4], Venkata Bhargavi Gopisetty[5], Samanthula Soundarya[6], and Dammalapati Haritha[7]

[1]Assistant Professor, Department of Computer Science and Engineering, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India
[2]Associate Professor, Department of Computer Science and Engineering, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India
[3,4,5,6,7]Student, Department of Computer Science and Engineering, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India

ABSTRACT- Several IoT solutions have emerged as a result of the industry's massive expansion. E-health has the potential to provide high-quality, accessible treatment. ' It's a challenge to keep the user 's private medical file safe. Using a cryptography method, such as protecting personal data, is one option. In order to communicate information with several participants, each receiver must have their own unique encryption key (physicians, health agencies, etc.). Recompilation of the master password is required by one side of the (t, n) cutoff selective encryption mechanism for data exchange. This study presents a decentralized decoding method for PHR distribution that is successful. It's simple to exchange information with others without having to reassemble the decoding password. We test the chosen-ciphertext safety of our technique. The JPBC package is used to execute our method on a PC. Our strategy seems to be viable and successful in ePHR, according on the results of our tests.

KEYWORDS- Encryption, Decryption, Internet of Things, Personal Health Records.

I. INTRODUCTION

Because of the increasing number of people living longer and developing persistent illnesses, access to affordable, basic therapy may become more difficult. Because of the Internet of Things, e-health solutions are rapidly expanding and becoming more user-friendly. In e-health, community safety, clinical computing, and business are all intertwined. WiFi and 5G technologies may be used to enhance wellness. [1]– [3]. Respiratory crises, cardiac arrest, and obesity may all be saved through real-time surveillance of connected equipment. Fig. 1 depicts a system of connected gadgets for gathering health-related information. Healthcare professionals get the data through smart devices and laptops. These are statistics from the PHR (PHRs). Health records and care-related details are both included in personal health records (PHRs). Biomedical computers are used to store this patient-managed data [4]. Organizations like hospitals do not develop or manage PHRs, in contrast to EMRs. The information gathered from the patients is sent to the cloud. Medical records are stored in Personal Health Records (PHRs). They offer Web service to clients or organizations that have been pre-approved. Surveys show that 44 percent of people have accessed their clinical files online [5]. In a conventional e PHRs design, data is collected and sent to medicinal computers, as shown in Fig. 2. To examine the patient's PHRs, the physician must get them from the clinical centre and retrieve them. Amazon Web Services and Google Cloud hold and analyze enormous amounts of PHRs information.

Figure 1: Using a device, gather observations

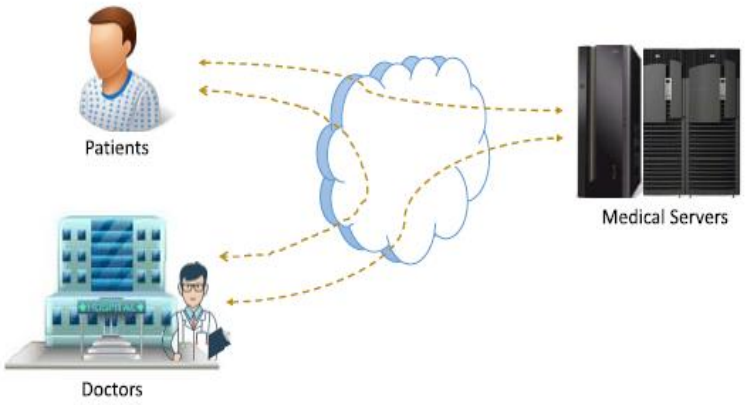

Figure 2: Common electronic health record design.

II. RELATED WORKS

The cloud system has become a hacker target because of confidential Personal Health Records (PHR). As a result, exchanging PHRs with several entities is challenging since they are protected using encryption labels. It is critical, in fact, that the PHRs of individuals be kept secure. The bulk of cybersecurity problems and the largest number of patient data were caused by phishing in the first half of 2019, based to the latest recent Protenus [6] analysis. Identification systems relying on passwords and Open Intellectual Initiative cryptographic keys have indeed been suggested, as noted in [7]. In addition, a number of publicly secret cryptography techniques [8]– [10] have been developed to secure individual Personal Health Records. Because the attacker cannot get the decoding secret password in the event of an information theft, the confidentiality or anonymity of PHRs information will not be jeopardized [11]. There is a lot of vulnerable information in the PHRs. Information that is critical to the confidentiality of a person. In certain cases, strategies have been implemented have been put up that would provide the sufferer to have command over the symmetric encryption PHR. In Indivo [17], for instance, users the ability to create and manage a secure backup of their PHRs. Accessibility management, on the other hand, necessitates some of these Authorized intermediary parties are used in programs. In the academic research [18], presented a dynamic key exchange protocol by Hu and coworkers design. It gives the healthcare practitioner the ability to oversee the PHRs are protected. Benaloh et al. [19] developed a platform that allows individuals to designate accessibility privileges and explore their records. The strategy isn't a viable option for a larger organisation. Sophisticated cryptography is required to protect individuals' PHRs and make data exchange simpler. Attribute-based cryptography is used in several PHR-sharing platforms.

III. PROPOSED METHODOLOGY

A new decentralized decoding algorithm built on Identity Encryption is presented in this chapter for digital PHR communication platforms. As a result, we want to make it possible for numerous entities to access protected health information (PHI). We're now going to go through the specifics of the plan we're thinking about implementing. Our platform paradigm for individual medical details distribution is shown in this chapter. Fig. 3 depicts a schematic representation of how the computerized individual details distribution platform operates.

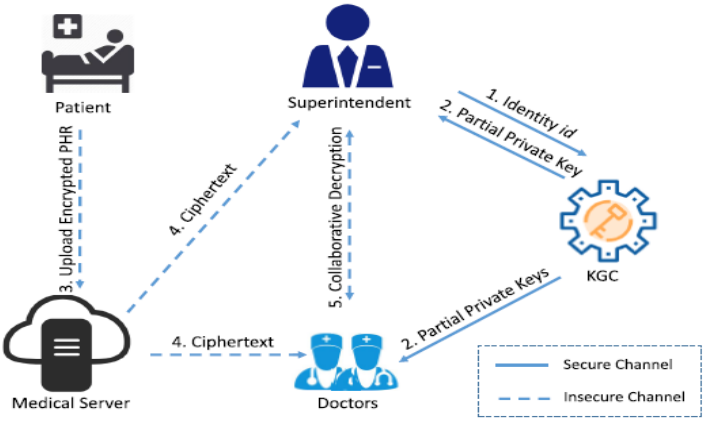

Figure 3: Proposed Methodology

The process of the model is given below:

- The supervisor delivers the Key Generation Center (KGC) a copy of the division's identifying id.
- To the supervisor and division physicians, the KGC delivers the incomplete secret keys it has extracted.

- Encrypting the PHR data and uploading it to the healthcare website is done by the individual in order to distribute the PHRs with the hospital.
- The encrypted message is downloaded from the healthcare website by the supervisor and the physicians.
- The supervisor and the physicians use their respective secret keys to calculate some transient quantities.
- Decrypting encrypted message, the supervisor generates Personal Health Records (PHR) after talking to the physicians.

IV. RESULTS AND DISCUSSION

On a personal computer, we evaluated the performance of our suggested technique against the existing identity-based cryptography approach. Table 1 displays the comparing outcomes. It is important to highlight that the duration expense of stage Decode in our method is the total of the runtime overhead of the dispersed decoding of three parties. We can see from the tables that the Extraction engine in our system is nearly identical to the Extraction engine in the Identity Based Encryption system that inspired it. Because KGC just has to randomly choose a fresh patient's quantity, the computation time factor somehow doesn't rise exponentially as the user base increases.

Fig 4 shows the previous application's process time in a computer setting. Then, we present the findings of our experimentation. A supervisor and two physicians are assumed to be involved in the dispersed decoding technique. Since the supervisor and physicians both use decoding techniques, we'll name the first one DisDecrypt1 and the other two DisDecrypt2. DisExtract is the name given to the KGC's Extraction method. Fig. 5 illustrates the amount of time it takes to implement our suggested method on a computer. The Extraction method in our system consumes the same amount of time as the BF-IBE Extraction method, as illustrated in Fig, 4 and Fig. 5. Consequently, the suggested plan is advantageous to physicians who use smart phones. A more effective method, particularly in a multi-doctor scenario, is possible since the physicians in the trustworthy network structure don't have to do a zero-knowledge demonstration, and the procedure performed by the supervisor is also more effective.

Table 1: Time comparison on personal computer

Method	SetUp	Extract	Encrypt	De-crypt
Identity Based Encryption	20.06 ms	46.94 ms	58.34 ms	24.42 ms
Proposed	20.06 ms	48.62 ms	60.58 ms	169.56 ms

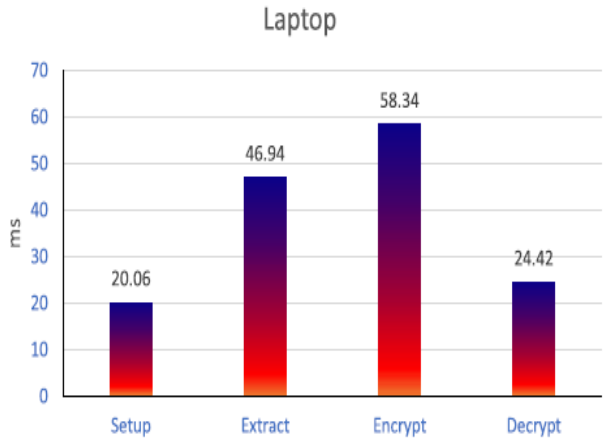

Figure 4: Running time of existing approaches on personal computer.

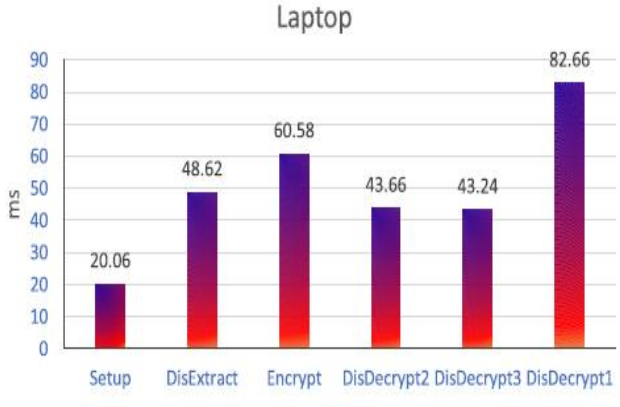

Figure 5: Running time of proposed approach on personal computer.

V. CONCLUSION AND FUTURE SCOPE

A large number of people make use of platforms for exchanging and storing computerized versions of their medical documents. In these kinds of technologies and situations, confidentiality and safety concerns become crucial. Secure storage of critical personal data, including as prescriptions, persistent medical conditions, vaccination records, and secret data, is critical yet difficult in these settings. E-health individual medical files may be shared securely and efficiently using the Boneh Franklin identity-based cryptography approach in this research. Patients may use our system to secure their PHRs under the guise of a physician or a division. Different entities may safely decipher the encrypted message such as multiple gadgets of physician, or the supervisor in a same division. The participants may decode the encrypted message without rebuilding the secret keys since our approach is small enough to run on portable machines. In a vulnerability examination, our method was found to meet the requirements of security standards. Our suggested methodology is practicable in real-world individual medical records communication platforms, as per the findings of the experiments we conducted. Eventually, we'll look at methods that don't need the zero-knowledge proof and disseminate the hidden message without the use of a concealed route.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] G. Eysenbach, "What is e-health?" J. Med. Internet Res., vol. 3, no. 2, p. e20, 2001.

[2] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Gener. Comput. Syst., vol. 57, pp. 24–41, Apr. 2016.

[3] M. Obaidat and N. Boudriga, Security of E-Systems and Computer Networks. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[4] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption," J. Amer. Med. Inform. Assoc., vol. 13, no. 2, pp. 121–126, Mar. 2006.

[5] R. Pifer. Patient Use of Digital Health Tools Lags Behind Hype, Poll Finds. Accessed: Sep. 12, 2019. [Online]. Available: https://www. healthcaredive.com/news/patient-use-of-digital-health-tools-lags-behindhype- poll-finds/562778/

[6] Protenus. (2018). 32 Million Breached Patient Records in First Half of 2019 Double Total for all of 2018. Accessed: Jul. 31, 2019. [Online]. Available: https://www.prnewswire.com/news-releases/32-million-breached-patient-records-in-first-half-of-2019-double-total-forall-of-2018-300894237.html

[7] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," J. Biomed. Informat., vol. 46, no. 3, pp. 541–562, Jun. 2013.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[9] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487–497, Nov. 2015.

[10] X. Liu, Y. Xia, W. Yang, and F. Yang, "Secure and efficient querying over personal health records in cloud computing," Neurocomputing, vol. 274, pp. 99–105, Jan. 2018.

[11] M. S. Obaidat, I. Traore, and I. Woungang, Biometric-Based Physical and Cybersecurity Systems, vol. 368. Cham, Switzerland: Springer,2019.

[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 2139, J. Kilin, Eds. Berlin, Germany: Springer, Aug. 2001, pp. 213–229.

[13] M. Focus. Voltage Securemail On-Premises On-Premises Email Encryption. Accessed: Oct. 20, 2018. [Online]. Available: https://www.microfocus.com/en-us/products/email-encryption-security/

[14] M. L. PURA and V. V. Patriciu, "Identity-based chryptography: From proposals to everyday use," Sci. Res. Educ. Air Force-AFASES, vol. 1, pp. 367–374, May 2014.

[15] X. Boyen and L. Martin, Identity-Based Cryptography Standard (IBCS)#1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems,document RFC 5091, Dec. 2007.

[16] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in Proc. IEEE Symp. Comput. Commun. (ISCC), Jun. 2011, pp. 850–855.

[17] K. D. Mandl, W. W. Simons, W. C. Crawford, and J. M. Abbett, "Indivo: A personally controlled health record for health information exchange and communication," BMC Med. Informat. Decis. Making, vol. 7, no. 1, p. 25, Dec. 2007.

[18] J. Hu, H.-H. Chen, and T.-W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," Comput. Standards Interfaces, vol. 32, nos. 5–6, pp. 274–280, Oct. 2010.

[19] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in Proc. ACM Workshop Cloud Comput. Secur. (CCSW), 2009, pp. 103–114.

[20] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in Proc. 2nd Int. Conf. eHealth, Telemedicine,Social Med., Feb. 2010, pp. 95–99.

[21] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proc. 1st ACM Workshop Secur. Privacy Smartphones Mobile Devices (SPSM), 2011, pp. 75–86.