Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 8, pp. 2419–2429
DOI : 10.47974/JDMSC-2015

A novel optimization-based time-enabled proxy re-encryption approach for securing e-health data in cloud environments : An interdisciplinary statistical perspective

K. Gurnadha Gupta *
Muma College of Business
University of South Florida
Vadeswaram 522502
Guntur
Andhra Pradesh
India

and

Department of CSE-HONERS
Koneru Lakshmaiah Education Foundation University (Deemed to be University)
Green Fields
Vadeswaram
Guntur 522302
Andhra Pradesh
India

Bhuvan Unhelkar §
Muma College of Business
University of South Florida
N. Tamiami Trail Sarasota
Florida 8350
USA

S. Siva Shankar ^
Department of Computer Science and Engineering
KG Reddy College of Engineering and Technology
Moinabad 501504
Telangana
India

* *E-mail:* **kbgrguptha@gmail.com (Corresponding Author)**
§ *E-mail:* **bunhelkar@usf.edu**
^ *E-mail:* **drsivashankars@gmail.com**

Tulika Chakrabarti [‡]
Department of Chemistry
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
lndia

Prasun Chakrabarti [@]
Department of Computer Science and Engineering
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
lndia

B. Sivaneasan [#]
Department of Computer Science and Engineering
KG Reddy College of Engineering and Technology
Moinabad 500075
Telangana
India

Martin Margala [$]
School of Computing and Informatics
University of Louisiana at Lafayette
Lafayette
LA- 70503 (337) 482-6768
U.S.A.

Abstract

Electronic health records (EHRs) aim to improve healthcare efficiency and workload management, but security concerns persist, especially in cloud storage. Proxy re-encryption (PRE) addresses these concerns by allowing authorized intermediaries to convert encrypted data without accessing plaintext. This paper introduces Whale-based Timing Enabled Proxy Re-encryption (WTEPRE), enhancing EHR security in the cloud. WTEPRE employs machine learning to generate keys for encryption and decryption. A designated proxy server re-encrypts data for cloud storage, while a time-seal server regulates file access. Experimental results show WTEPRE's effectiveness in bolstering security and privacy with acceptable performance.

Subject Classification: *94A60, 94-00.*

Keywords: *Electronic health records, Proxy re-encryption, Whale optimization, Symmetric encryption, Time seal server, Proxy server, Interdisciplinary, Statistics.*

[‡] *E-mail:* **tulika.chakrabarti@spsu.ac.in**
[@] *E-mail:* **drprasun.cse@gmail.com**
[#] *E-mail:* **sivaneasan@singaporetech.edu.sg**
[$] *E-mail:* **Martin.margala@louisiana.edu**

1. Introduction

Decades have seen the rise of E-health, revolutionizing healthcare delivery [1]. E-health records streamline processes, enhancing work-life balance for professionals [2], improving patient information accuracy [3], and facilitating secure collaboration [4]. However, security concerns persist, especially with the integration of cloud computing [5-6]. Medical devices monitoring vital signs generate vast data stored in the cloud, raising security issues [7-8]. Outsourcing computation expands the attack surface for malicious actors targeting Electronic Health Records (EHRs) [9-10]. Cloud security practices are crucial for safeguarding sensitive data [11-12].

This research proposes an optimized Proxy Re-encryption (PRE) scheme to enhance E-health data security [13]. The scheme allows authorized intermediaries to convert encrypted data without accessing plaintext. The objectives are to enhance E-health data security and develop an improved security framework for EHRs [14]. The model involves patient EHR training, WTEPRE design, data encryption, storage, time-based access control, and performance evaluation [15]. The article structure covers relevant literature, system model, methodology, experimental outcomes, and conclusion.

The key contribution of the developed model is that the system learned from diverse EHR data to establish essential patterns. Developed WTEPRE to protect medical records on cloud servers. EHRs were encrypted and stored securely using WTEPRE. Implemented a time-seal

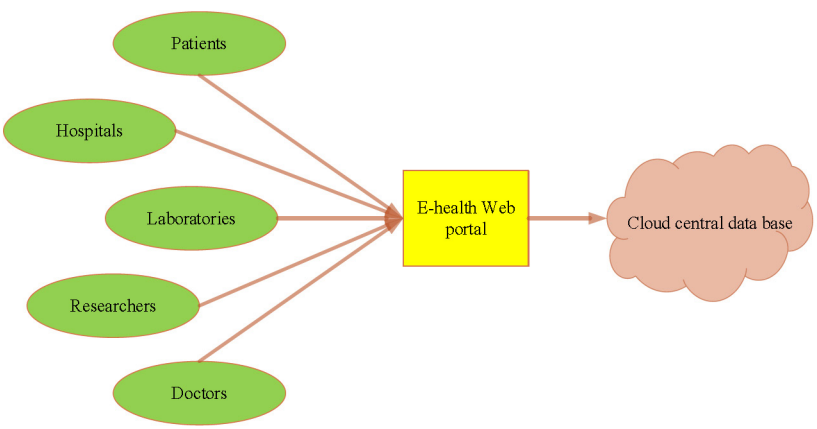

Figure 1

Cloud-based E-health system

server for precise data access control. WTEPRE's efficiency was rigorously compared against existing models.

II. Related works

Xhafa et al. proposed a proxy re-encryption (PRE) system based on identification for safe data sharing on social media, known for its fast encryption but higher delay rate compared to other methods. Hu et al. introduced a blockchain-based PRE model for cloud data security, minimizing attack risk through a threshold value and decentralizing storage to eliminate third-party reliance. Mittal et al. developed an identity-based encryption (IBE) algorithm for E-health records, offering faster encryption and decryption with lower power consumption but higher overhead. Hassan et al. presented a certificate-based incremental PRE model for efficient data sharing in fog computing, streamlining file modifications with improved key generation but increased encryption time. Vijayakumar et al. devised a timing-enabled PRE scheme for E-health data security, limiting access within specific timeframes to address vulnerabilities. This approach combines searchable encryption and PRE, enhancing energy efficiency but with longer execution times.

III. Problem statement and system model

IoT sensors transmit Electronic Health Records (EHR) to a cloud server, secured by Attribute-Based Encryption (ABE). Personal Health

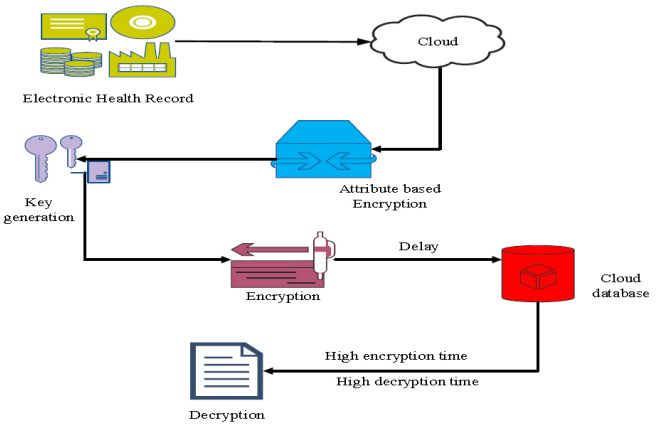

Figure 2

Problem statement and system model

Records (PHR) are stored using a confidential key. Encryption delays and vulnerabilities during transmission affect efficiency. Optimization-based Patient Record Encryption (PRE) uses re-encryption keys to mitigate network issues and enhance security.

IV. Proposed methodology

Improve cloud security for e-health by utilizing Whale-based Timing Enabled Proxy Re-Encryption (WTEPRE). Owners encrypt EHR data for secure searchability and store it in the cloud. Clients access data via a private key. Data owners secure EHRs in third-party databases, encrypting them for storage. Using Patient Record Encryption (PRE), data undergoes re-encryption for secure indices. Users access data within set timeframes managed by time seal servers. Time seals are generated and distributed for decryption.

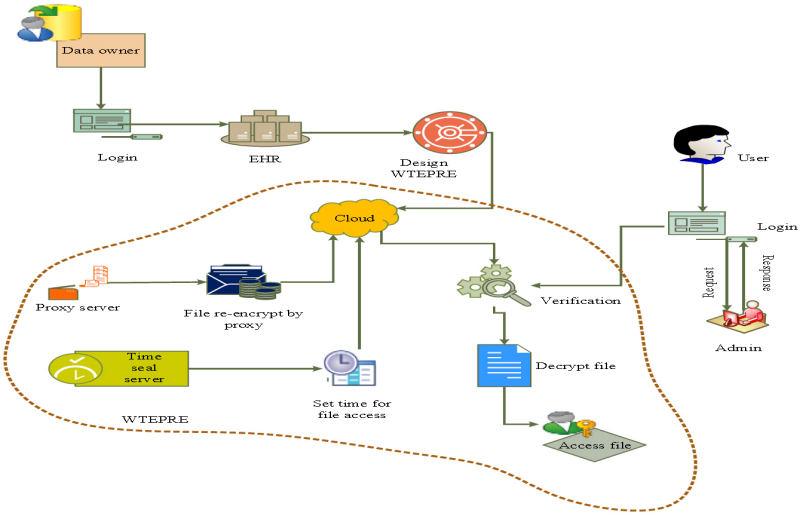

Figure 3

Proposed methodology

V. Process of designing the WTEPRE model

The model enhances E-health security using a proxy server, time seal server, and data centre, with Patient Record Encryption (PRE) for data security. Time seal servers regulate file access, and adjustments to whale fitness during encryption improve key generation.

Setup Phase: Generates security parameters and user counts. Users create key pairs with public parameters, maintaining an Empty Revocation List (ERL). System initialization follows using equation (1).

$$S(p) = (S_k, N_u, Mp_r, Mp_u, b, B_1, B_2) \tag{1}$$

Key generation: The generated public parameter P_p Depending on the Data Owner (DO) and Data User (DU), create your own private and public key pairs. Additionally, DO compute the public key and choose the private key at random. $R_k(a)$. Also, DU randomly selects the private key. $b \in Q_k$ and calculates the public key $R_k(b)$.

Data encryption: In phase, the plaintext Pi_t Is converted into cypher text using Whale fitness and symmetric encryption. It enhances the security from attacks and unauthorized access. Thus, symmetric key encryption needs the user to secrete the key. S_k. Frequently, encrypted data Ci_t Are uploaded to the cloud server. Thus, the encryption is obtained using eqn. (2)

$$Ci_t = encrypt(S_k(Q_k), data, W_t) \tag{2}$$

Re-encryption key generation: The DO measures and generates the re-encryption key based on the private and public key pairs of requester DU. Moreover, PRE generates a re-encryption key to enhance security, which computes the number of proxy nodes using re-encrypted keys. Thus, the computation is obtained using Eqn. (3)

$$\mathrm{Re}_{en}(DO \to DU) = g^{b/a} \tag{3}$$

Furthermore, the input of the DO is $S_k(DO)$ The public key of DU is $R_k(DU)$. Moreover, number of the proxy nodes is denoted as N_p The threshold value is represented as T_v. Also, g Is denoted as a random coefficient. The process of re-encrypted key generation is obtained using eqn. (4)

$$\mathrm{Re}_{en} = S_k / R_k \frac{T_v}{N_p} \to \mathrm{Re}_k \tag{4}$$

It generates the re-encryption key Re_k And sends to the proxy server without close-fitting the secret information about the user.

Time seal server: The assigned period of users is calculated in this phase which contains the name and assigned period. Using its unique private key, it generates the time seal. Q_k. It provides the period. t_p It is employed in time seal creation. ts_e In-time seal server.

Proxy Re-encryption: The proxy server sends the first level of cypher text $Ci_t(A) \in sender$ to the second level of cipher text $Ci_t(B) \in receiver$. The proxy nodes convert the original. Ci_t with re-encrypted keys Re_k to the re-encrypted data $C_q(t)$. Thus the re-encryption is calculated using eqn. (5).

$$Ci_t(B) = (Ci_t \rightarrow C_q(t) / \mathrm{Re}_k) \tag{5}$$

Thus proxy server checks the control list of access policy, and then the proxy server re-encrypts the file and allows the user to download it.

Data decryption: Finally, the user's private and public keys are verified with the cloud storage, DO responds to the user and offers to access the file. Moreover, decryption is processed using the public key R_k. Thus the data decryption is obtained using eqn. (6)

$$Pi_t = decrypt(R_k, ts_e, Ci_t) \tag{6}$$

Finally, access the user based on the timing access of the user and re-encrypted keys. The designed model accesses the plain text and verifies the correctness and integrity of data through the public key. The model enhances E-health data security by offering PRE with public key pairs and time-controlled access. It encrypts patient EHRs in the cloud to prevent unauthorized access, with only the suitable key owner able to decrypt the file, ensuring high confidentiality.

VI. Results

By employing PRE and efficient algorithms, it enhances data privacy and securely connects patient requests. Comparison with IBPRE, IBC, CB-PReS, TEPReE, and TPRE validates its effectiveness.

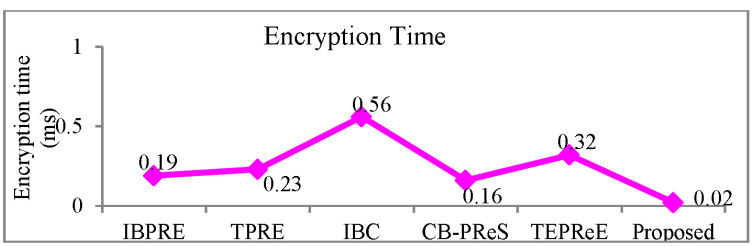

Figure 4

Comparison of encryption time

Figure 4 compares the encryption times of the proposed method with existing ones like IBPRE, TPRE, IBC, CB-PReS, and TEPReE.

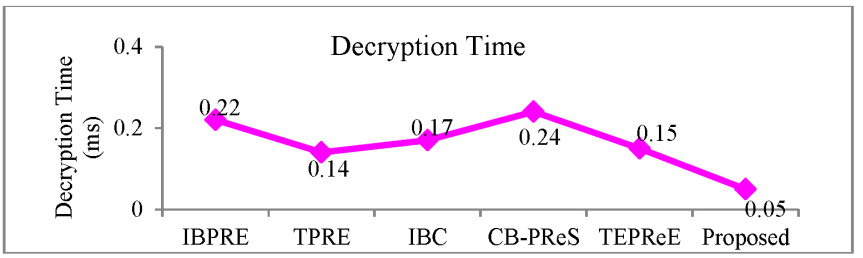

Figure 5

Comparison of decryption time

Figure 5 compares the decryption times of the proposed method with IBPRE, TPRE, IBC, CB-PReS, and TEPReE.

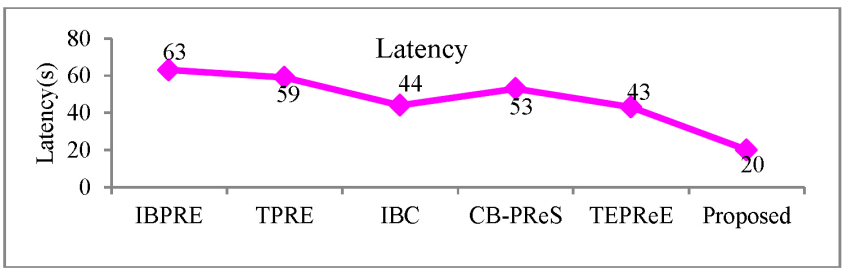

Figure 6

Comparison of latency

Figure 6 compares latency between the proposed method and existing ones like IBPRE, TPRE, IBC, CB-PReS, and TEPReE.

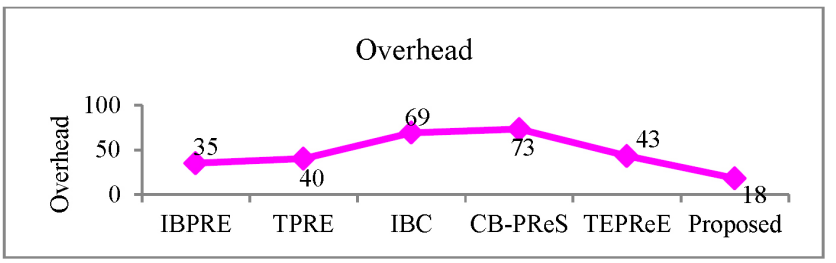

Figure 7

Comparison of overhead

Figure 7 compares overhead. The proposed method achieves significantly lower overhead.

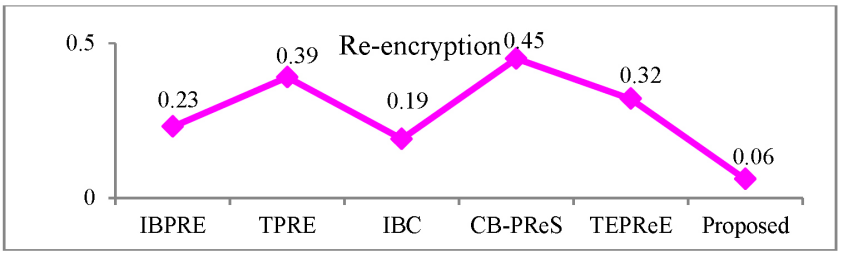

Figure 9

Comparison of re-encryption time

Figure 9 compares re-encryption time, calculated based on the conversion time of encrypted ciphertext.

VII. Discussion

The proposed model of WTEPRE has shown good performance by attaining the best performance in time spent on overhead, re-encryption, delay, encryption, and decryption. As a result, the created technique uses PRE and an improved algorithm to protect E-health data. It analyses the requests of all patients and provides access to a suitable person. Additionally, the PRE technique is utilized to allow the proxy to re-encrypting the encrypted ciphertext, also enhancing the protection of electronic health data privacy and security by utilizing appropriate public and private keys. Moreover, the fitness of the whale is updated to the encryption phase. Thus, the developed technique attains less time for encrypting data and gains network latency is low.

VIII. Conclusion

Design a new timing-enabled PRE scheme to enhance E-health security and privacy in the cloud. Initially, collect and train EHRs of various patients in the system. Encrypt the dataset using a symmetric encryption algorithm and upload it to the cloud using private keys. Update the whale fitness function during encryption to improve performance. During encryption, convert plaintext to ciphertext for enhanced security. Utilize the PRE model to re-encrypt ciphertext, generating keys for storage in the cloud. The model verifies data access for users, providing proper access to data owners. The developed model's outcomes are validated against other techniques, showing better results

with lower encryption and decryption times, as well as reduced latency and overhead for enhanced security and access control.

References

[1] G. I. Ahmad, J. Singla, and K. J. Giri, "Security and privacy of e-health data," in Multimedia Security: Algorithm Development, Analysis and Applications, pp. 199–214 (2021).

[2] M. N. Alolayyan, M. S. Alyahya, A. H. Alalawin, A. Shoukat, and F. T. Nusairat, "Health information technology and hospital performance: The role of health information quality in teaching hospitals," Heliyon, vol. 6, no. 10 (2020).

[3] S. Chen, X. Guo, T. Wu, and X. Ju, "Exploring the influence of doctor–patient social ties and knowledge ties on patient selection," *Internet Research*, vol. 32, no. 1, pp. 219–240 (2022).

[4] Z. Eslami, M. Noroozi, and K. Amirizirtol, "Public key encryption with distributed keyword search," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2369–2393 (2022).

[5] T. H. Tebeje and J. Klein, "Applications of e-health to support person-centered health care at the time of COVID-19 pandemic," *Telemedicine and e-Health*, vol. 27, no. 2, pp. 150–158 (2021).

[6] N. A. Saqib, A. A. Salam, Atta-Ur-Rahman, and S. Dash, "Reviewing risks and vulnerabilities in Web 2.0 for matching security considerations in Web 3.0," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 3, pp. 809–825 (2021).

[7] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications," *Computer Communications,* vol. 180, pp. 31–47 (2021).

[8] S. Gore, I. Dutt, R. P. Dahake, H. E. Khodke, S. L. Kurkute, B. J. Dange, and S. Gore, "Innovations in smart city water supply systems," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 9s, pp. 277–281 (2023).

[9] K. Rahul, R. K. Banyal, and P. Goswami, "Analysis and processing aspects of data in big data applications," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 23, no. 2, pp. 385–393 (2020).

[10] H. B. Mahajan, "Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: Solutions, challenges, and future roadmap," *Wireless Personal Communications,* vol. 126, no. 3, pp. 2425–2446 (2022).

[11] H. E. Khodke, M. Bhalerao, S. N. Gunjal, G. S. Nirmal, S. Gore, and B. J. Dange, "An intelligent approach to empowering the research of biomedical machine learning in medical data analysis using PALM," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 11, pp. 429–436 (2023).

[12] S. Gore, S. Hamsa, S. Roychowdhury, G. Patil, S. Gore, and S. Karmode, "Augmented intelligence in machine learning for cybersecurity: Enhancing threat detection and human-machine collaboration," in 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), pp. 638–644, IEEE, Aug. (2023).

[13] Q. Liu, D. Luo, J. E. Haase, Q. Guo, X. Q. Wang, S. Liu, and B. X. Yang, "The experiences of health-care providers during the COVID-19 crisis in China: A qualitative study," *The Lancet Global Health*, vol. 8, no. 6, pp. e790–e798 (2020).

[14] Q. Liu, D. Luo, J. E. Haase, Q. Guo, X. Q. Wang, S. Liu, and B. X. Yang, "The experiences of health-care providers during the COVID-19 crisis in China: A qualitative study," *The Lancet Global Health,* vol. 8, no. 6, pp. e790–e798 (2020).

[15] R. Mythili, N. Parthiban, and V. Kavitha, "Construction of heterogeneous medical knowledge graph from electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 921–930 (2022).

Received February, 2024