Healthcare 4.0 Enabled Lightweight Security Provisions for Medical Data Processing

Nilesh Uke[1], Priya Pise[2], Hemant B. Mahajan[3], Sumeet Harale[4], Shailaja Uke[5],

Professor, Trinity Academy of Engineering, Pune, nilesh.uke@gmail.com
Associate Professor, Associate Professor, Indira College of Engineering & Management, Pune
PHD Scholar, University of Technology Jaipur. Research Analyst, Godwit Technologies, Pune, mahhemant@gmail.com
Assistant Professor, Indira College of Engineering & Management, Pune,
Assistant Professor, SKN SITS, Pune

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract. The recent progress of the Internet of Things (IoT) for various smart city applications into the Industry 4.0 resolution offers different advantages and challenges. E-healthcare is one of the vital applications of Industry 4.0 emerging as the Healthcare 4.0 standard for remote health monitoring. Healthcare 4.0 is originally a sub-class of Industry 4.0 standard. The Healthcare 4.0 standard consists of different layers such as edge layer, fog layer, cloud storage layer, and blockchain layer. For E-healthcare systems, the main challenges are concerning medical data security and privacy-preserving while processing the data from edge-layer to cloud storage layer via fog computing. The development of blockchain technology connected with cloud storage and edge layer offers strong security provisions. However, there are not enough experimental works available to address lightweight cryptography with blockchain implementation. In this paper, the robust framework of securing the medical data processing using blockchain connected with the cloud storage system has proposed. The medical data collected at the edge layer first encrypted using Elliptic Curve Cryptography using Elliptic Curve Diffie Hellman (ECDH). The encrypted data has stored in cloud storage, and then it is reflected in the blockchain. For signature generation and authentication of medical data, the Elliptic Curve Digital Signature Algorithm (ECDSA) has been designed. The experimental outcome of the proposed framework outperforms the state-of-art solutions.

Keywords: Blockchain, cloud storage, elliptical curve cryptography, healthcare 4.0, internet of things, medical data, privacy preservation, security.

1 Introduction

Inspired by wireless Electronic Health Record (EHR) practices, real-time medical data collection using wearable things, Artificial Intelligence (AI), and enhanced data interpretation, a soft change is forthcoming in the healthcare domain. Across the upcoming years, it will improve how healthcare has presented and how the results are estimated. This novel revolution is known as Healthcare 4.0 [1-3]. It is a phrase that emerged recently and experienced from Industry 4.0 and the next revaluation of various Internet of Things (IoT) applications [4-7]. The IoT-assisted smart city applications like Intelligent Transportation System (ITS), intelligent health monitoring, precision farming, intelligent home automation, etc. obtained notable study from the researchers [1] [2]. The Healthcare 4.0 assisted e-healthcare is therefore developing technology for remote patient's health tracking. Cloud Service Provider (CSP) represents an essential role in Healthcare 4.0 standard. The basic cloud-based method of saving and sharing the medicinal data between the various providers assisting each supplier in dealing with their data, providing a steady technique for dealing and perhaps securing data between EHRs and Personal Health Records (PHR), and carrying a bound collectively perspective on personal services records for each victim. In PHR, victims get their data and save it in the cloud. The Electronic Medical Record (EMR) at each healthcare administrator can obtain the records of the particular victim from the cloud storage. The EHR is a cloud storage system from which the dispensaries or users can obtain the medical records of the victim for medical examination from any geographic place.

Since the occurrence of novel Covid-19 disease worldwide, the healthcare systems have now become more digital. The chest X-ray data, oxygen level, blood pressure, and other medical tests of particular patients have been exchanged digitally to examine Covid-19 infection in worldwide healthcare systems [8-10]. It shows that medical information preparation has become a significant activity of the Healthcare 4.0 standard particularly the circumstances like the Covid-19 pandemic. Since the most recent decade, it saw that medical care is information escalated innovation in which a tremendous measure of information presented, spread, saved, and brought oftentimes. At the point when the patient goes through any tests, for instance, its data is made that further requirements to scatter to the medical specialists like radiographer and doctor. In brilliant medical services frameworks, the medical information put away in the emergency clinic workers considering the future necessities of access by the approved doctor from the clinic situated inside their organizations. A huge job can play by innovation while improving the nature of administration for the patients. It permits information examination to take proper medical choices. Moreover, it assists with lessening the expenses by the proficient assignment of medical assets like hardware, staff, and so forth [8-10].

The evolution of blockchain technology over various areas provides a solid solution to overcome security-related issues according to appealing highlights like immutability and decentralization [11-14]. Blockchain technology has shown an efficient resolution to deliver higher safety and computation performance than traditional cryptography methods for cloud storage and sharing operations. Recently, some efforts were made for secure data processing using blockchain for e-healthcare in association with CPS, but with insufficient scope and lack of relevant examinations. The blockchain is an innovation prepared to amass an open and circled online data set involved an overview of information structures called impedes that associated with creating the chain. These blocks are passed on among various centers of an establishment and not midway set aside. Each block contains a timestamp of its creation, the hash of the past block and the trade information, a patient's medical care information, and the medical care provider information. In this paper, we proposed the novel Healthcare 4.0 assisted medical data processing framework with CSP using robust Blockchain technology for data security, privacy preservation, and reduction computational and space requirements. The lightweight cryptography algorithm using ECC has been designed for the encryption and decryption of medical data in the proposed framework. Section 2 presents the review of related works and research contributions. Section 3 presents the proposed methodology. Section 4 presents the experimental background, results, and analysis. Section 5 presents the simulation results.

2 Related Works

A. Healthcare Security

The security worries for e-medical services increasing while performing data activities with CSPs. Presenting the blockchain for data security and privacy conservation with the CSP is a difficult research issue. As of late, a few endeavors were made to address this issue. The blockchain-based data-sharing structure proposed in [15] sufficiently approaches the entrance control troubles associated with reasonable medical data gathered in the cloud utilizing worked and permanence autonomy highlights of the blockchain. Solid cryptographic techniques were inferred to ensure powerful access control for shared data pool(s) applying an authorization blockchain. In [16], the MeDShare proposed to handle the issue of medical services data dividing among drug huge data accompanies in trust-less conditions. The blockchain innovation applied to accomplish the data evaluating, data provenance, and control for divided data in cloud holders between large data substances. In [17], the TKSE (Trustworthy Keywords Search over Encrypted data) had proposed without utilizing an outsider structure. They utilized blockchain for data stockpiling and imparting tasks in association with CSP. In [18], system for individual medical data stockpiling on cloud and blockchain had proposed. To address the difficulties of privacy conservation in PHRs, blockchain-based admittance control calculations were suggested in [19]. The blockchain-based medical data stockpiling and sharing methodology had proposed in [20] called MedChain. They planned capacities like blockchain joining and condensation chain. The chain digest creation strategy to confirm the honesty of medical data got from the IoT stream. For cryptography tasks, they utilized a lightweight ECC plot. Nonetheless, a few impediments have been identified with manual data age and worker-related intricacies. In [21], the new methodology utilizing ordinary data stockpiling and security capacities for EHRs had proposed. They planned a blockchain-based framework to address medical data honesty and upgrade framework interoperability. The blocks were made utilizing a novel motivator method. Nonetheless, this methodology didn't perform activities like medical data stockpiling, sharing, and searching under different dangers. In [22], another blockchain-based system for medical data stockpiling and sharing under altering dangers had introduced. They planned an agreement method to improve the blockchain execution and indications coordinating with calculation for shared confirmation. The epic MedSBA structure proposed in [23] utilizing attributed-based encryption and blockchain innovation for medical data preparation. They presented the GDPR (General Data Protection Regulation) conspire for privacy conservation and fine-grain access control of patient's data. The security framework had intended for media medical services data utilizing blockchain in [24]. They had utilized the hash age strategy for each data to ensure against change or altering dangers. In any case, CSP had not considered any medical data preparing tasks. The united structure of blockchain and distributed computing had proposed in [25] for privacy protection of medical data connections with cloud and blockchain. They planned a technique for distributed computing and its connection with blockchain hubs to play out the safe medical data activities. Recently similar kind of methodology had introduced in [26] where they formulated the requirements for the real-time health monitoring using blockchain.

A. Research Gaps and Contributions

The above study of recent works shows that the integration of blockchain and cloud computing technologies for smart healthcare systems still at the initial level. From these studies, the research gaps are identified such as lack of generality, inefficient cryptography, conventional threats, over-dependent on blockchain tools, and lack of benchmark results. In this paper, we attempt to address these challenges by the novel consolidated framework using the lightweight cryptography operations connected with cloud computing and blockchain. The contributions are:

- A reliable and generalized consolidated framework has been proposed to process the medical data functions with security and privacy provisions that consist of edge, fog, cloud storage, and blockchain layers.
- The lightweight ECC-based cryptography algorithms have been used to reduce the computational burden and provide strong security provisions using ECDSA for signature verification and ECDH for encryption/decryption operations.
- To claim the scalability and reliability of the proposed consolidated framework, experimental analysis considering different parameters has been presented.

3 Methodology

A. System Model

The system model of proposed Healthcare 4.0 assisted medical data processing in connection with CSP and blockchain technologies have been presented in this section. Figure 1 shows the proposed united structure by considering all the essential advancements of arising Healthcare 4.0. The connections between the parts are bidirectional for handling the send and get activities of collected medical data. The proposed system comprises five parts like data proprietor (IoT hub or patient), medical client, fog hubs, CSP, and blockchain. On the opposite side, figure 1 likewise shows the layers of Healthcare 4.0 innovation, for example, edge layer, fog layer, a cloud layer, and blockchain layer. The edge layer comprises an assortment of IoT gadgets like Wireless Body Area Network (WBAN) hubs, mobiles phones, PCs, and so forth. Fog layer is fog registering administrations in which activities of data focuses are relocated into fog hubs to diminish data transmission time with high data rates. The Cloud layer performs activities of data stockpiling, at long last blockchain layers answerable for circulated capacity of CSP meta-data and logs in the chain of various blocks. Supposedly, this is the primary endeavor that characterized the four layers for Healthcare 4.0 applications.

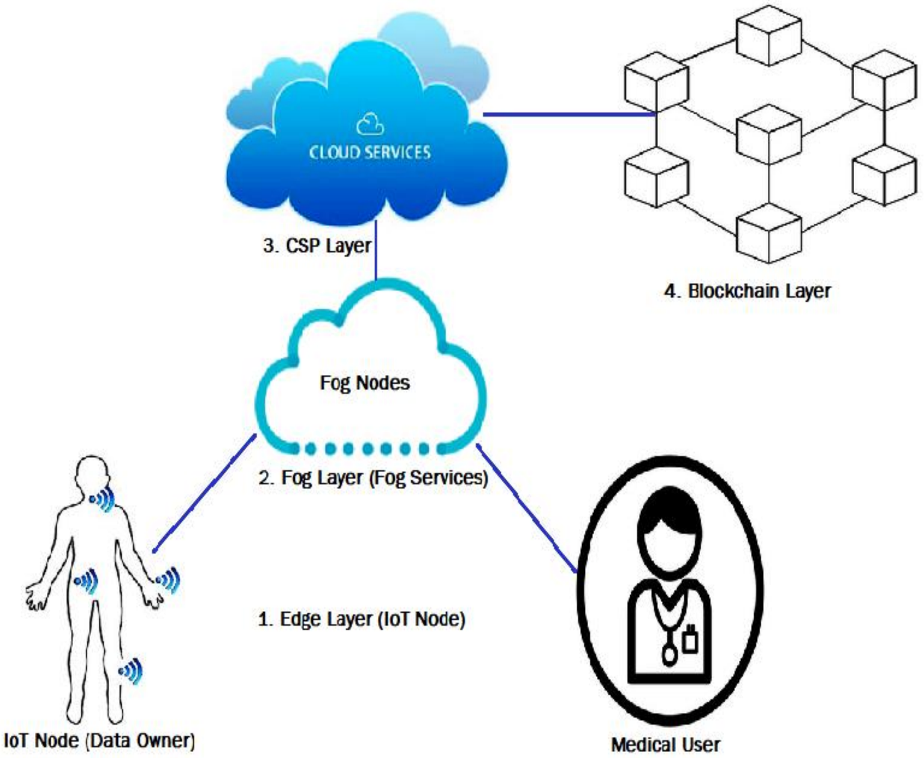

Figure 1. Proposed architecture of Healthcare 4.0 enabled secured medical data storage and sharing.

The design is shown in figure 1 proposing a Healthcare 4.0 assisted safe smart healthcare system. Consequently, we effectively defined elements and their communications in the proposed model. At first sight, the medical data sensed by body sensor nodes installed on each patient's body has already been registered and verified with the smart hospital practice. The sensed data then encrypted and transmitted to the fog nodes. At fog nodes, collected data verified, and then transmitted to CSP storage including indexing. The access log and meta-data has produced for every incoming encrypted data from the victims and saved into distributed private blockchain for effective security goals against the different vulnerabilities. The proposed system model consists of five components such as IoT Node (IN), Medical User (MU), Fog Node (FN), Cloud Storage (CS), and Private Blockchain (PB). A next section presents the two important operations of this model such as medical data storage and sharing.

B. Medical Data Storage

This section presents the proposed algorithm for secured medical data storage from edge layer to cloud layer and blockchain layer via fog computing. Algorithm 1 shows the processing of medical data storage. The periodic medical data generated at IN is encrypted using the ECC-based proposed encryption method. After that, a digital signature has produced for the encrypted information using the ECDSA succeeded by the index formation. The index produced applying the current timestamp connected with IN. The encrypted information has then been forwarded to the FN where the digital signature is validated to verify its integrity toward the various threats. If the validation is successful, then the received encrypted message is forwarded to CS for storage. At CS, the obtained message has been newly verified and then made its storage into CSP. At the corresponding period, the meta-data of encrypted data created and saved into PB in a distributed model. This approach not only produces lightweight medical data storage with the least communication time but also powerful security against multiple threats. If the verification of the digital signature of an encrypted message failed at any component, then the message is discarded with all its associated keys, and an alert is raised to hospital management and associated IN to take necessary measures. It also reveals that medical data auditing operations can directly be performed by obtaining its access logs from PB by IN. The consolidated method of authentication and signature employing hybrid ECC-based cryptography has been demonstrated in algorithm 1. The symbols and notations used in algorithm 1 are presented in Table 1.

Table 1. Notations and their significance

Notation	Significance
IN	IoT node (data owner)
FN	Fog nodes (Fog computing services)
CS	Cloud storage
MU	Medical user
PB	Private blockchain
G	Elliptic curve base point
Pr	ECC private key
Pu	ECC public key
TS	Current timestamp associated with M and IN
M	Periodically collected medical data at IN
i	Index associated with encrypted M and IN
(r, s)	ECDSA signature pair
Sh	Shared secrete key of ECDH
$M^{encrypt}$	Encrypted medical data associated with M and IN
M^{hash}	Hash of $M^{encrypt}$
n	multiplicative order of curve point G

Algorithm 1: Secured Medical Data Storage

```
Inputs
$M$: $data\ from\ IN$
$TS$: $Timestamp\ of\ system\ to\ generate\ index$
1. At $IN$
    1.1. $(Pr, Pu) = GenECCKey()$
    1.2. $Sh$: Compute ECDH shared secrete key using Eq. (3)
    1.3. If $(M \neq null)$
             $(M^{encrypt}, i) = encryption(M, Sh, TS)$
         Else
             $discard\ (M)$
         End If
    1.4. $M^{hash} = SHA2\ (M^{encrypt})$
    1.5. $(r, s) = signing\ (M^{hash}, Pr, Pu)$
    1.6. $forward\ (M_{sign}^{encrypt}, i, r, s)$
2. At $FN$
    2.1. Get associated $Pu$
    2.2. Check the $Pu$ validity
    2.3. $M^{hash} = SHA2\ (M^{encrypt})$
    2.4. $f = verify\ (M^{hash}, r, s,\ Pu)$
    2.5. If $(f\ == 1)$
```

```
                $forward\ (M^{encrypt}, i, r, s)$
            Else
                $discard\ (M^{encrypt});\ break$
            End If
    3.  At $CS\ and\ PB$
        3.1.  Get associated $Pu$
        3.2.  Check the $Pu$ validity
        3.3.  $M^{hash} = SHA2\ (M^{encrypt})$
        3.4.  $f = verify\ (M^{hash}, r, s,\ Pu)$
        3.5.  If $(f\ == 1)$
            $store \rightarrow CSP\ (M^{encrypt}, i)$
            $PB \leftarrow built\_meta\_data(M^{encrypt}, i)$
            $PB \leftarrow update\ access \log associated\ IN\ \&\ index\ i$
      Else
            $discard\ (M^{encrypt});\ break$
      End If
    4.  Stop
```

As showing in algorithm 1, the first step is related to key generation $(Pr, Pu) = GenECCKey\ (.)$. For input medical data $M,\ IN$ creates the key pair of private and public keys. Private key is randomly generated within range mentioned in below Eq. (1):

$$Pr = rand\ (1, n-1) \tag{1}$$

The public key is generated by using the base curve point and private key as:

$$Pu = Pr\ \times G \tag{2}$$

Where, × represents the scalar multiplication of elliptic curve point.

For hybrid encryption approach, we used the ECDH by generating its shared secrete key as:

$$Sh = Pu\ \times Pr \tag{3}$$

The Sh is then used for AES-128 symmetric encryption in proposed model.

C. Secure Data Searching

The next operation of the proposed model is secure searching of medical data from the CSP and blockchain via fog computing. As discussed earlier, the search functionality enabled only for pre-defined users called MU that belongs to hospital, insurance, and pathology.

- ***Step 1:*** At MU, MU first send the search request to CS. The search request contains information such as data owner (IN) ID with associated index i. The meta-data shares the associated private and public keys to MU which is further verified by MU. If the authentication outcome is sucess, then MU performs the signature generation using the current timestamp and transmit it as a request for retrieval of actual data towards CS via FN.
- ***Step 2:*** At FN, signature verification is performed similarly as we did in algorithm 1 for MU using the current timestamp. If signature verification succeeds for MU, then request forwarded to CS node.
- **Step 3:** At CS, signature verification was performed for MU. If signature verification succeeds for MU, then meta-data of request created and store it on PB for auditing. Then, CS extracts the requested encrypted medical data and signs it using the associated keys to protect from threats.
- **Step 4:** The signed data received at FN, verified and forwarded towards MU if verified successfully.
- **Step 5:** At MU, the encrypted data received which is further required to convert into plaintext form by applying decryption. As the MU, already had a key pair of public and private (Pr, Pu) associated with IN and index i, it first computes the shared secrete key Sh. Finally, once Sh discovered, MU apply symmetric decryption according to the AES-128 bit algorithm and recover the original plaintext.

4 Experimental Results

The proposed model had implemented on Windows 10 OS with 4 GB RAM and Intel® Core i5 processor. The programming language Java used with Netbeans IDE. For all the cryptographic operations, we used Java security library, Bounty Castle libraries, and Java Pairing-Based Cryptography (jPBC). For the CS node, we designed the Amazon Web Services (AWS) called Amazon S3. The Java AWS SDK (Software Development Kit) has been used to allow the CS node functionality of the proposed model and state-of-art models. The FN had implemented using virtual functions to understand their functionality in the proposed model. For the PB node, we designed the Hyperledger blockchain network in the Docker background with node.js. The PB node consists of two peer nodes, the order node, and the endorser node. For comparative analysis, searchable symmetric encryption (SSE) based method called TKSE [17], Proxy Re-Encryption Scheme (PRES) [21], and Proxy Re-

Encryption using RSA (PRER) [25] have been implemented. We compare the performance of the proposed model with these three state-of-art techniques by varying the data size with a fixed number of medical users 20. The medical data is generated from these sources periodically with help of publically available research datasets of Covid-19 disease [27] [28]. Figure 2 (table 2) and figure 3 (table 3) shows the results of average encryption and average decryption time using each method by varying the data size. Figure 3 shows the outcome of both encryption and decryption time considering all the scenarios.

Table 2. Average encryption time (milliseconds) analysis in varying medical data size scenario

Data Size	PRER	TKSE	PRES	Proposed
128 KB	671	645	201	115
512 KB	753	741	231	149
2 MB	845	829	325	192
8 MB	939	910	434	234
32 MB	1678	1626	759	431
64 MB	4839	4709	3837	2139

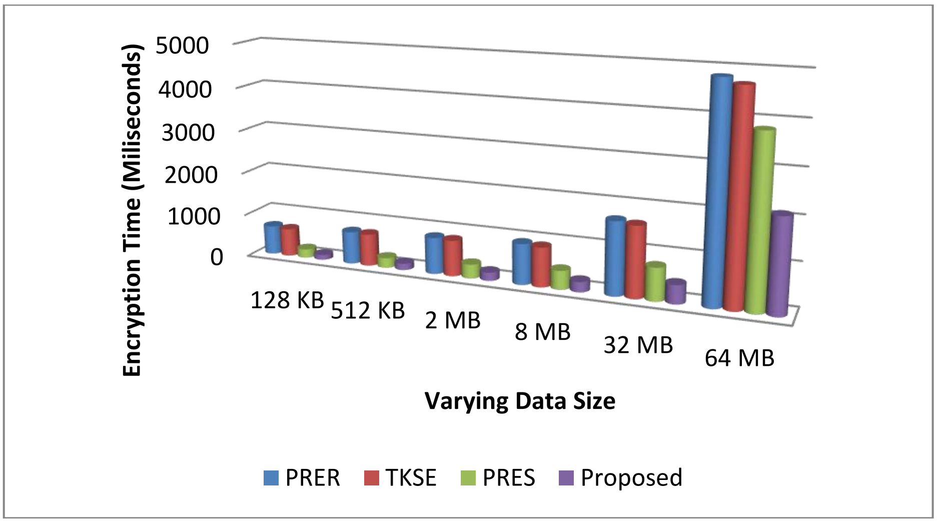

Figure 2. Average encryption time analysis for varying data size scenario

Table 3. Average decryption time (milliseconds) analysis in varying medical data size scenario

Data Size	PRER	TKSE	PRES	Proposed
128 KB	352	324	14	9
512 KB	379	741	19	14
2 MB	457	433	49	37
8 MB	682	649	147	121
32 MB	1048	1010	648	398
64 MB	4187	4029	3751	1903

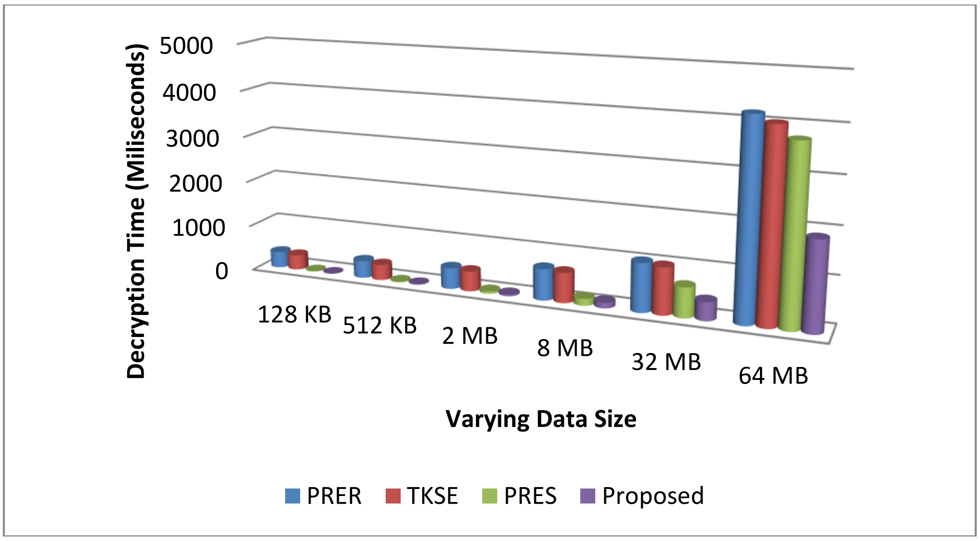

Figure 3. Average decryption time analysis for varying data size scenario

The result of encryption and decryption time for every system with changing data size reveals that there a fast improvement in execution time as the medical data size increases to sparse MB's. The proposed cryptography algorithm results in a notable decrease in encryption and decryption time for all scenarios of data size as opposed to all state-of-art techniques. This is because of the small size of public and shared secrete keys of the ECC-based encryption of the proposed technique. The 256-bits public and private keys in the proposed model reduces the overhead of encryption and decryption procedures. Among the existing methods, 1024 bits PRER and TKSE have shown the worst results due to using RSA and symmetric key encryption mechanisms respectively compared to PRES. Figure 4 shows the summed outcomes for varying data size scenarios of every cryptography method. The proposed method shows that encryption time decreased by approximately 400 milliseconds and decryption time decreased by 350 milliseconds approximately.

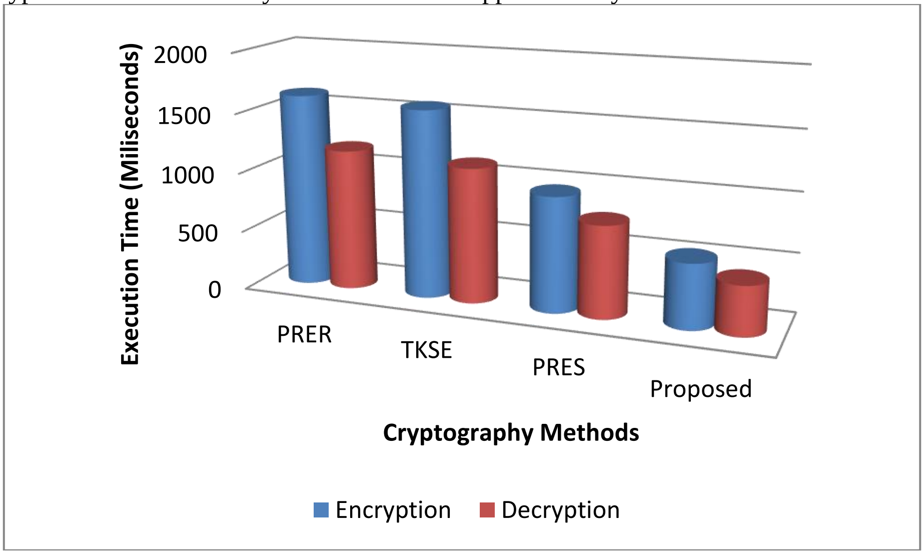

Figure 4. Overall encryption and decryption time for varying data size scenario

5 Conclusion and Future Work

In this paper, we proposed lightweight cryptography with powerful security and privacy provider for medical data processing services in Healthcare 4.0 enabled applications. To protect the data from security threats, the blockchain had connected with CSP. The cryptography methodology designed for secure and lightweight operations such as secure medical data storage and secure medical data searching in Healthcare 4.0 supported medical data processing. For that purpose, the ECC-driven lightweight cryptography techniques had designed. The authorized IN can also perform the operations like data auditing and modifications by directly interacting with blockchain nodes by accessing metadata and access logs stored. The experimental results prove the efficiency and scalability of the proposed model. For future work, we suggest preparing a similar kind of mechanism for multimedia medical data processing.

References

1. Parveen S., Singh P., Arora D. (2021) Fog Computing Enabled Healthcare 4.0. In: Singh P.K., Singh Y., Kolekar M.H., Kar A.K., Chhabra J.K., Sen A. (eds) Recent Innovations in Computing. ICRIC 2020. Lecture Notes in Electrical Engineering, vol 701. Springer, Singapore. https://doi.org/10.1007/978-981-15-8297-4_42.
2. Chanchaichujit J., Tan A., Meng F., Eaimkhong S. (2019) An Introduction to Healthcare 4.0. In: Healthcare 4.0. Palgrave Pivot, Singapore. https://doi.org/10.1007/978-981-13-8114-0_1.
3. Chen, C., Loh, EW., Kuo, K.N. et al. The Times they Are a-Changin' – Healthcare 4.0 Is Coming!. J Med Syst 44, 40 (2020). https://doi.org/10.1007/s10916-019-1513-0
4. Mahajan, H.B., Badarla, A. & Junnarkar, A.A. (2020). CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02502-0.
5. Mahajan, H.B., & Badarla, A. (2018). Application of Internet of Things for Smart Precision Farming: Solutions and Challenges. International Journal of Advanced Science and Technology, Vol. Dec. 2018, PP. 37-45.
6. Mahajan, H.B., & Badarla, A. (2019). Experimental Analysis of Recent Clustering Algorithms for Wireless Sensor Network: Application of IoT based Smart Precision Farming. Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 9. 10.5373/JARDCS/V11I9/20193162.
7. Mahajan, H.B., & Badarla, A. (2020). Detecting HTTP Vulnerabilities in IoT-based Precision Farming Connected with Cloud Environment using Artificial Intelligence. International Journal of Advanced Science and Technology, Vol. 29, No. 3, pp. 214 - 226.
8. Sundararaman, T., Muraleedharan, V.R. & Ranjan, A. Pandemic resilience and health systems preparedness: lessons from COVID-19 for the twenty-first century. *J. Soc. Econ. Dev*. (2021). https://doi.org/10.1007/s40847-020-00133-x.
9. Khalid, A., Ali, S. COVID-19 and its Challenges for the Healthcare System in Pakistan. ABR 12, 551–564 (2020). https://doi.org/10.1007/s41649-020-00139-x.
10. Dy, L.F., Rabajante, J.F. A COVID-19 infection risk model for frontline health care workers. Netw Model Anal Health Inform Bioinforma 9, 57 (2020). https://doi.org/10.1007/s13721-020-00258-3.
11. Rathee P. (2020) Introduction to Blockchain and IoT. In: Kim S., Deka G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, Singapore. https://doi.org/10.1007/978-981-13-8775-3_1.
12. Yalla S.T., Nikhilendra P. (2020) An Overview on Blockchain Technology and Its Applications. In: Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, vol 601. Springer, Singapore. https://doi.org/10.1007/978-981-15-1420-3_113.
13. Li, Y. Emerging blockchain-based applications and techniques. *SOCA* **13,** 279–285 (2019). https://doi.org/10.1007/s11761-019-00281-x.
14. Cappiello B., Carullo G. (2021) Introduction: The Challenges and Opportunities of Blockchain Technologies. In: Cappiello B., Carullo G. (eds) Blockchain, Law and Governance. Springer, Cham. https://doi.org/10.1007/978-3-030-52722-8_1.
15. Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 8(2), 44. doi:10.3390/info8020044.
16. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access, 5, 14757–14767. doi:10.1109/access.2017.2730843.
17. Zhang, Y., Deng, R. H., Shu, J., Yang, K., & Zheng, D. (2018). TKSE: Trustworthy Keyword Search Over Encrypted Data With Two-Side Verifiability via Blockchain. IEEE Access, 6, 31077–31087. doi:10.1109/access.2018.2844400.
18. Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 43(1). doi:10.1007/s10916-018-1121-4.
19. Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Security and Communication Networks, 2019, 1–15. doi:10.1155/2019/8315614.
20. Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences, 9(6), 1207. doi:10.3390/app9061207.
21. Yang, Guang & Li, Chunlei & Marstein, Kjell. (2019). A blockchain-based architecture for securing electronic health record systems. Concurrency and Computation: Practice and Experience. 10.1002/cpe.5479.

22. Liu, Xiaoguang & Wang, Ziqing & Jin, Chunhua & Li, Fagen & Li, Gaoping. (2019). A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2937685.
23. Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-020-01710-y.
24. Rathee, Geetanjali & Sharma, Ashutosh & Saini, Hemraj & Kumar, Rajiv & Iqbal, Razi. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications. 79. 10.1007/s11042-019-07835-3.
25. Huang, L., & Lee, H. (2020). Decentralization and Security Issues in Blockchain Enabled Internet of Things. Wireless Communications and Mobile Computing. doi: 10.1155/2020/8859961.
26. Indumathi, J. & Shankar, Achyut & Ghalib, Dr. Muhammad & Jayaraman, Gitanjali & Hua, Qiaozhi & Wen, Zheng & Qi, Xin. (2020). Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U 6 HCS). IEEE Access. 8. 216856-216872. 10.1109/ACCESS.2020.3040240.
27. https://www.kaggle.com/allen-institute-for-ai/CORD-19-research-challenge.
28. https://www.kaggle.com/sudalairajkumar/novel-corona-virus-2019-dataset.