Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.027779
Article

Tech Science Press

Encryption with User Authentication Model for Internet of Medical Things Environment

K. S. Riya[1], R. Surendran[2,*], Carlos Andrés Tavera Romero[3] and M. Sadish Sendil[4]

[1]Department of Information Technology, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, 600062, India
[2]Center for Artificial Intelligence and Research (CAIR), Chennai Institute of Technology, Chennai, 600069, India
[3]COMBA R&D Laboratory, Faculty of Engineering, Universidad Santiago de Cali, Cali, 76001, Colombia
[4]Department of Emerging Technologies, Guru Nanak Institute of Technology, Ibrahipatnam, 501506, Telangana, India
*Corresponding Author: R. Surendran. Email: dr.surendran.cse@gmail.com
Received: 25 January 2022; Accepted: 28 February 2022

Abstract: Internet of Medical Things (IoMT) enabled e-healthcare has the potential to greately improve conventional healthcare services significantly. However, security and privacy become major issues of IoMT because of the restricted processing abilities, storage, and energy constraints of the sensors. Therefore, it leads to infeasibility of developing traditional cryptographic solutions to the IoMT sensors. In order to ensure security on sensitive medical data, effective encryption and authentication techniques need to be designed to assure security of the patients and healthcare service providers. In this view, this study designs an effective metaheuristic optimization based encryption with user authentication (EMOE-UA) technique for IoMT environment. This work proposes an EMOE-UA technique aims to accomplish mutual authentication for addressing the security issues and reducing the computational complexity. Moreover, the EMOE-UA technique employs optimal multikey homomorphic encryption (OMKHE) technique to encrypt the IoMT data. Furthermore, the improved social spider optimization algorithm (ISSOA) was employed for the optimal multikey generation of the MKHE technique. The experimental result analysis of the EMOE-UA technique takes place using benchmark data and the results are examined under various aspects. The simulation results reported the considerably better performance of the EMOE-UA technique over the existing techniques.

Keywords: User authentication; security; privacy; internet of medical things; homomorphic encryption; optimal key generation

1 Introduction

The Internet of Things (IoT) is a data transmission network that hosts a rising amount of objects and devices could exchange, collect, sense, and connect information amongst wide-ranging applications. The IoT method has been widely employed for improving the quality of life [1]. This domain includes industrial systems, transportation, marketing, healthcare application, smart homes, smart agriculture, smart education, and smart cities [2]. The research focused on the Internet of Health Things (IoHT), called as

Internet of Medical Things (IoMT) that is main application which affects human life and unaddressed security vulnerability might result in dangerous situations [3,4]. The IoMT improves the healthcare field and provides health care by permitting on-demand connection with hospitals and doctors, easing accessibility, and enhancing efficiency. Additionally, the IoMT decreases the time consumed in physical meet with physicians [5]. In the IoMT, patient needs some devices to be connected with hospitals, families, and physicians at the time of healthy quarantine including what has happened with the COVID19 pandemic that appears at the end of 2019 or any other pandemic crisis. This situation has forced researchers and scientists for increasing the effort using IoMT system. But, the wide-ranging deployment of IoMT system has made new security problems that extend the 3 layers of this system. The most significant security problems include device identity management module and the IoT device authentication that appears in the IoT perception layer [6,7].

The edge inherits cloud security attributes and challenges to new threats and vulnerabilities (for example, access control, secured data computation, privacy protection, secured data storage, and authentication [8]). The researchers concentrated on how to maintain the integrity of information transmitted by IoMT devices to the cloud using edge computing and simultaneously allowing the edge and the cloud devices to validate the origin and the integrity of the information [9]. Authentication is determined as the capacity to show you are who you say you are. With respect to data exchange in a transmission system, there is authentication when the transmitter of information could be unequivocally recognized by the receiver. Consecutively, there is integrity if it could be revealed that a message or data hasn't been deleted, created, or modified by unauthorized systems or users [10].

The purpose of this work is to develop an efficient metaheuristic optimization-based encryption with user authentication (EMOE-UA) technique for the Internet of Things (IoT). The EMOE-UA technique suggested here seeks to achieve mutual authentication in order to meet security concerns while reducing computing complexity. Additionally, the EMOE-UA approach encrypts the IoMT data using optimal multikey homomorphic encryption (OMKHE). Additionally, the improved social spider optimization algorithm (ISSOA) was used to optimise the MKHE technique's multikey generation. The EMOE-UA technique's performance is validated using benchmark data, and the results are analysed using a variety of metrics.

2 Literature Review

Guo et al. [11] introduced an effectual, outsourced online or offline revocable ciphertext policy ABE technique with utilize of cloud servers and blockchain from the IoMT ecosystem. It can be offered attains the features of fine-grained access controls, user revocation, fast encryption, ciphertext verification, and outsourced decryption. It can be notable that dependent upon chameleon hash function, it generates the private key of data users with collision resistances, semantically secures, and key-exposures free for achieving revocation. The authors in [12] examined an effective, strong authentication protocol, to the MP for accessing patient information to healthcare applications dependent upon Cloud-IoT network. The presented protocol contains: (i) 3-factor MP authentication (for instance, smartcard, password, and biometrics); (ii) mutual authentication amongst MP as well as cloud server; (iii) creates a secure shared session key; and (iv) maintain key freshness.

The authors in [13] presented a new remote users authentication technique for cloud-IoT applications. This technique was lightweight and robust for attacking and also is minimal computational overhead. The presented method fulfills the chosen vital elements of security. Sadhukhan et al. [14] presented the ECC based 3-factor remote user authentication method which runs from the smart devices and preserves privacy and data secrecy of interconnecting users. For supporting our claim, several cryptographic attacks were analyzed and revealed that the presented technique could not be vulnerable to individual's attack.

Sudhakaran [15] presented the Energy Efficient Distributed Lightweight Authentication and Encryption (EEDLAE) approach to IoT securities. During the presented approach, the receiver creates the token for all senders. The token finishing time was defined as dependent upon the trust value of all senders, and sleep period of receiver radio was defined as dependent upon their RE. In order to encryption, Counter with Cipher Block Chaining-Message Authentication Code (CCM) was executed. Jin et al. [16] presented RLWE based homomorphic encryption communication protocols to user authentications and message controlling from CC based IoT convergence environments. It can be demonstrated result analysis on communication protocol from the current IoT environments and the presented communication protocols to make sure security as well as safety. The authors in [17] presented the lightweight smartcard based secure authentication (LS-BSA) method utilizing the mathematical model of bilinear-pairing or mapping, ECC, and fuzzy verifier. An extensive security analysis illustrates that the presented LS-BSA not only securities the AKA property for preventing important vulnerability.

3 The Proposed Model

In this study, a new EMOE-UA technique has been developed to accomplish mutual authentication for addressing the security issues and reducing the computational complexity in the IoMT environment. The proposed EMOE-UA technique encompasses two major processes OMKHE based encryption and ISSOA based optimal key generation process. The ISSOA technique is derived by the use of LF concept. Fig. 1 depicts the block diagram of EMOE-UA technique.

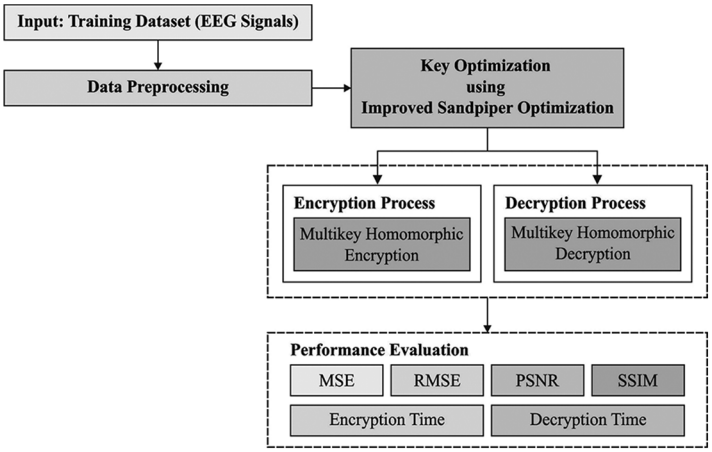

Figure 1: Block diagram of EMOE-UA technique

3.1 Process Involved in MKHE Technique

At the initial stage, the MKHE technique is used to encrypt the medical data. The semantically secured homomorphic public key encryption method is focal cryptographic device to some secured multi-party assessment problems. The property of homomorphic is extremely helpful to create a secure technique with superior security data retrieval approach. This encryption structure was utilized to implement task by encoding data with no knowledge of private keys (without decryption), namely, user is an initial holder of confidential key [18]. The homomorphic computation technique assumed the polynomial cipher image to be exact, encrypted from N keys, besides the comparing computation key, and deliver cipher image.

Several encryptions was the particular approach to change on special message for confused shape by executing encryption many times, if implementing the distinctive or similar processes. It could be

demonstrated as cascade ciphering, several encryptions, and cascade encryption. During the process of examination, decrypt and encrypt are applied to utilize several keys [19].

The projected MHE assumed three stages such as encryption or decryption approach, several key generations, and an optimum key determination. The key was utilized to encrypt or decrypt all information is being decrypted/encrypting. This technique is under the procedure of decoded and encoded keys and the correlated image with symmetric key; trust value security and confidentiality are offered. The comparative public key (pu_k) and private key (pr_k) in several keys are employed. The key equal was utilized by asymmetric key; now, several keys $K = \{K_1, \quad K_2, \ \ldots K_n\}$ are developed for MHE. In many samples, key is arbitrarily generated by Arbitrary Number Generator for selecting optimum keys in several keys, optimized technique is obtained as to account. The stimulation behind hand optimized is that it improves the privacy of key selective in the image decrypt and encrypt method.

Afterward, the optimal ciphered frame was selected as last encryption frame. In order to enhance the public as well as private keys from several key sets, ISSOA technique was utilized. Next, the transformative technique was utilized to increase the encryption procedure, however, it could be predicted. Eventually, the optimal ciphered content was selected as final encryption contents [20]. The homomorphic encryption presents encryption in that cipher and plain images were procedures with equal algebraic functions. Homomorphic encryption allows the server for implementing the performance on encrypted data without the knowledge of primary plain image. Utilizing confidential keys a customer encrypts a novel image and create pr_k and $pu_{k-optimal}$ and, besides the public key (pu_k), this cipher image is transferred to servers $pu_k = (k, \quad i)$ and $K = (p, \quad q)Enc(I, \quad pr_k)$ to pick arbitrary parameters $\ldots r \in Z_k^*$, Compute the cipher data $c = I.r^k \ \ mod k^2$. In recent times, an encryption technique was effective from the confidential image of novel images. During the encryption method, it can be suggested that for possess the lock inside for encoding every image pixels. During the decryption technique, an image which contains encrypting pixel is undertaken as (p, q) and Secret vector. The decryption procedure has 2 masks, particularly the confidential and Mask from a fixed progression. For decrypting the message bit (pixel regard) m in the cipher image and another confidential variable.

3.2 Optimal Key Generation Using ISSOA

For optimally tuning the key generation process of the MKHE technique, the ISSOA is applied to it. The presented approach is a metaheuristic method that simulates the social spider behavior to live together, searching for food and transferring the required data among them [21]. Generally, the population of social spiders is separated into females and males, in which the female represents 60%–90% of the overall spider number, and this group creates a web (searching domain) and searches for prey in this web.

The solution of the SSO is characterized by the location of spider in the web that translates the data about the position of each spider and the prey to each spider. This data is characterized as vibration that is generated at the movement of the spider from one location to another location in the web and is determined by [22]:

$$\mathrm{Vib}_{ij} = w_j e^{-d_{ij}^2}, \ d_{ij} = \|x_i - x_j\|, \quad w_j = \frac{F_j - \mathrm{worst}_x}{\mathrm{best}_x - \mathrm{worst}_x} \tag{1}$$

$$\mathrm{Best_x} = \max_{k=1,\ldots,N} F(x_k), \quad worst_x \ = \min_{k=1,\ldots,N} F(xk) \tag{2}$$

Whereas F_j, w_j and Vib_{ij} represents the fitness function value of spider j, the weight spider j and the vibration among the pairs i and, correspondingly. The spider location is upgraded according to its type (that is female and male). In the male group, the location of spider is upgraded depending on whether the male is a non-dominated or dominated spider. The dominated male updates the position for reaching the female, whereas the other kind of male is attracted towards the center location of the group to be a dominant

spider. This behavior can be shown here:

$$x_{m_i}^{k+1} = \begin{cases} x_{m_i}^{k} + \alpha \times Vibf_i \times (x_f - x_{m_i}^{k}) + \delta \times (\xi - .5), & w_{m_i} \geq ind_{med} \\ x_{m_i}^{k} + \alpha \left(\left(\sum_{j=1}^{Nm} x_{m_i}^{k}.wNf + j / \sum_{j=1}^{Nm} wNf + j \right) - x_{m_i}^{k} \right), & \text{otherwise} \end{cases} \tag{3}$$

Whereas xf, ind_{med}, k and Nm represent the nearby female to the i th male, the median of weight of each male spider, the amount of the existing iteration, and the amount of males, correspondingly. The non-dominated spider have weight lesser than ind_{med} [23], or else, dominant male. $Vi\ \ bf_i = w_f e^{-} d_{if}^2$ Characterizes the transferred vibrations among the existing female and nearby one.

There is alternative way, where the female spider is utilized for updating the position as follows:

$$x_f^{k_i+1} = \begin{cases} x_{f_i}^{\text{k}} + \beta_2 \times Vibc_i \times (x_c - x_{f_i}^{\text{k}}) + \beta_1 \times Vibb_i \ \ \times (x_b - x_f^{k_i}) + \beta_3 \times (\beta_4 - .5),\ \beta_5 \geq p_m \\ x_{f_i}^{k} - \beta_2 \times Vibc_i \times (x_c - x_{f_i}^{k}) - \beta_1 \times Vibb_i \times (xb - x_f^{k_i}) + \beta_3 \times (\beta_4 - .5) \text{otherwise} \end{cases} \tag{4}$$

Whereas x_c, xb and $\beta_i \in [0,\ \ 1](i = \ \ 1,\ 2,\ \ \ldots,\ \ 5)$ represents the nearby spider to ith female that has the highest weight, the optimal spider and arbitrary number, correspondingly. The spider is moved to or away from the source of vibration according to the values of $p_m \in [0,\ 1]$. The Vi bb_i and Vi bc_i signify the vibration transferred by xb, and x_c:

$$Vibb_i = wbe^{-d_{ib}^2},\ w_b = \max_{k=1,\ldots,N} w_k \tag{5}$$

$$Vibc_i = w_c e^{-d_{ic}^2},\ w_c > w_i \tag{6}$$

The dominant females and males in the social spider population might be mating when they are laying in the neighbourhood that can be determined on the basis of radius r_{m} (named mating radius):

$$r_{\text{m}} = \frac{\sum_{j=1}^{n} (x_j^{\text{high}} - x_j^{\text{low}})}{2n} \tag{7}$$

But, if current female is with several males and in this neighbor, the roulette wheel model is utilized for choosing the parent to create new offspring; next, this offspring replaces the parent that has the worst fitness function. Fig. 2 illustrates the flowchart of SSOA.

In order to enhance the performance of the SSOA, the ISSOA is derived by integrating the concepts of Levy flight (LF). It is a type of natural and artificial phenomenon, as defined by Levy statistics. It is a common kind of stochastic non Gaussian walk where the step length value can be distributed based on Levy stable distribution [24,25]. It can be represented using Eq. (8):

$$Levy(\beta) \ \ \sim u = t^{-1-\beta},\ \ \ 0 < \beta \leq 2 \tag{8}$$

Here, β signifies substantial Levy index to adjust stability. The Levy random number can be determined as follows.

$$Levy(\beta) \sim \frac{\varphi \times \mu}{|\text{v}|^{1/\beta}} \tag{9}$$

where μ and v implies uniform distribution, Γ denotes Gamma function, $\beta = 1.5$, and φ can be represented as follows:

$$\varphi = \left[\frac{\Gamma(1+\beta) \times \sin\left(\pi \times \frac{\beta}{2}\right)}{\Gamma\left(\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\frac{\beta-1}{2}}\right)} \right]^{\frac{1}{\beta}} \tag{10}$$

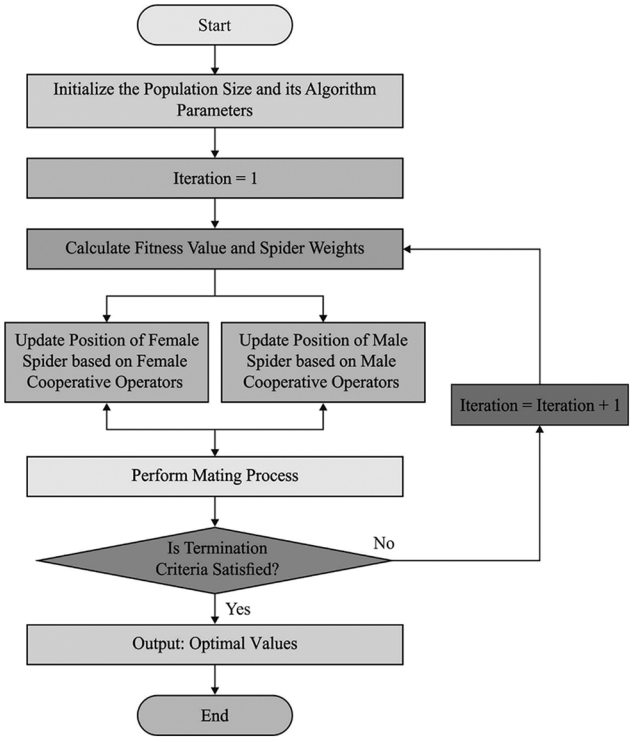

Figure 2: Flowchart of SSOA

To attain an effective tradeoff among the exploitation and exploration capabilities of SSOA, LF method can be employed to update the position of the searching agent, as provided below.

$$X_i^{levy} = X_i + r \oplus levy(\beta) \tag{11}$$

where X_i^{levy} means newly attained position of ith searching agent X_i after updating, r represents arbitrary vector in [0, 1], and $\oplus$ specifies dot product.

The ISSOA based several key optimized techniques assume Fitness Function (FF) of Peak Signal to Noise Ratio (PSNR) with regenerated image quality. This technique was suitable for amplifying several non-linear and linear issues. The dimension of debased image matrix and dimensional of correct image matrix was indistinguishable. The projected key optimized technique assumed as PSNR is defined under the subsequent:

$$F_i = \text{Max}(PSNR) \tag{12}$$

4 Performance Validation

In this section, a comprehensive experimental study of the EMOE-UA technique takes place under ten EEG signals. Tab. 1 provides an overall result analysis of the EMOE-UA technique in terms of different measures on ten Electroencephalography (EEG) signals. Fig. 3 demonstrates the Mean Square Error (MSE) investigation of the EMOE-UA technique under ten distinct EEG signals [24–28]. The results indicated that the EMOE-UA technique has resulted in least values of MSE under all EEG signals. For instance, with signal 1, the EMOE-UA technique has reached to MSE of 1707. Similarly, with signal 2, the EMOE-UA technique has attained MSE of 1891. Likewise, with signal 3, the EMOE-UA technique has obtained MSE of 1776. Moreover, with signal 4, the EMOE-UA technique has accomplished MSE of 1806. Furthermore, with signal 5, the EMOE-UA technique has attained MSE of 1884.

Table 1: Overall encryption results of EMOE-UA technique

EEG signals	MSE	PSNR (dB)	SSIM	PDR (100% noise)
Signal 1	1707	15.708	0.115	1758.000
Signal 2	1891	15.230	0.116	1775.000
Signal 3	1776	15.639	0.112	1799.800
Signal 4	1806	15.480	0.127	1804.700
Signal 5	1884	15.405	0.119	1726.900
Signal 6	1752	15.535	0.125	1771.600
Signal 7	1942	15.378	0.118	1740.800
Signal 8	1826	15.622	0.120	1762.500
Signal 9	1783	15.511	0.128	1740.400
Signal 10	1809	15.593	0.126	1823.800
Average	1818	15.510	0.121	1770.350

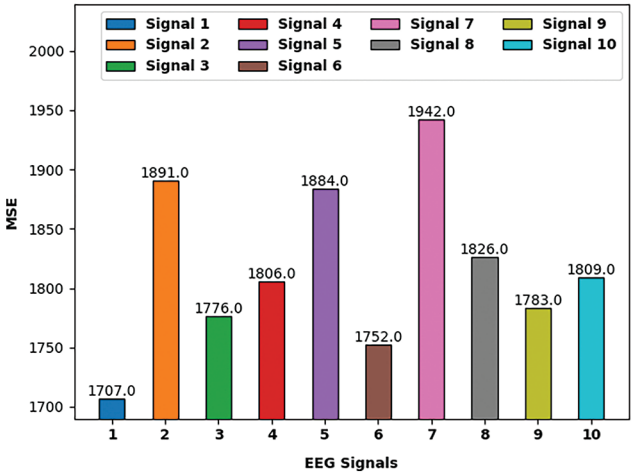

Figure 3: MSE analysis of EMOE-UA model on ten EEG signals

Fig. 4 validates the PSNR investigation of the EMOE-UA technique under ten different EEG signals. The figure specified that the EMOE-UA technique has led to maximum values of PSNR under all EEG signals. For instance, with signal 1, the EMOE-UA technique has gotten PSNR of 15.708 dB. Concurrently, with signal 2, the EMOE-UA technique has reached PSNR of 15.230 dB. Simultaneously, with signal 3, the EMOE-UA technique has gained PSNR of 15.639 dB. Also, with signal 4, the EMOE-UA technique has accomplished PSNR of 15.480 dB. At the same time, with signal 5, the EMOE-UA technique has attained PSNR of 15.405 dB.

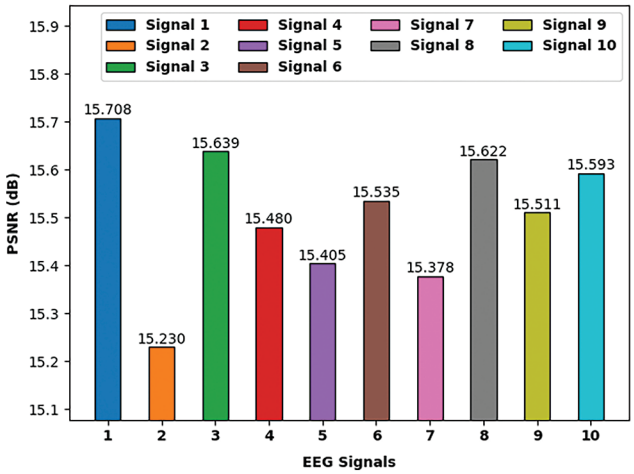

Figure 4: PSNR analysis of EMOE-UA model on ten EEG signals

Fig. 5 reveals the SSIM study of the EMOE-UA technique under ten dissimilar EEG signals. The results directed that the EMOE-UA technique has accomplished lower values of SSIM under all EEG signals. For instance, with signal 1, the EMOE-UA technique has reported SSIM of 0.115. Meanwhile, with signal 2, the EMOE-UA technique has achieved SSIM of 0.116. Eventually, with signal 3, the EMOE-UA technique has obtained SSIM of 0.112. Moreover, with signal 4, the EMOE-UA technique has accomplished SSIM of 0.127. Lastly, with signal 5, the EMOE-UA technique has reached to SSIM of 0.119.

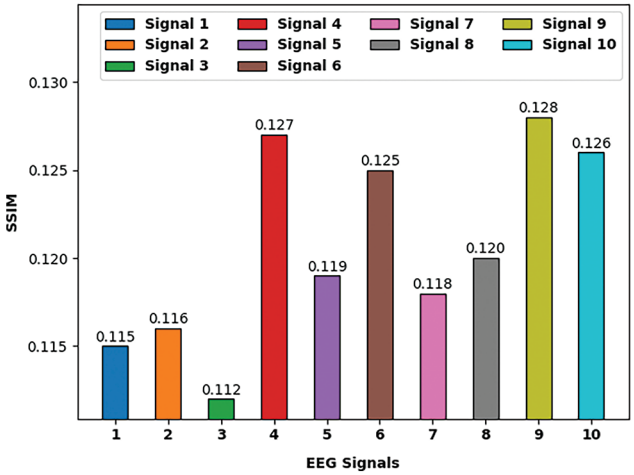

Figure 5: SSIM analysis of EMOE-UA model on ten EEG signals

Fig. 6 exhibits the PDR examination of the EMOE-UA technique under ten diverse EEG signals. The figure pointed out that the EMOE-UA technique has accomplished effective outcomes with minimal values of PDR under all EEG signals. For instance, with signal 1, the EMOE-UA technique has reached to PDR of 1758. Similarly, with signal 2, the EMOE-UA technique has attained PDR of 1775. Likewise, with signal 3, the EMOE-UA technique has obtained PDR of 1799. Moreover, with signal 4, the EMOE-UA technique has accomplished PDR of 1804. Furthermore, with signal 5, the EMOE-UA technique has attained PDR of 1726.

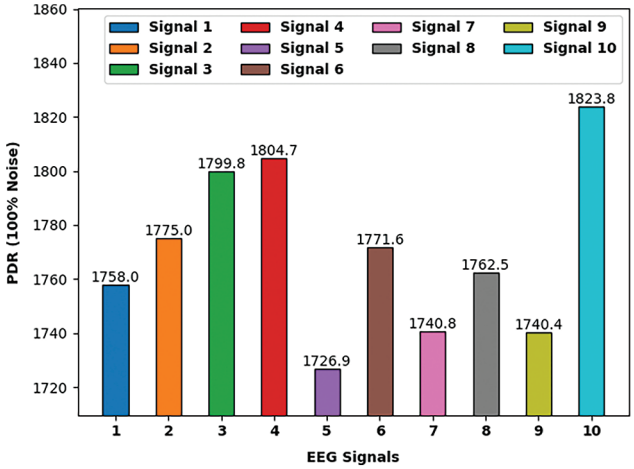

Figure 6: PDR analysis of EMOE-UA model on ten EEG signals

Tab. 2 and Fig. 7 demonstrate the ET and DT examination of the EMOE-UA technique under ten distinct EEG signals. The results indicated that the EMOE-UA technique has demonstrated superior results with the lower ET and DT. For instance, with EEG signal 1, the EMOE-UA technique has attained ET and DT of 0.114 and 0.103 s respectively.

Table 2: ET and DT analysis of EMOE-UA model

EEG signals	Encryption time (s)	Decryption time (s)
Signal 1	0.114	0.103
Signal 2	0.127	0.122
Signal 3	0.117	0.127
Signal 4	0.114	0.105
Signal 5	0.105	0.134
Signal 6	0.100	0.106
Signal 7	0.096	0.122
Signal 8	0.094	0.128
Signal 9	0.114	0.122
Signal 10	0.100	0.136
Average	0.108	0.121

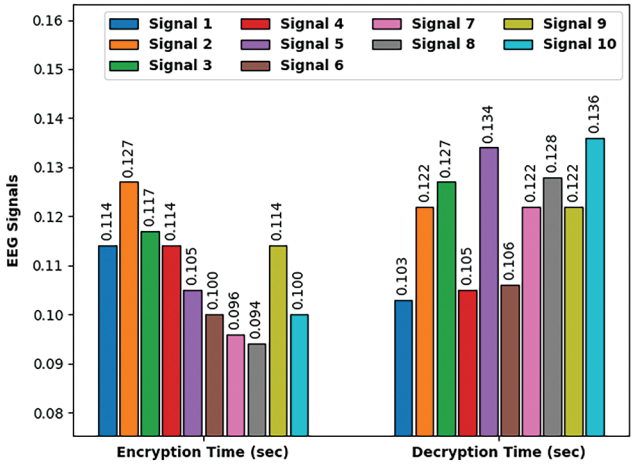

Figure 7: Encryption and decryption time analysis of EMOE-UA technique

In addition, with EEG signal 2, the EMOE-UA technique has reached ET and DT of 0.127 and 0.122 s respectively. Moreover, with EEG signal 3, the EMOE-UA technique has achieved ET and DT of 0.117 and 0.127 s respectively. Besides, with EEG signal 4, the EMOE-UA technique has accomplished ET and DT of 0.114 and 0.105 s respectively. Along with that, with EEG signal 5, the EMOE-UA technique has got ET and DT of 0.105 and 0.134 s respectively. In addition, with EEG signal 6, the EMOE-UA technique has achieved ET and DT of 0.100 and 0.106 s respectively.

In order to exhibit the enhanced outcomes of the EMOE-UA technique, a comparison study is made interms of MSE, PSNR, SSIM, and PDR in Tab. 3 and Fig. 8. The results indicated that the EMOE-UA technique has accomplished superior outcomes with the lower values of PDR, MSE, and PSNR along with higher value of SSIM.

Table 3: Comparison study of EMOE-UA and existing techniques

Methods	MSE	PSNR (dB)	SSIM	PDR (100% noise)
DCLE	11011	7.713	0.045	3269.390
HLE–SO	10043	8.112	0.073	2130.900
EMOE-UA	1818	15.510	0.121	1770.350

The results represented that the DCLE technique has led to ineffectual results with MSE of 11011, PSNR of 7.713 dB, SSIM of 0.045, and PDR of 3269.390. In addition, the HLE-SO technique has gained somewhat improved outcomes with MSE of 10043, PSNR of 8.112 dB, SSIM of 0.073, and PDR of 2130.900. However, the EMOE-UA technique has outperformed the other methods with the MSE of 1818, PSNR of 15.510 dB, SSIM of 0.121, and PDR of 1770.350.

Finally, a brief encryption time (ET) and decryption time (DT) assessment of the EMOE-UA technique with recent methods take place in Tab. 4 and Fig. 9 [26,27]. The results depicted that the DCLE technique has resulted in poor results with the larger ET and DT of 0.164 and 0.171 s respectively. In addition, the HLE-SO technique has achieved slightly enhanced performance with the ET and DT values of 0.137 and 0.140 s respectively.

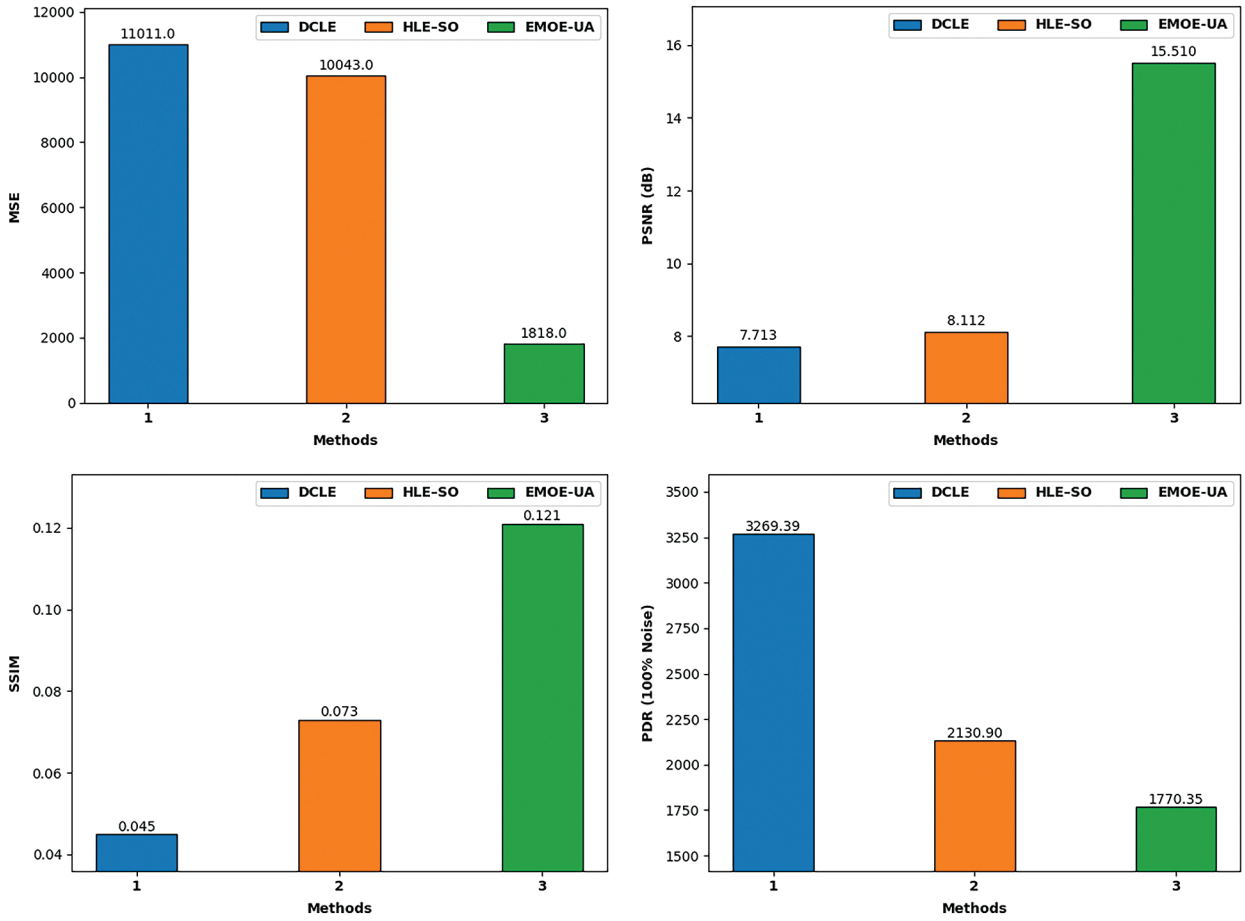

Figure 8: Comparative encryption results of EMOE-UA technique

Table 4: Comparative results of EMOE-UA technique interms of ET and DT

Methods	Encryption time (s)	Decryption time (s)
DCLE	0.164	0.171
HLE–SO	0.137	0.140
EMOE-UA	0.108	0.121

However, the EMOE-UA technique has resulted in effectual outcomes with the ET and DT of 0.108 and 0.121 s respectively. From the above mentioned results, it is confirmed that the EMOE-UA technique has resulted in maximum performance over the other methods [29–31].

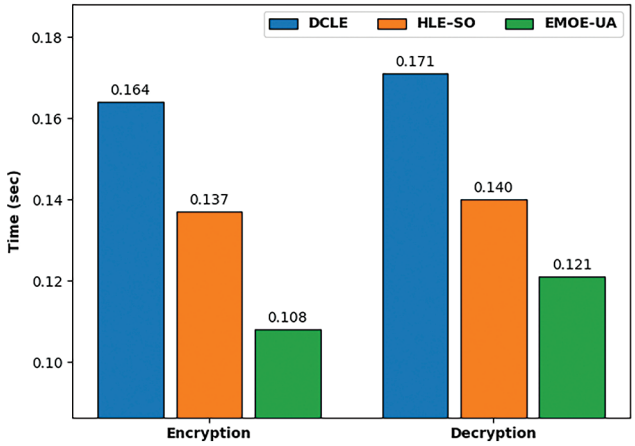

Figure 9: ET and DT analysis of EMOE-UA technique with recent methods

5 Conclusion

In this study, a new EMOE-UA technique has been developed to accomplish mutual authentication for addressing the security issues and reducing the computational complexity in the IoMT environment. The proposed EMOE-UA technique encompasses two major processes OMKHE based encryption and ISSOA based optimal key generation process. The ISSOA technique is derived by the use of LF concept. The performance validation of the EMOE-UA technique is performed on benchmark data and the results are inspected interms of different measures. The simulation results reported the considerably better performance of the EMOE-UA technique over the existing techniques. Thus, the EMOE-UA technique can be utilized as an effective tool for enhancing security in the IoMT environment. In future, the encryption performance can be improved by the design of hybrid metaheuristics algorithm.

Acknowledgement: The authors would like to thank Vel Tech Multi Tech Dr. Rangarajan Dr.Sakunthala Engineering College, Chennai Institute of Technology and Guru Nanak Institute of Technology for providing us with various resources and unconditional support for carrying out this study

Funding Statement: This research has been funded by Dirección General de Investigaciones of Universidad Santiago de Cali under call No. 01-2021.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues *et al.,* "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[2] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop *et al.,* "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, vol. 12, pp. 4049–4063, 2020.

[3] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou and C. Douligeris, "A Blockchain-enabled architecture for IoMT device authentication," in *Proc. 2020 IEEE Eurasia Conf. on IOT, Communication and Engineering (ECICE)*, IEEE, Yunlin, Taiwan, pp. 89–92, 2020.

[4] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. K. Al-Ali *et al.,* "Recent advances in the internet of medical things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2020.

[5] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and ipfs technology," *The Journal of Supercomputing*, vol. First Online, pp. 1–40, 2021.

[6] S. Razdan and S. Sharma, "Internet of medical things (IoMT): Overview, emerging technologies, and case studies," *IETE Technical Review*, Online First, pp. 1–14, 2021.

[7] M. A. Jan, M. Usman, X. He and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1576–1583, 2018.

[8] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh *et al.,* "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *Journal of Network and Computer Applications*, vol. 174, pp. 102886–102895, 2021.

[9] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop *et al.,* "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, Special Issue, pp. 4049–4067, 2020.

[10] R. Surendran and T. Tamilvizhi, "Cloud of medical things (CoMT) based smart healthcare framework for resource allocation," in *Proc. 3rd Smart Cities Symposium (SCS 2020)*, IET, Online Conference, Sakhir–Kingdom of Bahrain, pp. 29–34, 2020.

[11] R. Guo, G. Yang, H. Shi, Y. Zhang and D. Zheng, "O 3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8949–8963, 2021.

[12] P. K. Dhillon and S. Kalra, "Multi-factor user authentication scheme for IoT-based healthcare services," *Journal of Reliable Intelligent Environments*, vol. 4, no. 3, pp. 141–160. 2018.

[13] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *Journal of Information Security and Applications*, vol. 42, pp. 95–106, 2018.

[14] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114–1151, 2021.

[15] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *International Journal of Communication Systems*, vol. 35, no. 2, pp. e4198, 2022.

[16] B. W. Jin, J. O. Park and H. J. Mun, "A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment," *Wireless Personal Communications*, vol. 105, no. 2, pp. 599–618, 2019.

[17] B. D. Deebak and A. T. Fadi, "Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing," *Future Generation Computer Systems*, vol. 116, pp. 406–425, 2021.

[18] R. Surendran, R. Karthika and B. Jayalakshmi, "Implementation of dynamic scanner to protect the documents from ransomware using machine learning algorithms," in *Proc. 2021 Int. Conf. on Computing, Electronics & Communications Engineering (iCCECE)*, Southend, United Kingdom, IEEE, pp. 65–70, 2021.

[19] C. Hao, D. Wei, K. Miran and S. Yongsoo, "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference," in *Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security*, London, United Kingdom, pp. 395–412, 2019.

[20] H. C. Jung, K. Andrey, K. Miran and S. Yongsoo, "Homomorphic encryption for arithmetic of approximate numbers," in *Int. Conf. on the Theory and Application of Cryptology and Information Security*, Hong Kong, China, Springer, pp. 409–437, 2017.

[21] R. V. Raghupathy, O. I. Khalaf, C. A. Tavera Romero, S. Sengan and D. K. Sharma, "Interactive middleware services for heterogeneous systems," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1241–1253, 2022.

[22] E. Cuevas, M. Cienfuegos, D. Zaldívar and M. Pérez-Cisneros, "A swarm optimization algorithm inspired in the behavior of the social-spider," *Expert Systems with Applications*, vol. 40, no. 16, pp. 6374–6384, 2013.

[23] R. Surendran, O. I. Khalaf and C. A. Tavera Romero, "Deep learning based intelligent industrial fault diagnosis model," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 6323–6338, 2022.

[24] T. T. Nguyen, "A high performance social spider optimization algorithm for optimal power flow solution with single objective optimization," *Energy*, vol. 171, pp. 218–240, 2019.

[25] M. Rajalakshmi, V. Saravanan, V. Arunprasad, C. A. Tavera Romero, O. I. Khalaf *et al.,* "Machine learning for modeling and control of industrial clarifier process," *Intelligent Automation & Soft Computing*, vol. 32, no. 1, pp. 339–359, 2022.

[26] K. Tamilarasi and A. Jawahar, "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm," *Wireless Personal Communications*, vol. 114, no. 3, pp. 1865–1886, 2020.

[27] S. Rajendran, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, "Mapreduce-based big data classification model using feature subset selection and hyperparameter tuned deep belief network," *Scientific Reports*, vol. 11, no. 24138, pp. 1–18, 2021.

[28] S. Gill, T. Singh, B. Kaur, G. S. Gaba, M. Masud *et al.,* "A metaheuristic approach to secure multimedia big data for IoT-based smart city applications," *Wireless Communications and Mobile Computing*, vol. 2021, no. 7147940, pp. 1–10, 2021.

[29] I. S. Farahat, A. S. Tolba, M. Elhoseny and W. Eladrosy, "A secure real-time internet of medical smart things (IOMST)," *Computers & Electrical Engineering*, vol. 72, pp. 455–467, 2018.

[30] Y. K. Saheed and M. O. Arowolo, "Efficient cyber-attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021.

[31] A. Verma, G. Agarwal, A. K. Gupta and M. Sain, "Novel hybrid intelligent secure cloud internet of things based disease prediction and diagnosis," *Electronics*, vol. 10, no. 3013, pp. 1–25, 2021.