
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org

Volume 25, Issues 6, pp. 5240–5249, DOI 10.12694/scpe.v25i6.3315

IMPLEMENTING A SECURE CLOUD-BASED SYSTEM TO SAFEGUARD SENSITIVE MEDICAL DATA FOR HEALTHCARE

NOOR ABDUL KHALEQ ZGHAIR *, AMEER MOSA AL-SADI †, AND ALI ABDUL RAZZAQ TARESH ‡

Abstract. In most developed countries, the medical healthcare system is experiencing rapid development from the stage of clinical information to the stage of information dissemination. In all of these countries, it is undeniable that the Internet of Medical Things (IoMT) technologies have contributed in order to develop information medical healthcare. In reality, the development of smart medical healthcare has been hindered by the protection of medical privacy, according to research and acceptance. This is especially true as telecommunications systems continue to expand and wireless sensor networks (WSN) develop, as well as ways to penetrate those checks that have become increasingly difficult. In the smart healthcare system, protecting users' information remains an outstanding issue. IoMT features and the protection of privacy and security have led to the development of an extended privacy homomorphism algorithm based on scrambling matrixes, an encryption algorithm enhanced by Modified RSA (mRSA), and a method of encrypted data compression that ensures data confidentiality. For the above purpose, we built a prototype system on a demo temporary domain using both hardware and software. According to the results, the proposed scheme protects E-healthcare from potential threats by providing stakeholders with a secure interface and preventing unauthorized users from accessing the mCloud, thus ensuring privacy. E-healthcare services based on cloud technology are protected by the proposed scheme because it is simple and robust.

Key words: Internet of Medical Things (IoMT); Modified RSA (mRSA); Discrete Wavelet Transform (DWT); Wireless Sensor Networks (WSN); Bit Error Ratio (BErR).

1. Introduction. Medical IoT technology has allowed privacy protection systems for medical data to be developed, including active surveillance, medical restrictions, smart healthcare, smart homes, and location-based services [1, 2]. A number of issues have arisen in sensing and obtaining medical data, such as how private and public information is collected, who asks for it, and who is responsible for overseeing or storing the data when that private data is leaked [3] Similarly, the rapid growth of populations in developed countries poses a number of challenges, including monitoring patients with chronic diseases, daily treatments, health care and rehabilitation, as well as medical restrictions imposed by the population and the methods of preserving and scheduling them, both of which form the basis of any society's health care system [4, 5]. In addition to keeping the privacy of elderly patients as much as possible, how to obtain their real-time physical information remains an unresolved issue. As a result, algorithms such as the K-Means clustering method and morphological operations such as erosion, dilation, and so on are used With the emergence of the IoT and traditional health care systems, this paper explores a privacy-protecting medical health care system based on IoM, ideally suited to the special demands of social aging management and care in developed countries [6]. The leading causes of mortality around the globe. It is critical to be able to identify the type of tumour as well as forecast patient clinical results. Lung cancer sufferers have a lower standard of living than the general population and patients with other cancers. If lung cancer is detected early, at least 50% of patients will still be alive 5 years later, free of recurrence.

Below is an organization of the rest of the paper. The literature related works are highlighted in the 2nd Section was organized. The 3rd Section describes the System Methodology. A detailed description about personal information protection is provided in the 4^{th} Section. Analyzing the security of mRSA cryptosystems was given in the 5^{th} Section. In the 6^{th} Section, a system model implementation was explained.

*Computer engineering department, University of technology, Baghdad, Iraq (Noor.A.Zghair@uotechnology.edu.iq),
†Computer engineering department, University of technology, Baghdad, Iraq (Ameer.M.AlSadi@uotechnology.edu.iq)
‡Computer engineering department, University of technology, Baghdad, Iraq (Ali.A.Taresh@uotechnology.edu.iq)

2. Literature Related Works. A review of some works on secure medical data sharing is presented in this section.

2.1. Data Sharing in a Secure Environment. Private cloud architectures are typically utilized in medical organizations to deploy IT infrastructure, which provides a trusted authority for secure medical data sharing [7]. The problem with this paradigm is that it requires a high level of computing and storage investment and is limited in terms of scaling. Collaboration outside the perimeter of the domain can be inconvenient for collaborators [8]. Data sharing that is flexible and fine-grained, however, is inefficient when using one-to-one encryption in a public environment. Multiple ciphertexts are generated in this case in order to encrypt medical data for each user, resulting in enormous computation and storage overheads.

As a control mechanism for outsourced medical data, Sahai and Waters [9] proposed attribute-based encryption. Users can specify access policies that determine what data they are allowed to read when utilizing key-policy attribute-based encryption (KP-ABE) [10]. According to the user's access policy, ciphertext can be decrypted using the key associated with it. Several studies have used attribute-based encryption primitives to address practical issues in secure medical data sharing [11], including multi authority [12], light-weighting [13], and anonymization [14]. In [15] presented a scalable Internet of Things device for heart disease diagnostics. The detected data from the Internet of Things device was processed using the logistic regression approach. The vast volume of data acquired from patients was stored and retrieved via cloud services. ROC analysis was used to assess the efficiency of the regression models in predicting heart disease, The issue of updating user privileges (revocation or extension) is also a popular research topic since it pertains to data sharing. It is still challenging to change user access rights without affecting others because attribute-based encryption attributes are shared.

2.2. The Revocation Process in Attribute-Based Encryption . Bethencourt et al. [15], explained revocation in their ciphertext-policy attribute based encryption scheme, in which each attribute is defined to expire after a certain period of time. The solution proposed by Piretti et al. [16], was improved by a single expiration time associated with each secret key. In these schemes, users are required to update their keys frequently, so revocation cannot be done in a timely manner. Rather than periodic revocation, Attrapadung et al. [17], proposed revocable attribute-based encryption that supported direct user revocation.

Secret keys are associated with attributes as well as identities in their scheme. An integrated revocation list protects the ciphertext encrypted under its attributes so that even users with credentials matching those in the list cannot decrypt it. In a paper published by Liang et al. [18], CP-attribute-based encryption-R schemes were proposed. During revocation, it uses binary tree and linear secret-sharing techniques to reduce communication and computation costs. Direct revocation, however, is limited by the predefined revocation list [19, 20, 21]. Revocation schemes that use indirect revocation [22, 23] propose updating the secret keys when revocation occurs to address this issue. A new encryption should be applied to the old ciphertext, so that revoked users are unable to read it. As a result, the data owner is burdened with a great deal of computation and communication costs. Yu et al. [24] introduced an honest proxy server into their revocable attribute-based encryption scheme, with the proxy server performing the bulk of the ciphertext and key update operations, allowing the authority to revoke any attribute of any user. Utilizing the second scheme [25], users' secret keys are outsourced to the cloud server, and an essential dummy attribute is added to ciphertexts and secret keys. Users' privacy is not compromised by the semi-honest cloud server updating ciphertext and secret keys. Encryption/decryption rely on the dummy attribute, so redundant computations and communications are necessary.

The majority of revocable schemes are concerned with the revocation of the identity of the user rather than the attributes of the user, so a user who is revoked cannot utilize any of his attributes. It is possible to decrypt ciphertext with an unrevoked user's secret key when only a portion of their attributes have been revoked, therefore the ciphertext can still be decrypted utilizing their secret key. Assigning users two access trees in KP-attribute-based encryption addresses the problem of single attribute revocation by utilizing two concrete constructions of attribute revocation. There can, however, only be one revoked attribute determined per encryption. CP-associate-based encryptions were implemented by Cui et al [27] using key separation and binary tree data structures to support selective revocation of attributes, and an untrusted server was introduced to reduce the workload of users during key updates. They do, however, realize attribute-level revocation only through a periodic key update phase, but not in a timely fashion.

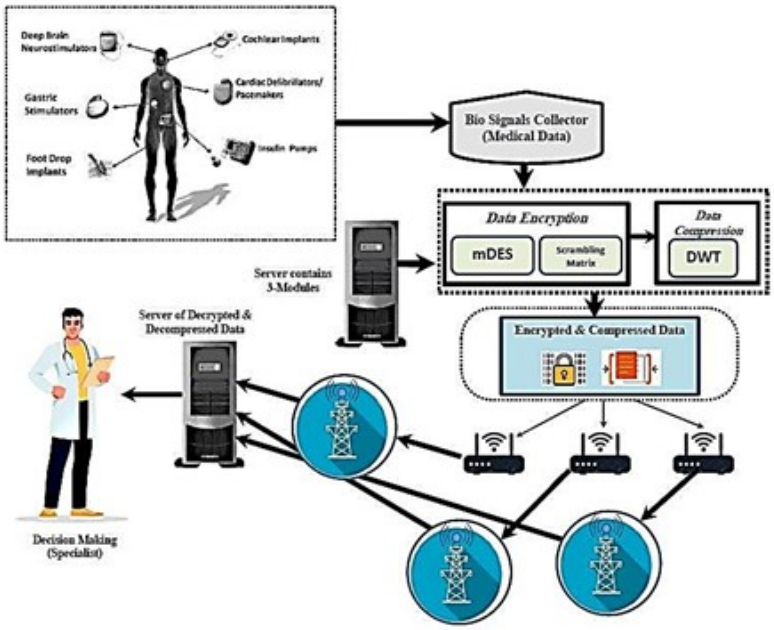

Fig. 3.1: Overall System Methodology

3. System Methodology. The wearable medical sensor nodes we deploy in nursing homes and communities for our intelligent medical applications provide benefits to the elderly. A network of gateway nodes will convert ZigBee signals to TCP/IP simultaneously in the community, and data will be transmitted to hospitals nearby via routers via distributed WSN. Hospitals can analyze and process feedback results from the web application, which allows users to measure physiological items (ECG, EEG, EOG, etc.). A diagram of the network topology can be found in Fig. 3.1. It is easy for attackers to intercept, modify, or alter physiological data transmitted online, such as eavesdropping, forgeries, etc. To protect and ensure the privacy and security of data sent between the source and recipient, three units are proposed:

Module 1: Data is disabled before a server session by creating a confusion matrix.

Module 2: Encryption is utilized for data transmission through WSN.

Module 3: Encrypt medical data sent so that it cannot be hacked, manipulated, or altered. The attacker cannot translate the compressed and incomprehensible plain text into clear text even if he obtains the encrypted data. As a result of the proposed algorithm, the feedback data from the server is guaranteed to be valid without requiring the algorithm to be realized or verified.

3.1. Algorithm of an Extended Privacy Homomorphism. The privacy homomorphism of Rivest in 1978 is a way to manipulate encrypted data directly. The main idea of the book can be summarized as follows.

Considering K_1 and K_2 as encryption and decryption keys respectively, E_{k1} and D_{k2} stand for encrypted and decrypted functions, and α and β are operations [28].

$$\alpha(E_{k1}(M_1), \alpha(E_{k1}(M_2), ..., \alpha(E_{k1}(M_n)) \textit{ equal to } E_{k1}(\beta(M_1, M_2, ..., M_n))$$

and

$$D_{k2}(\alpha(E_{k1}(M_1), E_{k1}(M_2), ..., E_{k1}(M_n)) \textit{ equal to } \beta(M_1, M_2, ..., M_n))$$

Hence, the algebraic system $(E_k, D_k, \alpha, \beta)$ satisfies the privacy homomorphism.

On integers, privacy homomorphism produces the best results with only two operations: addition and subtraction. Additionally, privacy homomorphism must be extended from integer to real number, and its operations must be expanded from addition to subtraction, multiplication, and division [29] [21].

In the first place, fmod stands for real mode operation:

$$fmod(r,i)\ equal\ to\ \begin{Bmatrix} mod(r,i), & if\ i \geq 0 \\ -mod(|r|,i), & if\ i \leq 0 \end{Bmatrix} \tag{3.1}$$

Function $fmod$'s first parameter r is a real number, while its second parameter i is an integer, and its mod is a normal mathematical mod function. The math.h head file must contain the $fmod$ function in $C++$ because it is utilized in real applications [21, 22].

3.2. Addition of Encrypted Real Numbers with Privacy Homomorphism. Homomorphism encryption need only discuss the addition operation since subtraction can be shown by addition. Following is the design of the detail encrypted algorithm:

Let a prime number p is equal to a prime number q meaning that n is the product of p and q, we get the plaintext space.

$Z_p\ equal\ to\ \{x|\ |x| \leq p_{max}\}$ is the set of the plaintext.

$O_p\ equal\ to\ \{+p, -p, xp, *p, /p\}$ is the operation set of the plain text, and system of algebra $(Z_p, plusp, minusp, *p, /p)$ is creates the plaintext space [25].

Likewise, $Z_c\ equal\ to\ \{x|\ |x| < c_{max}\}$ is the set of the ciphertext, the set of the operation of the ciphertext homomorphic.

$O_c\ equal\ to\ \{+c, -c, xc, /c\}$, and a system of algebra $(Z_c, plusc.minusc, xc, /c)$ contains the space of the ciphertext.

Develop the function of the homomorphic encryption $\forall x \in Z_p$, is the value of its encryption $y\ equal\ to\ E_{(x)}$ is computed by the below formula:

$$\begin{aligned} &y\ equal\ to\ E(x)\ equal\ to\ fmod \\ &\qquad ((x\ multiply\ sign(x)\ multiply\ rand()\ multiply\ p), n) \\ &\qquad srand((unsigned)time\ NULL)); \end{aligned} \tag{3.2}$$

A signed subsection is represented by sign in the formula above.

$$sign(x) = \begin{Bmatrix} One....., & if\ x\ Greator\ than\ Zero \\ Zero...., & if\ x\ Equal\ to\ Zero \\ MinusOne...., & if\ x\ Less\ Than\ Zero) \end{Bmatrix} \tag{3.3}$$

$E(x)$ proves to be a monotonic, odd, and double-reflective homomorphic encrypted function. In addition to linear transformations and similar compounds, homomorphic functions can also be defined by linear transformations [24].

Generate Ciphertexts The Ciphertexts is generated by applying two steps. Beginning by converting the plaintexts into integers, and then adding the two real numbers x_1 and x_2. The mathematical representation of the above steps is shown below:

$y_1\ equal\ to\ E(x_1), y_2\ equal\ to\ E(x_2)$ by applying formula 3.2 [29].

Condition Checking If $|x_1|\ minus\ p\{x_2| \geq 0$ | then it should ensure the $|y_1|\ minus\ c|y2| \geq 0$ true, else, continue encrypting any real number until the condition is met by reversing the last step [26].

Sum Calculation Directly compute $y\ equal\ to\ y_1\ plus\ c\ multiply\ y_2$, and automatically the result is also encrypted. In reverse, the algorithm of decrypted is easy: $x\ equal\ to\ D(y)\ equal\ to\ fmod(y, p)$.

3.3. A Proposed Modified RSA (mRSA). A public key and a private key are both required in proposed mRSA cryptography because it makes use of asymmetric keys. A one-way system allows exclusive use of public/private keys for encryption/ decryption. As a result, cryptographic signing cannot be utilized for authentication. For the proposed mRSA cryptosystem, the following algorithm is utilized to generate keys [27, 18].

1. *Algorithm of Key Generation Phase*:

(a) Prime numbers are selected at random and independently p, q, r, and s should be made. All prime numbers should be equal in length.
(b) Calculate n *equal to* p *multiply* q, m *equal to* r *multiply* s,
ϕ *equal to* (p *minus* 1) *multiply* (q *minus* 1) and
λ *equal to* (r *minus* 1) *multiply* (s *minus* 1). Select e integer, when e greator than one and less than ϕ, $gcd(e, \phi)$ *equal to one*
(c) Calculate the exponent of the secret d, when d *greater than one* and less than $\phi, e\ x\ d\ mod\ \phi$ *equal to* 1.
(d) Choose g integer, wheng equal m *pluse one.*
(e) Calculate the inverse of the modular multiplicative: μ *equal to* λ^{-1} *mod* m.
(f) Key (encryption) for public utilize: (n, m, g, e).
(g) Key (decryption) for private utilize is (d, λ, μ) [9].

2. *Phase of Encryption*:
(a) Let m be a message to be encrypted where $mesg$ greator than $Zero$ and less than n.
(b) Choose a random r where r less then m.
(c) Calculate ciphertext as: c equal to $g^{(mesg^e mode\ n)}\ x\ r^m\ mod\ m^2$ [29].

3. *Phase of Decryption*:
(a) Calculate message:

$$m = ((\frac{c^\lambda\ mod\ m^2\ minus\ 1}{m})\ multiply\ \mu\ mod\ m)^d\ mod\ n \tag{3.4}$$

3.4. Discrete Wavelet Transform (DWT) for Data Compression. In order to overcome the weaknesses of Discrete Cosine Transform (DCT)-based techniques, DWT are utilized [21]. DWT is mostly related to 1D/2D DWT. In the first step, DWT can be implemented row-wise utilizing 1D-DWT). As a second option, 1D-DWT can provide four sub-bands such as Low Low (LL), Low High (LH), High Low (HL), and High High (HH) by applying it column-wise. There are four sub-bands within each of these four bands. A number of wavelet-based schemes have been proposed by researchers and are discussed below. Signal decomposition is studied with the DWT. Fast Fourier Transform (FFT) differs from this because it utilizes coefficients such as 'details' and 'approximation' [22]. A novel CAD method for early lung nodule detection. The volumetric variations in the detected lesion over time are used to calculate the growth rate of the identified lung nodule. Finding the threshold level that gives the best results requires a Graphical User Interface (GUI). Right now, the global threshold is being utilized instead of a threshold by level, which is the most accurate method. However, due to its complexity, the global threshold is being utilized for the time being. Signal types are chosen according to their complexity based on 1D data [23]. Hence, we will analyze which method works best with certain signals based on the criteria listed above. All the signals (length 1024) will be compared by the Mean Square Error (MSE), Root-Mean-Square Error (RMSE), and compression ratio. The complexity of 2D data will determine how many images are considered [24]. There is a fixed size (resolution) for all 2D data (image). Finally, real-life data (such as medical images) will be analyzed through a case study.

4. Personal Information Protection. Wireless sensor networks (WSNs) collect, aggregate and transport physical information. The purpose of this is to maintain data confidentiality and invisibility against hackers by utilizing privacy homeomorphisms and an mRSA-based lightweight encryption algorithm [25].

4.1. Algorithm Analysis. Compared to algorithms of a symmetric encryption RC5 and RC6, the proposed encryption algorithm is more efficient. The speed of the system is demonstrated through several experiments. The proposed algorithm, additionally RC6, and RC5, are utilized to encrypt 100 messages, and costs of their time are respectively [26]. The proposed algorithm is also resistant to a variety of attacks. Due to the ROL operation, linear and differential cryptanalysis are less effective than exhaustive attacks for our proposal. According to the proposed algorithm, RC5 and RC6 are no more secure than each other [27]. An exhaustive attack will be estimated in terms of computation costs. Cryptography algorithms RC5 and RC6 utilize 64-bit main keys. Hence, the key space consists of 264 elements. In practice, this is exaggerated, but

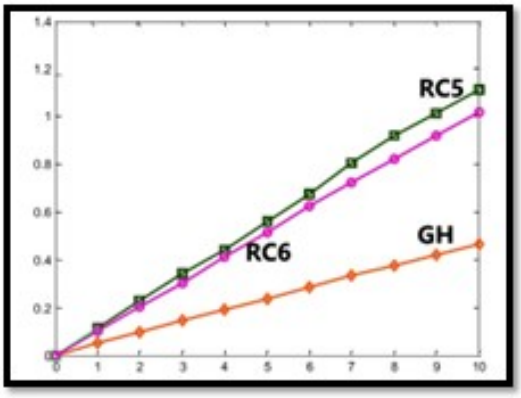

Fig. 4.1: Encryption Algorithm Comparisons

we can assume that the attackers' computer runs 109 instructions each minute. In other words, it will take 264/109/3600/365=14038 years to crack the plaintext of the message, exceeding the validity period of the data [23, 28].

5. A System Model Implementation. Nodes for medical sensors are deployed on multiple wearable devices for nursing home monitoring.

5.1. Medical Device Sensor Nodes. Sensors are used to collect patient information (ECG, EEG, pulse, blood oxygen levels, temperatures, etc.). Various types of medical sensors can be used for a variety of applications, as described below:
Temperature probes: Temperature measurement is performed using this device.
Force sensors: A kidney dialysis machine uses this material.
Airflow sensors: Laparoscopic systems, heat pumps, etc., operate on airflow.
Pressure sensors: Sleep apnea and infusion pumps use them. Embedded systems usually integrate pressure sensors.
Implantable pacemaker: Maintains proper cardiac rhythm with synchronized rhythmic electric pulses.
Oximeter: Measures the ratio of hemoglobin saturation to hemoglobin count.
Glucometer: Glucose concentration is approximated by this device.
Magnetometer: Determines the direction of the user by examining the earth's magnetic field.
Heart electrical activity: is measured by an electrocardiogram sensor. ECG sensors are used for ECGs.
Heart rate sensor: Minutely heartbeats are counted.
Electroencephalogram sensor: Measures brain activity.
Electromyogram sensor: Measures muscle electrical activity.
Respiration rate sensor: Measures the number of chest rises per minute.

5.2. Node for Gateways. The ZigBee signals are converted to TCP/IP at gateway nodes in the communication, and data is sent to nearby hospitals via routers [11].

5.3. A System Testing. Sensors such as blood oxygen sensors, pulse sensors with variable speed triggers, and temperature sensors are utilized to collect physiological data. Additionally, it ensures data transmission accuracy and reliability. Our sensor nodes were tested in a general environment in order to prove that they are capable of collecting accurate data. Temperature, oxygen saturation, and pulse are measured by sensor nodes. As a comparison, hospitals utilize standard instruments. The results of this study suggest that all sensors can be highly accurate. In order to get close to true value, we rely on a reliable data source.

Statistical analysis of the success rate and BErR of package transport is conducted in two more experiments. According to the proposed system's results, its success rate of transmissions (more than 0.899) and BErR (less than 0.049) are high. Communication with nodes and gateways ensures high reliability by conveying valid

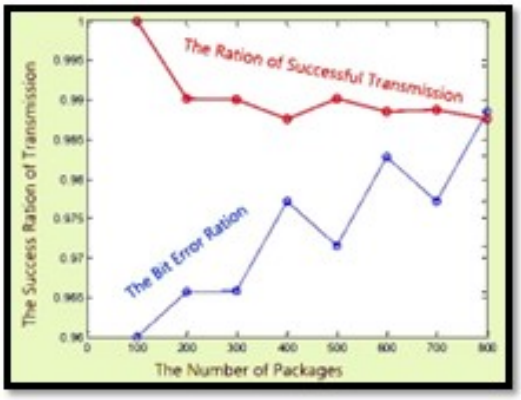

Fig. 5.1: BErR and Success Ration of Transmission Analysis

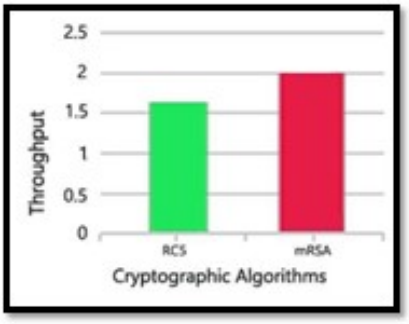

Fig. 5.2: Data Files Encryption Runtime

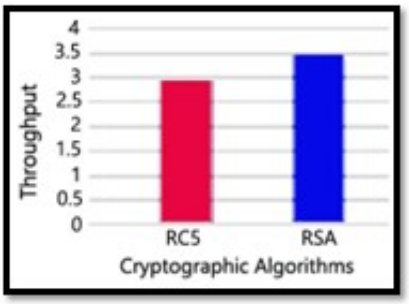

Fig. 5.3: Data Files Decryption Runtime

physiological data of patients. The sampled data were divided into sixty percent for training, twenty percent for validation, and twenty percent for testing, as shown in Figure 5.1.

By using our system interface, it is possible to compare both plaintext and ciphertext data. When an attacker eavesdrops on the information channel, he or she can only gain cipher information, unable to crack further due to the lack of a key. Obtaining the plaintext is possible if the attacker obtains the secret keys of decryption through accessing memory information. Homomorphic encryption prevents attackers from gaining any useful information about physiological data since they only obtain a confusing matrix.

Table 5.1: Encryption runtime of data files

File(MB)	RC5 (in sec)	RSA (in sec)
0.2	1.6	1.1
0.6	1.9	1.6
0.85	4.3	3.6
1.1	4.9	4.1
Average time	12.7	10.4
Throughput(MB/sec)	1.6	2

Table 5.2: Decryption runtime of data file

File(MB)	RC5 (in sec)	RSA (in sec)
0.2	1.6	1.1
0.6	2.1	1.6
0.85	2.6	2.1
1.1	3.6	3.1
Average time	9.9	7.9
Throughput(MB/sec)	1.6	2

Table 5.3: CR and PRD for 1D data and 2D data

Thresholding					
1D Data			2D Data		
CR			PRD		
1^st Tier	2^{nd} Tier	3^{rd} Tier	$1st$ Tier	2^{nd} Tier	3^{rd} Tier
10.87	52.27	79.42	1.576	3.11	16.45

Table 5.1 shows the encryption runtime of data files.

Table 5.2 shows the decryption runtime of data files.

Table 5.3 shows the CR and PRD for 1D data and 2D data.

6. Conclusion. Due to the rapid development of IoMT and WSNs, as well as our focus on privacy protection, we can expect that our medical healthcare scheme will have a wide scope of applications. A prototype system that proved it to be functional was created, where an encryption algorithm using a Modified RSA (mRSA), a compression technique using DWT, and a homomorphic strategy for data security and privacy protection have been proposed based on a scrambling matrix. Through values readings of compression ration and accuracy) (CR=79.42, and PRD=1.576) they are proving to be a more efficient algorithm. The proposed mRSA cannot be broken by guessing only the private key The LIDC dataset is obtained, pre-processed, and segmented to train and choose pre-trained deep learning models. As a result, we can conclude that mRSA is more secure in terms of brute force attacks, where the findings mention that the proposed mRSA algorithm becomes more secure against mathematical attacks due to improvements in security. Despite the abundance of sensor nodes, some problems remain unresolved, such as the lack of secure key management. These issues will be taken into consideration in the future.

REFERENCES

[1] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, *Big healthcare data: preserving security and privacy*, J. Big Data, 5.1, 2018.

[2] Alani, Talah Oday, and Ameer Mosa Al-Sadi, *Survey of optimizing dynamic virtual local area network algorithm for software-defined wide area network*, TELKOMNIKA (Telecommunication Computing Electronics and Control), 21.1, (2023), pp. 77-87.

[3] Hassan, Hassan J., and Noor Kadhim Hadi, *Implementation of wireless area network for patient monitoring system*, Iraqi Journal of Computers, Communication and Control & System Engineering (IJCCCE), 17.1 (2017): pp. 1-9.

[4] Khazaal HF, Al-Abassi HK, Al-Sadi AM, Al-Sherbaz A., *Evaluating healthcare system based sd-wan backbone*, International Journal of Advanced Science and Technology. 2020;29(1): pp. 671-80.

[5] K. Abouulmehdi, A. Beni-HSSane, H. Khaloufi, and M. Saadi, *Big data security and privacy in healthcare: a review*, Procedia Comput Sci 113, (2017) pp. 73–80.

[6] A.S. Abdulbaqi. et al., *Recruitment Internet Of Things For Medical Condition Assessment: Electrocardiogram Signal Surveillance*, Special Issue, AUS Journal, Institute of Architecture and Urbanism, University of Austral de Chile, (2019), pp. 434-440.

[7] L. Anying, C. Ke, S. He, and L. Yu, *The industry data analysis processing model design-the regional health disease trend analysis model*, In: 2014 International Conference on Cloud Computing and Big Data. IEEE, (2014), pp. 130-133.

[8] J. Archenaa, and E. Anita, *A survey of big data analytics in healthcare and government*, Procedia Comput Sci 50, (2015), pp. 408–413.

[9] Mahmood, S. D., Hutaihit, M. A., Abdulrazaq, T. A., Abdulbaqi, A. S., & Tawfeeq, N. N., *A telemedicine based on EEG signal compression and transmission*, Technology, 18(SI05), (2021), pp.894-913.

[10] A. Belle, R. Thiagarajan, SM. Reza Soroushmehr, F. Navidi, DA. Beard, and K. Najarian, *Big data analytics in Healthcare*, BioMed research international, 2015.

[11] G. Bertoni, L. Breveglieri, P. Fragneto, and G. Pelosi, *Parallel hardware architectures for the cryptographic Tate Pairing*, In: Third International Conference on Information Technology: New Generations (ITNG'06). IEEE, (2006). pp. 186-191.

[12] F. Guo, Y. Mu, W. Susilo, H. Hsing, and DS. Wong, *Optimized identity-based encryption from bilinear pairing for lightweight devices*, IEEE Transactions on Dependable and Secure Computing, 14.2 (2015), pp. 211-220.

[13] Al-Rubbiay, F. H., Youssef, A. Y., & Mahmood, S. D., *Medical Image Authentication and Restoration Based on mCloud Computing: Towards Reliant Medical Digitization Era*, In Doctoral Symposium on Computational Intelligence. Singapore: Springer Nature Singapore, pp. 487-500, 2023.

[14] S. Hamrioui, I. De la Torre Diez, BG. Zapirain, K. Saleem, JPC. Rodrigues, *A systematic review of security mechanisms for big data in health and new alternatives for hospitals*, Wireless Communications and Mobile Computing, 2017.

[15] A.S., Abdulbaqi, S.A.M. Najim, , R.H. Mahdi, *Robust multichannel EEG Signals Compression Model Based on Hybridization Technique*, International Journal of Engineering & Technology(JATIT), 7 (4), (2018), pp. 3402-3405.

[16] YH. Kim, and EN. Huh, *Towards the design of a system and a workflow model for medical big data processing in the hybrid cloud*, In: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE, (2017). pp. 1288-1291.

[17] IT. Kim, C. Park, SO. Hwang, and CM. Park, *Implementation of bilinear pairings over elliptic curves with embedding degree 24*, In: International Conference on Multimedia, Computer Graphics, and Broadcasting. Berlin, Heidelberg: Springer Berlin Heidelberg, (2011). pp. 37-43.

[18] M. Saif Al-din. Najim and M. Shokhan. Al-Barzinji, *Research On Key Security Strategies of Cloud Computing*, Journal of Theoretical and Applied Information Technology (JATIT), 2018, Vol. 96. No.18.

[19] Mahmood, S. D., & Panessai, I. Y., *A Tele Encephalopathy Diagnosis Based on EEG Signal Compression and Encryption*, In Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers (Vol. 1347, p. 148). Springer Nature. 2021.

[20] Abdulbaqi, A. S., & Panessai, I. Y., *Designing and implementation of a biomedical module for vital signals measurements based on embedded system*, Int. J. Adv. Sci. Tech, 29(3), (2020), pp. 3866-3877.

[21] C.s Stergiou, and KE. Psannis, *Efficient and secure big data delivery in cloud computing.*, Multimedia Tools and Applications 76 (2017), pp. 22803-22822.

[22] D. Thilakanathan, Y. Zhao, S. Chen, S. Nepal, RA. Calvo, and A. Pardo, *Protecting and analyzing health care data on cloud*, In: 2014 Second International Conference on Advanced Cloud and Big Data. IEEE, (2014). pp. 143-149.

[23] T. Unterluggauer, and E. Wenger, *Practical attack on bilinear pairings to disclose the secrets of embedded devices*, ÷n: 2014 Ninth International Conference on Availability, Reliability and Security. IEEE, (2014). pp. 69-7.

[24] A.S. Abdulbaqi, and Panessai, Ismail Yusuf, *Efficient EEG Data Compression and Transmission Algorithm for Telemedicine*, Journal of Theoretical and Applied Information Technology (JATIT), 97(4), (2019), pp. 1060-1070.

[25] R. Vargheese, *Dynamic protection for critical health care systems using Cisco CWS*, In: 2014 fifth international conference on computing for geospatial research and application. IEEE, (2014). pp. 77-81.

[26] Weiwei F, Dongsheng Z, and W. Songjun, *A fast statistics and analysis solution of medical service big data*, In: 2015 7th International Conference on Information Technology in Medicine and Education (ITME). IEEE, (2015). pp. 9-12.

[27] J. Xie, Z. Song, Y. Li, Y. Zhang, H. Yu, J. Zhan, Ma Z, Y. Qiao, J. Zhang, and Guo J., *A survey on machine learning based mobile big data analysis: challenges and applications*, Wireless Communications and Mobile Computing, 2018. https://doi.org/10.1155/2018/87386613.

[28] Al-Barzinji, S. M., Al-din, M. S., Abdulbaqi, A. S., Bhushan, B., & Obaid, A. J., *A Brain Seizure Diagnosing Remotely Based on EEG Signal Compression and Encryption: A Step for Telehealth*, In: Artificial Intelligence for Smart Healthcare. Cham: Springer International Publishing, (2023). pp. 211-225.

[29] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, *Certificateless key-insulated generalized Signcryption scheme without bilinear*

pairings, Security and Communication Networks, 2017.

Edited by: Mustafa M Matalgah
Special issue on: Synergies of Neural Networks, Neurorobotics, and Brain-Computer Interface Technology: Advancements and Applications
Received: Feb 2, 2024
Accepted: Mar 13, 2024