Assessment of Encryption and Decryption Schemes for Secure Data Transmission in Healthcare Systems

Kazeem B. Adedeji[1], Nnamdi I. Nwulu[1], Clinton Aigbavboa[2] and Saheed L. Gbadamosi[1]
[1]Department of Electrical and Electronic Engineering Science, University of Johannesburg, South Africa
[2]Department of Construction Management and Quantity Surveying, University of Johannesburg, South Africa
Email: kezman0474@yahoo.com

***Abstract*—In the biomedical research community, transmitting a patient medical record via wireless means to an administrative centre or other medical centres is increasingly common. However, due to the open nature of wireless media, the security of such a system is a major concern, so, it is desirable to have a reliable security scheme. Amidst the numerous methods used to secure medical data, encryption schemes are becoming more popular due to their performance and relative simplicity. In this study, the performance of some data encryption and decryption schemes used to secure medical data is evaluated. These schemes are Blowfish, DES, AES, RC4, RSA, ECC, CBE, MTLM and CEC. The performance of these schemes was assessed through their execution time, throughput, average data rate and information entropy. For this performance assessment, some medical data were used for this task. The results showed that the performance of CBE, MTLM and CEC was better. CBE and MTLM offer a secure way to encrypt data with a significant reduction in the execution time. Moreover, if some of these schemes were combined to form a hybrid system, an enhancement in the security of medical data over wireless communication networks is guaranteed.**

***Keywords*—Data security, decryption, encryption, healthcare system, medical data, wireless media.**

I. Introduction

The wireless communications market has enjoyed significant growth over the years. Moreover, with the recent advancement in the internet of things (IoT), the biomedical research community is moving towards transmitting a significant amount of clinical data (such as patient medical data) from a workstation to a remote centre via wireless communication networks [1]. For example, Fig. 1 presents an example of medical data being measured, processed and transmitted to a distant medical centre via a wireless medium. As illustrated in Fig. 1, medical data is protected in order to avoid eavesdropping by digitizing the image and the resulting digital sequence encrypted into an unintelligible image [2].

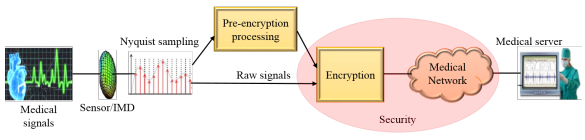

Fig. 1. Secure medical data transmition over a wireless media [3].

The authors wish to acknowledge University of Johannesburg, South Africa for the support.

As illustrated in Fig. 1, the transmission of patient medical information such as the electrocardiograph (ECG) to a remote centre by wireless means is becoming increasingly common in the biomedical research community. Some medical regulations require the sharing of medical data beyond a single inter-disciplinary medical centre [1]. Therefore, utilizing sensors planted on human body, this medical data can be measured and transferred to a processing hub. Thereafter, the processed information can be transferred to a remote centre through a wireless medium. Moreover, with the rapid development of micro-electro-mechanical-systems (MEMS), smart sensors are been deployed to several areas of healthcare services such as wireless body area networks (WBANs) [4] shown in Fig. 2 to track clinical data and health status of patients.

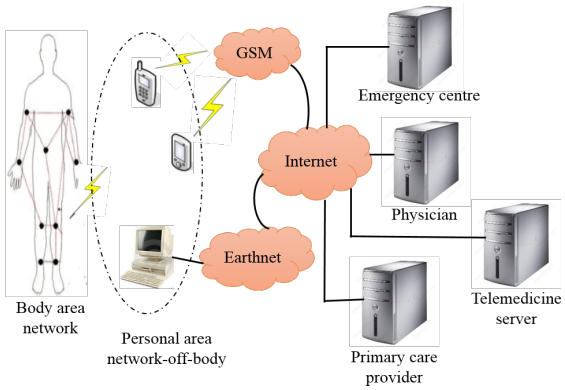

Fig. 2. WBANs deployment in healthcare system [4].

In a WBAN, sensor nodes are positioned near the cloth or occasionally implanted on the skin to track the patients health [5]. These sensors, such as a temperature sensor, for example, measures a patients body temperature while other wearable devices may provide a patient's pulse rate information. The sensor readings are transmitted to a remote admin centre via wireless media. This seamless capacity and continuous interchange of medical information in real-time have made a WBAN a promising sensor technology to enhance healthcare services [6]. However, the security of this system is a challenge due to the open nature of wireless media, which makes it exposed to various attacks from unauthorized users. Thus, the security of medical data is a major concern in e-health monitoring as all entities could access open wireless media

such as the internet environment. This raised a question about the leakage to an unauthorized party, of patient's private physiological data. In the case of a jamming attack [7], the content of this data may be compromised to deceive a medical professional. Therefore, protecting patient medical information is vital. For secured data transmission over a wireless communication medium, numerous methodologies have been developed. These methodologies are known as encryption and decryption schemes. These schemes are algorithm way of transforming sensitive information to a form that an unauthorized recipient cannot read. Usually, this is accomplish via an encryption formula and a key to hide its meaning, making it strenuous for any competitor to retrieve the original information. Fig. 3 illustrates an encryption and decryption process used to secure a plaintext data. As shown in Fig. 3, the encryption process is executed at the sending end, where the plaintext is encrypted/coded with the use of a key (sequence of N-bit) to form a ciphertext. The ciphertext sent over the wireless media can only be decrypted/decoded by personnel having the correct decryption key to retrieve the original data.

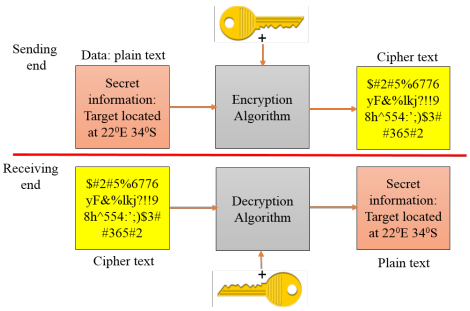

Fig. 3. Illustration of an encryption and decryption process.

Earlier studies classified these schemes into symmetry and asymmetry encryption schemes [8–10]. Each of these schemes has one advantage over the other. The former uses a single key for the encryption and decryption process. Encrypting data using this scheme is relatively faster, however, such a scheme is faced with key management challenge. If anyone knows the key, the entire system collapses as all entities with the key can easily access the data. On the other hand, asymmetry encryption schemes utilise two separate but mathematically related keys; one key is deployed for encryption, while the other is deployed during decryption. This scheme overcame the key management concern; however, it is computationally demanding.

In the past and in recent times, many studies have been accomplished using encryption schemes to secure medical data across wireless communication media [1–6, 11–18]. However, we postulate that based on the level of clinical data importance, the performance assessment of these schemes is essential for secure data transmission in healthcare systems. Therefore, this paper presents a performance assessment of some of the encryption schemes used to secure medical data. The authors are optimistic that the assessment of these schemes could provide useful information on which schemes perform better and are suitable for use in healthcare systems. Consequently, for application in the healthcare system, a robust encryption scheme could be developed for data transmission over future generation wireless media. The paper is arranged as follows. Section II presents the methodology, overview of the schemes and the metrics used to assess the performance of each scheme. Section III outlines the results obtained from the assessment. Finally, Section IV presents the conclusion and future work.

II. Research Method

This work involves examining the performance of some data encryption schemes to secure medical data when transmitted via wireless communication media. The performance metrics used to evaluate these schemes are based on their execution time, throughput, the average data rate and information entropy. At first, an overview of the operation involved in some of these schemes is presented before evaluating the performance.

A. Overview of the Assessed Data Encryption Schemes

In this section, an overview of the encryption and decryption process of Elliptic Curve Cryptography (ECC), Rivest Cipher 4 (RC4), Blowfish and the Chaos-Base Encryption (CBE) schemes is presented. The Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), Cyclic Elliptic Curve (CEC) and Mixed Transformed Logistic Map (MTLM) encryption and decryption processes could be found in [15, 16, 19, 20].

1) Elliptic curve cryptography (ECC) scheme: This is an IEEE P1363 standardised scheme. It is a public-key (asymmetry) encryption scheme based on the algebraic structure of elliptic curves over finite fields. The ECC requires short keys than non-ECC encryption schemes to give virtually the same security [21]. It is therefore regarded as an alternative method for implementing public-key encryption schemes. The encryption and decryption processes is briefly illustrated in Fig. 4. The scheme consists of three stages, namely key generation, encryption and decryption. Fig. 5 illustrates the key generation process for the ECC scheme.

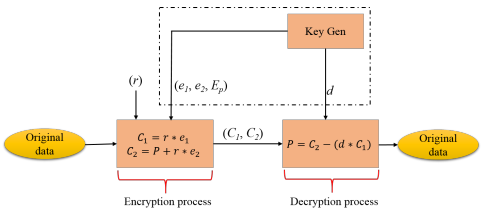

Fig. 4. ECC encryption scheme [21].

Since the ECC scheme uses an elliptic curve for its operation, its key generation algorithm begins by finding point $E_p(a, b) : y^2 = x^3 + ax + b$ on an elliptic curve and also selecting a point $e_1(x_1, y_1)$ on the curve such that $4a^3 + 27b^2 \neq 0$ if e_1 is odd and $b \neq 0$ if e_1 is a power of 2. An integer d is

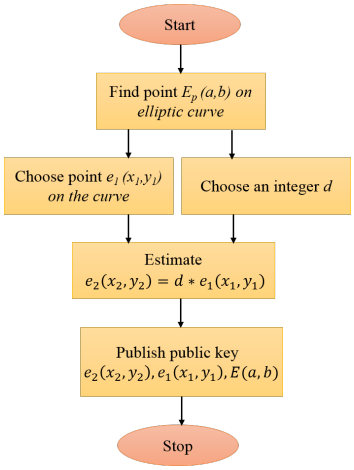

Fig. 5. ECC key generation flow chart adapted from [21].

also selected as a private key. The algorithm then computes the estimate of $e_2(x_2, y_2)$ as [21]

$$e_2(x_2, y_2) = d \times e_1(x_1, y_1) \tag{1}$$

Thereafter, the public key is published as e_1, e_2. The private key is kept secret and used during the decryption process. At the sending end, the image data P, after transforming into a series of binary bits, is combined with the public keys e_1 and e_2 with a randomly generated number r, giving rise to encrypted (cipher) data C_1 and C_2 as

$$\left.\begin{aligned} C_1 &= r \times e_1 \\ C_2 &= P + (r \times e_2) \end{aligned}\right\} \tag{2}$$

The encrypted data C_1 and C_2 are sent over a wireless communication medium. At the other end, the receiver uses a private key d on the cipher data to retrieve the original data P as

$$P = C_2 - (d \times C_1) \tag{3}$$

2) RC4 encryption scheme: This is a symmetric key encryption scheme that utilises the same key during both encryption and decryption processes. The data to be encrypted is digitized and XORed with a generated key sequence. RC4 scheme uses 1 to 256-bit state variable key. Its operation includes both the key initialisation and the encryption/decryption process. The pseudo-code [22] in **algorithm 1** illustrates the key initialisation process.

Algorithm 1: RC4 key initialisation process

1. **Start**
2. j=0;
3. **for** i=0:255 and $S[i] = i$;
4. Compute $j = (j + S[i] + K[i])mod256$;
5. Swap $S[i]\&S[j]$;
6. **end for** i;
6. **Stop**

After the key initialisation process, the encryption operation is given by the sets of pseudo-code shown in **algorithm 2**. By reversing the encryption operation, the original data can be retrieved.

Algorithm 2: The encryption process

1. **Start**
2. $i = j$=0;
3. **for** $k = 0 : N - 1$; {
4. $i = (i + 1)mod256$;
5. $j = (j + 1)mod256$;
6. Swap $S[i]$ & $S[j]$;
7. Compute $K_s = S[(S[i] + S[j])mod256]$;
8. % K_s denotes the key stream;
9. % The encrypted data C is given as;
10. $C = M[k] \oplus K_s$;
11. % where $M[0, ..., N - 1]$ denotes input data bits.
12. **end for** k }
13. **Stop**

3) Blowfish encryption scheme: The Blowfish scheme is designed by Schneier [23]. It is an unpatented and licensed free data securing. The scheme has a 16 round of key-dependent operations, and the input data to be encrypted is transformed to a 64-bit data element. The encryption process may be achieved using the pseudo-code [24] in **algorithm 3**.

Algorithm 3: The Blowfish encryption process

1. **Start**
2. % Divide the data element x into 32-bits halves; left half; xL and right half xR;
3. **for** $i = 1 : 16$;
% i is an integer representing the number of operations.
4. $xL = xL \oplus Pi$;
% P_i is the key bits
5. $xR = F(xL) \oplus xR$;
6. Swap xL and xR;
% after the 16th round, undo the last swap by swapping; xL and xR again;
7. Then, compute $xR = xR \oplus P_{17}$; $xL = xL \oplus P_{18}$
% to get the encrypted data, xL and xR are recombined;
% the decryption is a reverse process of the above.
8. **end for** i
9. **Stop**

4) Chaos-base encryption (CBE) scheme: The encryption and decryption process of a CBE scheme is based on confusion and diffusion principles. That is chaotic confusion and pixel diffusion [17, 18]. The former employs chaotic maps to accomplish the confusion of pixels. In the later, a plain image is altered and the value of each pixel changes one by one by the chaotic confusion stage. Encryption process is described by the following steps [17, 18]:

- Establish a mapping scheme of trajectory;
- Select an initial condition and a parameter key;
- Set the initial condition as current trajectory and iterate the chaotic equation $x_{n+1} = r_c x_n(1 - x_n)$ until the tra-

jectory reaches the stopping point for each data symbol. A logistic map [25] is used to produce the iterates using the chaotic equation by selecting the parameter r_c for the chaotic regime and $x_0 \in (0, 1)$ for the initial condition. A set of large numbers of these iterations [$\sim$ 60, 000] is referred to as the trajectory [25].

- Store the number of iterations as a cipher and encrypt the next data stream with the current trajectory.
- Produce the cipher and repeat the process. For details analysis of this scheme, the reader is referred to [17, 18].

B. Performance assessment metrics

Each of the schemes was used to encrypt and decrypt six medical data samples shown in Fig. 6, of different sizes ranging from 51 kB to 100 kB. The simulation time for encryption and decryption was recorded in each case, and the throughput (MB/s) [20] estimated thus;

$$TP = \sum \left(\frac{D_s}{S_t} \right) \tag{4}$$

where TP denotes the throughput of encryption/decryption, D_s is used to represents the size (kB) of the medical data encrypted or decrypted while S_t is the simulation time $(seconds)$ used to execute the encryption or decrypting process. Moreover, the average data rate (MB/s) may be estimated using (5) [20].

$$ADR = \frac{1}{N_T} \sum_{i=1}^{N} \frac{D_i}{S_i} \tag{5}$$

In (5), ADR denotes the average data rate of encryption or decryption, D_i represents the size (kB) of the i^{th} medical data encrypted or decrypted while S_i is the simulation time $(seconds)$ used to execute the encryption or decryption of the i^{th} medical data. Also, i is a positive integer that range from $(i = 1, 2, ...N)$. For this study, the number of medical data encrypted $N = 6$.

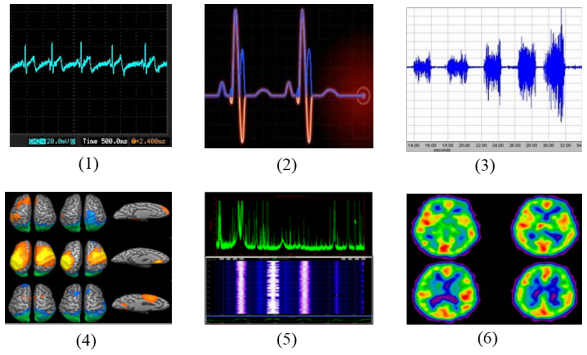

Fig. 6. Medical data samples used for the simulation.

In addition, information entropy is evaluated. This is a criterion used to evaluate the strength of an encryption scheme. It concerns the expected amount of information that can be inferred from the encrypted image. The entropy of an information $H(s)$ may be expressed as [16].

$$H_e(S) = -\sum_{i=0}^{M} P(s_i) log_2(P(s_i)) \tag{6}$$

where M denotes the total number of symbols ($s_i \in S$) in the information S while $P(s_i)$ is used to represents the possibility of occurrence of symbol s_i from the information. If $H_e(s) \cong 8$, such scheme is considered safe against an entropy attack [16, 17].

III. Obtained Results

The data encryption schemes have been used to encrypt six medical data in a Microsoft visual C sharp environment, performed on an Intel(R) Core i7-2620M, 2.7 GHz processor with Windows 8.1 platform. Fig. 7 and Fig. 8 show the simulation time used to perform the encryption and decryption of the data.

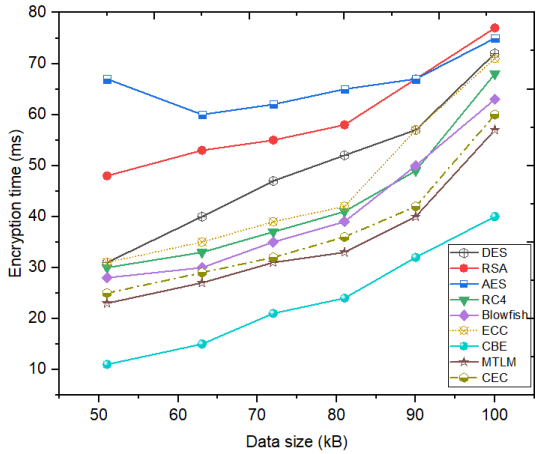

Fig. 7. Simulation time for encryption.

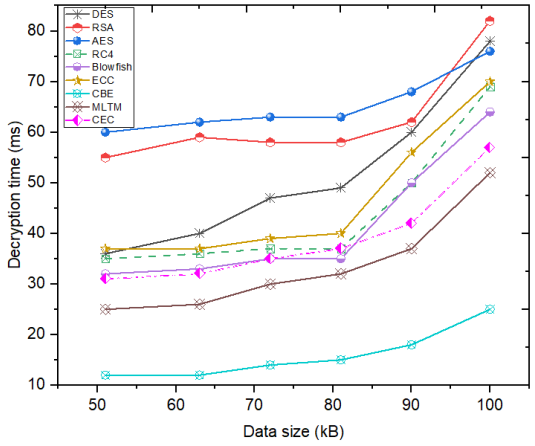

Fig. 8. Simulation time for decryption.

In Fig. 9 and Fig. 10, the encryption and decryption throughput for the schemes is presented, while in 11 and Fig. 12, the average data rate for encrypting and decrypting these data is presented.

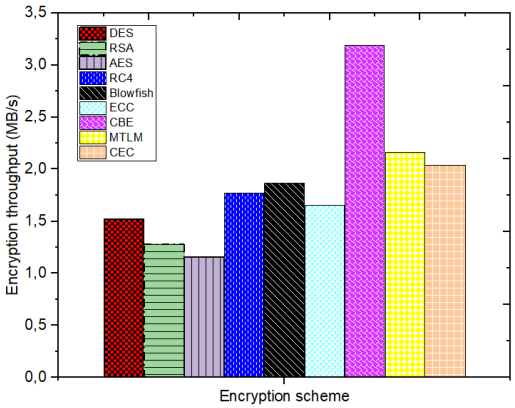

Fig. 9. Encryption throughput.

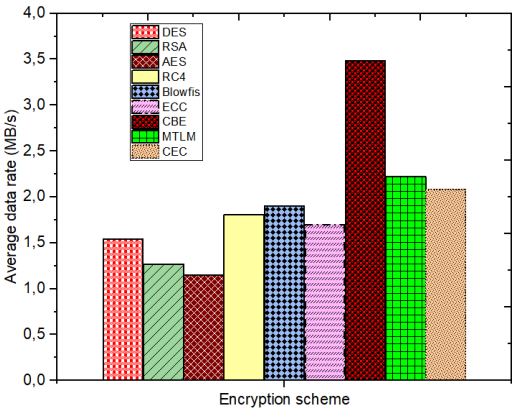

Fig. 11. Average data rate for encryption.

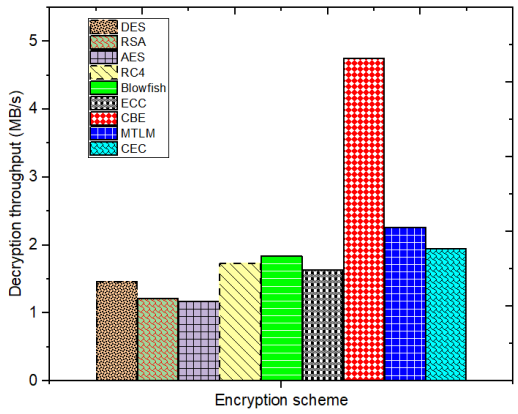

Fig. 10. Decryption throughput.

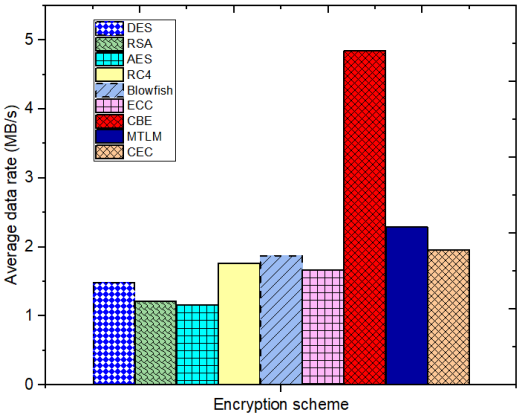

Fig. 12. Average data rate for decryption.

A. *Analysis of Results*

The simulation time gives an indication of the running speed of the schemes. In real-time applications for healthcare systems, this is fundamental for a good scheme. It is important to mention that this speed depends on the CPU structure and the RAM size. It may be inferred from Fig. 7 and Fig. 8 that both the CBE and MTLM has the lowest simulation time. They show better performance than other schemes under the same data size. It also takes more time for AES and RSA schemes to encrypt/decrypt the data. The CBE scheme has a significant reduction in the execution time with a total execution time of about 143 milliseconds (ms) for all the data. The MTLM and CEC have a total execution time of 211 ms and 224 ms respectively. However, during the decryption process, the total execution time due to these three schemes are 96 ms for CBE, 202 ms for MTLM and 234 ms for CEC respectively. This shows that the CBE and MTLM spent less time during their decryption process when compared to the CEC counterpart.

Considering Fig. 9 and Fig. 10, it may be observed that CBE and MTLM have higher throughput in both cases. Consequently, they consume more CPU power during these processes. The throughput of a scheme varies inversely as the CPU power consumption [26]. Thus, in this respect, the throughput of the AES scheme can be considered better than other schemes for both encryption and decryption processes.

Moreover, with regard to the average data rate for encrypting and decrypting the data as presented in Fig. 11 and Fig. 12, it may be observed that CBE, MTLM and CEC has a high data rate (with the CBE scheme having the highest). During the encryption process (Fig. 11), the data rates due to CBE, MTLM, and CEC schemes are 3.492 MB/s, 2.222 MB/s and 2.087 MB/s respectively. However, during their decryption process, 4.840 MB/s, 2.292 MB/s, and 1.960 MB/s data rates were observed. This shows that the CBE and MTLM offer a higher data rate during their decryption process. The data rates for both RSA and AES schemes is relatively low during both processes. In general, the three schemes (CBE, MTLM and CEC) can be used to encrypt/decrypt more data in a few seconds, than any other schemes presented in the figures.

Table I reports the information entropy for the assessed encryption schemes. As shown in Table I, it was noticed that CBE and MTLM have an entropy of 7.991 and 7.821 respectively which are closer to the conceptual value of 8 than the remaining schemes. Therefore the data content during encryption process of such schemes can be considered safe

against an entropy attack than other schemes presented. The entropy results for both DES and AES indicate that secure information transmission with both schemes is far less good than those of CBE and MTLM.

TABLE I
ENTROPY RESULTS FOR THE ASSESSED ENCRYPTION SCHEMES.

S/N	Encryption scheme	Entropy value
1	DES	5.791
2	RSA	6.221
3	AES	5.832
4	RC4	6.021
5	Blowfish	6.122
6	ECC	6.322
7	CBE	7.991
8	MTLM	7.821
9	CEC	6.312

IV. CONCLUSION

In this paper, the performance of nine different data encryption schemes for securing medical data is presented. The results obtained showed that CBE, MTLM and CEC schemes show better performance in terms of simulation time, the data rate of encryption and decryption, and the entropy. Moreover, it was observed that CBE offers a secure way to encrypt data with a significant reduction in the execution time than all other schemes. Also, DES and RSA require more time to encrypt data.

We are at the dawn of the 21st century, where several key events in technological improvements have been encountered. And with the improvement in computing power, many decrypting schemes are being developed, raising fears about a robust security scheme for clinical data transmission over the open wireless media. Therefore, if some of these schemes such as CBE and MTLM/CEC were combined to form a hybrid system, an enhancement in the security of healthcare medical data transmission across the wireless communication media may be guaranteed. In general, improved research studies are necessary for the provision of active security schemes for today's and future generation wireless network, which may be used in healthcare systems.

REFERENCES

[1] M. Canim, M. Kantarcioglu, and B. Malin, "Secure management of biomedical data with cryptographic hardware," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 166–175, 2012.

[2] J. E. John, "Biomedical image transmission based on modified feistal scheme," *International Journal of Computer Science and Information Technology*, vol. 5, no 3, pp. 175–182, 2013.

[3] F. Hu, Q. Hao, and M. Lukowiak, "Implantable medical device communication security: pattern vs. signal encryption," *In: Proceedings of the 2nd USENIX conference on Health security and privacy*, USENIX Association, August, 2011, pp. 1–2.

[4] L. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transaction on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2013.

[5] P. Sandeep, Z. Heye, C. M. Subhas, L. Chunyue, W. Yumei, L. Guanglin, W. Wanqing, and Z. Yuan-Ting, "An efficient biometric-based scheme using heart rate variability for securing body sensor networks," *Sensors*, vol. 15, pp. 15067–15089, 2015.

[6] M. Tao, L. S. Pradhumna, H. Michael, P. Dongming, S. Hamid, and C. Hsiao-Hwa, Assurance of energy efficiency and data security for ECG transmission in BASNs," *IEEE Transactions on Biomedical Engineering*, vol. 59, no. 4, pp. 1041–1048, 2012.

[7] Z. Lu, W. Wang, and C. Wang, "Modelling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp.1746–1759, 2014.

[8] P. Chaitanya, and R. Sree, "Design of new security symmetric and asymmetric cryptography schemes," *World Journal of Science and Technology*, vol. 2, no. 10, pp. 83–88, 2012.

[9] J. Jaleel, and J. M. Thomas, "Guarding image using symmetric key cryptographic technique: blowfish scheme," *International Journal of Engineering and Innovative Technology*, vol. 3, no. 2, pp. 196–201, 2013.

[10] N. Kaladharan, "Unique key using encryption and decryption of image," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 10, pp.8102–8104, 2014.

[11] A. Samoud, and A. Cherif, "RSA scheme implementation for ciphering medical imaging," *International Journal of Computer and Electronics Research*, vol. 1, no. 2, pp. 44–49, 2012.

[12] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt, A. and Uhl, "Confidential storage and transmission of medical image data," *Computers in Biology and Medicine*, vol. 33, no. 3, pp. 277–292, 2003.

[13] C. Fu, W. H. Meng, Y. F. Zhan, Z. L. Zhu, F. C. Lau, K. T. Chi, and H. F. Ma, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp.1000–1010, 2013.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based scheme for image encryption," *World Academy of Science, Engineering and Technology*, vol. 27, pp.206–211, 2007.

[15] S. Sam, P. Devaraj, and R.S. Bhuvaneswaran, "A novel image cipher based on a mixed transformed logistic map," *Multimedia Tools and Applications*, vol. 56, no. 2, pp. 315–330, 2012.

[16] A. Abd El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.

[17] S. Ahadpour, and Y. Sadra, "A chaos-based image encryption scheme using chaotic coupled map lattices," arXiv preprint arXiv:1211.0090, 2012.

[18] E. Yavuz, R. Yazc, M.C. Kasapba, and E. Yama, "A chaos-based image encryption scheme with simple logical functions, *Computers and Electrical Engineering*, vol. 54, pp.471–483, 2016.

[19] K.B. Adedeji, and A.A. Ponnle, "A new hybrid data encryption and decryption technique to enhance data security in communication networks: scheme development, *International Journal of Scientific and Engineering Research*, vol. 5, no 10, pp. 804–811, 2014.

[20] K.B. AdedejI, and J. O. Famoriji, "Investigating the effects of increasing the key size on the performance of AES scheme for encryption of data over a communication channel," *International Journal of Applied Information Systems*, vol. 7, no. 8, pp. 6–10, 2014.

[21] A.P. Shaikh, K. Vikas, and S.K. Narayankhedkar, "Security enhancement scheme for data transmission using elliptic curve diffie-hellman key exchange," *IJAIS Proceedings on International Conference and workshop on Advanced Computing*, no. 2, June, 2014, pp. 10–16.

[22] A. Mousa, and A. Hamad, Evaluation of the RC4 scheme for data encryption," *International Journal of Computer Science and Application*, vol. 3, no. 2, pp. 44–56, 2006.

[23] B. Schneier, "Applied cryptography," New York, USA, John Wiley and Sons, 1994.

[24] A. Deshpande, and P.S. Choudhary, "FPGA implementation of blowfish cryptographic scheme," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 4, pp. 542–547, 2014.

[25] Q.V. Lawande, B.R. Ivan, and S.D. Dhodapkar, "Chaos based cryptography: A new approach to secure communications," it BARC Newsletter, no. 258, pp. 1–28, 2005.

[26] K. Aman, J. Sudesh, and M. Sunil, "Comparative analysis between DES and RSA scheme," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, pp. 386–390, 2012.