University of Sindh Journal of Information and Communication Technology (USJICT)
Volume 4, Issue 3, October 2020
ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Body Sensor Network – ID-Based Cryptography

Muzna Junaid Chishti, Shariq Mahmood Khan,
Department of Computer Science & Software Engineering, NED University of Engineering and Technology Karachi Technology Karachi, Pakistan
muzna.chishti@gmail.com, shariq@neduet.edu.pk

***Abstract*— Healthcare is one of the largest sectors where the influence of major scientific interventions has assisted practitioners in a variety of ways. Today, majority of the diagnosis and patient care methods are vulnerable due to limitations in fulfilling security objectives. Thus, both the doctors and the patients have to suffer from many medicinal complications. With analyzing such problems in the current healthcare industry, a technology-based mechanism is introduced with a purpose to monitor patient's health in a supervised manner. The present study followed a qualitative research method in which the main focus was secondary resources for gathering essential information regarding the concept. The researcher developed a conceptual framework and an algorithm to minimize security concerns that are related to sharing information between a doctor and a patient and developing a valid diagnosis.**

Keywords—body sensor network, cryptography, security, healthcare

I. INTRODUCTION

Since there is a huge demand of integration of mass smart technology in most of the areas, healthcare also requires massive attention to overcome healthcare and patient-related problems [1]. In this regard, there have been researches conducted to explore a variety of ways through which a supervised system and completely security-based mechanism could be deployed so that medical facilities will make clinical practices easy to be furnished [2]. Through this way, it analyzes that the healthcare industry may sustain its expertise in the future, which will not only provide ease to practitioners but also satisfy patients in terms of effective diagnosis and on-time treatments [3]. Thus, the concept of wireless sensor networks has evolved in this regard, which is explored and investigated in a variety of ways to provide ultimate solutions to remove healthcare barriers [4].

With an increased demand for technical facilities in healthcare [5], wireless-based Body Sensor Network (BSN) is developed as one of the vital healthcare applications, which is associated with providing valuable contributions in satisfying clinical practices. It is one of the efficient and secured applications that offer significant contributions in improving patient's health, delivering an on-time diagnosis, and also assisting in therapeutic monitoring [6]. These features enabled healthcare authorities to rely on smart technology. It produces satisfying results for both the doctors, as well as the patients. However, the BSN network is still in the development process due to acquiring specifications and knowledge regarding essential wireless communication technologies to fulfill healthcare needs.

The main purpose of the study is to understand the need for improving the healthcare environment to support patient care in a supervised manner. Moreover, the study intends to offer a smart and secure solution to satisfy patient care globally so that they can avail efficient and effective clinical services. It is also important to explore that current healthcare needs are not meeting patient safety while practitioners are under the negative influence of limited resources. This lacking restricts their expertise, and thus, it impacts patient care. Furthermore, the exchange of information among doctors and patients is not reliable due to which many theft cases have been reported and thus, problems occur during diagnosis and treatment. One of the reasons for performing the research is to investigate the potentials of Body Sensor Network (BSN) in the area of clinical practices for monitoring patient's health conditions. In this way, it is likely to explore patient mobility, secured channels for transmitting information, data reliability, energy efficiency, and other features based on which the network will be successfully deployed.

II. LITERATURE REVIEW

A. Body Sensor Network (BSN)

According to [7], a body sensor network is a major public network application, which has a high demand in the medical sector due to its many facilities associated with diagnosis and patient care. The technology has become a significant area of research in recent years because of its technical abilities in aiding different medical cases. The study indicates that BSN has a broad scope in medical care because it constitutes several sensors that gather patient information efficiently. This information helps in diagnosis relative to the disease [8]. However, BSN is viewed in terms of these sensors as they can perform such functions efficiently for gathering sufficient amount of information. The research emphasizes the placement of these sensors on

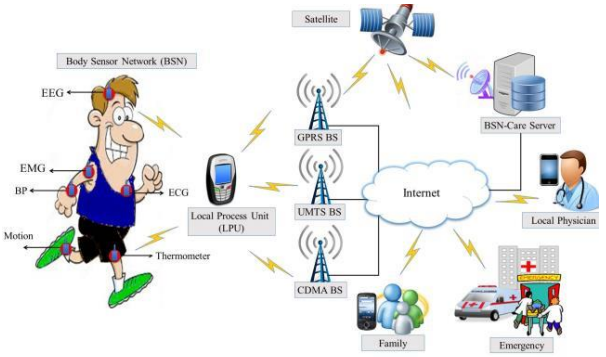

Figure 1: IoT Based Architecture of Body Sensory Network

the human body in a physiological pattern that is responsible for sensing changes in the body according to a defined algorithm [9].

B. Architecture of Body Sensor Network

The illustration in figure 1 represents the allocation of nodes and communication channels that transmits essential information collected from the patient to the doctor. All the nodes attached to the human body comprises of bio-sensing properties, which tend to acquire information about the patient regarding its body functions [10]. Some of the data collected by the sensors are Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), etc. [11]. The physiological information collected by the sensors transmits to the coordinator, known as the Local Processing Unit (LPU), which is mainly a portable device, such as PDA, smartphone, etc. [12]. The primary function of LPU is to perform as a router placed between BSN nodes and the central server, known as the BSN-care server. It comprises of wireless communication mediums, including mobile networks 3G/CDMA/GPRS. However, it also can send alerts to the individual wearing bio-sensors when there is any abnormality detected. The example related to the working of LPU is elaborated by [13], which indicates that when BP of the patient is increased from the standard rate, then LPU immediately provides alert to the person through the attached LPU device.

After LPU aids the first transmission of the data, the BSN-care server receives important medical details of the patients, which are stored in the database and then it analyzes the data to monitor a health condition. The important principle of the system is that it immediately acts on the abnormality and provides necessary information or alert to the person using attached mobile devices. In this way, even family members or emergency units are also informed about the progress. According to [14], the underlying architecture of BSN in the healthcare unit provides details of the information flow from the patient to the doctor and other related individuals based on which the health professionals take necessary actions. It ensures that it monitors patients efficiently through BSN, which gives accurate results to the patients in order for the patient to receive reliable disease preventive measures.

C. Security Requirements and Vulnerabilities in BSN

Table 2 provides a list of major security requirements that are needed to be present in BSN to perform efficient diagnostic practice with the support of key security measures. These security-based aspects are crucial for the network for providing doctors accurate and protected information.

Table 1 Security Requirements in BSN

Security Requirements	Description
1. Confidentiality	Medical data provided by the patient must be secured and stored in a protected way. Encryption and access-list are the best practice to ensure confidentiality
2. Integrity	No unauthorized individual can change, alter, or modify the patient's record
3. Dependability	Patient's data should be easily retrievable when failure of data erasure happens
4. Access Control	Enforcement of policy which limits access to any patient's records
5. Accountability	All the devices within BSN must be held accountable if there is any abuse to the attached components
6. Revocability	All the nodes or privileged users must be deprived in time if their behavior is found compromised or malicious
7. Non-Repudiation	The source of the patient's record must not deny for providing the information to the doctor
8. Authentication	The sender of the patient's record must be authenticated whereas any attack or intrusion should be prevented
9. Availability	The gathered record must be available when requested for access

D. Cryptography in BSN

According to [15], security algorithms are classified as symmetric key encryption and asymmetric key encryption. Both of these classifications most popular in a network system. Each of these algorithms is implemented according to the requirement. [16] states that symmetric key encryption mainly used the same key in the process of both encryption and decryption. One of the advantages of these algorithms is that they utilize low

computation power whereas perform efficiently during encryption. Also, symmetric key encryption is further categorized into block ciphers and stream ciphers. As far as asymmetric key encryption is concerned, [17] highlights that it is the opposite of symmetric key encryption because both encryption and decryption use a unique set of the public and private keys.

Several researches present a variety of contribution in developing cryptography algorithms for BSN. One of the logic for enabling security in the BSN is proposed by [18]. The algorithm is considered significant for the following research because it has enhanced their work by implementing more extended logic to make the algorithm secure and efficient for BSN. The researchers found authentication code as a unique identifier and it establishes further technique. It has utilized some logical operators in the algorithm to make the algorithm complex so that the attacker cannot easily break the mechanism and violate the integrity and confidentiality of the data transmission. One of the loopholes identified in the algorithm was a lack of distinctiveness, which should be required to make the algorithm more secure and challenging for the attacker to comprehend. In this way, the researcher of the following study has carefully analyzed the algorithm and implemented more enhancements to improve the security for BSN.

III. METHODOLOGY

A. Research Methodology

Concerning the nature and requirements of the present study, it followed experimental research methodology. The primary purpose of emphasizing on the method is that the researcher has introduced a new solution in protecting the information from being misused or harm in a healthcare organization. In this way, the researcher proposed a new security algorithm, which was experimented to ensure that it is most secure and reliable as compared to other conventional algorithms. Most importantly, the methodology also demands to explore similar experiments that were researched in the past and introduce a better version that is appropriate and logical in every manner. The researcher performed review and explored many contributions of different authors that were close to its focus of the study. Although reproducing same experiments for analysis was not achievable, the new security algorithm is experimented to witness how security is ensured in the body sensor network.

B. Record Keeping

As the algorithm is entirely based on user input, the researcher analyzed execution of encryption and decryption on the basis based on the size of the data. Table 2 shows the pattern of data input and its sizes based on which execution time is compared.

Table 2 Data Used in the Experiment

Data Input	Input Size (bytes)
Ihave Acne	10
IhaveLeukemiaDisease	20
Ihave type I diabetes problem	30
I have Relapsing Polychondritis disease	40
I have abdominal aortic aneurysum disease 04 years	50

From the above table, it can be noticed that all the user input for the encryption and decryption process are sentences that have the disease name which the patient is suffering from. Since the network is based on accurate diagnosis and providing a secure mechanism to safeguard information transmission, the type of data input is chosen to match healthcare criteria. However, the data input can be changed according to the discipline if required. Moreover, the sizes of these samples were also recorded to make sure that the results of the experiment are consistent and credible as well. In this way, the sizes were distributed in the difference of 10. This means that if the original data input size is 10, then the second data input size will be 20, and so on. In this experiment, the data input or user input is basically a plain text in the encryption phase, which is when encrypted, is known as ciphertext.

C. Logi-Guard Security

1) Pin Code and Its Specification

In the following cryptographic algorithm, the concept of identity was introduced to make the function unique and secured. However, it was also made sure that only when automatically generated code through algorithm retrieved at the source station is matched, a further process of health care assessment will be considered. This is an important approach used in the algorithm so that no faulty application or intruder can access the data without authentic permission. Here, the identity of the patient is referred to as a pin code, which has been used as an authentication code generated at the source and thus, matched at the base station. When the computer indicates a successful match of the code, the user will be directed to proceed to the key generation process that has further complex functionalities leading to a secured process of acquiring patient information.

Besides, it was also ensured that pin code generation is a complete random procedure comprising of various methods to generate numbers that further contribute to developing a new and consistent pin code of the patient. In this way, a frame is generated that has information about a patient's primary information. The size of the frame will be an 8-bit string in which the distribution is identified as first 2-bits represent pin code, third 1-bit represents randomly selected frame number, fourth bit shows updated field number, fifth, sixth, and seventh bits represent patient's information about ECG, Heartbeat, and sugar level respectively, and last bit is the

current sequence number. The distribution of bits is shown in figure 2.

Figure 2: Frame Representation

2) Algorithm to Generate Pin Code

i. Take birth year and initials of the first and last name of the patient as user input that makes up a string ***s***

ii. Split the string in step (i) and consider letters only in the given input

iii. By following table 3, declare values of each letter in the range starting from 0 to 25.

Table 3 Values of Each Letter in the Code

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23
Y	Z						
24	25						

iv. From the result in step (iii), the obtained value must be multiplied by 3 and divide the answer by 8. The significance of number 3 is that we are taking 3 different data from the patient, while 8 represents the string size of the frame.

v. By obtaining value in step iv, take first and the last number before the decimal and indicate it as patient's hash ID.

vi. Apply OR operation on patient hash ID in step (v) with the randomly generated frame number.

vii. The result obtained in step (vi) will be required pin code that must be matched at the base station to proceed further.

3) Key Generation Algorithm

i. In order to generate a key, the following formula will be followed:

Key = (PC + Field) mod 8

ii. Take the value of pin code generated previously and randomly generated field number

iii. Convert pin code and field number in the binary value

iv. Interchange both values with each other and store it in the respective variable, i.e. pin code will be field number whereas field number will be pin code

v. Take values from step (iv) and apply NOR operator along with 2's compliment

vi. Convert a random number "12" in binary and OR it with the value obtained in step (v).

vii. Lastly, convert the value obtained in step (vi) in decimal and take its mod 8. Consider the result as key1. Also, split the key1 as key1L and key1R.

viii. For key2, apply circular shift to key1. Split key2 as key2L and key2R.

4) Algorithm for Encryption

i. Take the patient's data as input and convert it into binary.

ii. Split the input in step (i) and refer each part as inputR and inputL.

iii. Apply XOR operation between key1L with inputL and key1R with inputR. The obtained value will be referred to as the first encryption result and denoted by result1

iv. Now, split the resultant value obtained in (v) into two parts, i.e. result1L and result1R.

v. Again apply XOR operation between result1R with key2R and result1L with key2L and merge the result in the end

vi. In the final result obtained in (vii), again apply XOR with 8 (convert it into binary).

vii. The resultant value obtained in (viii) will be converted into decimal and referred to as ciphertext.

5) Algorithm for Decryption

i. Take the ciphertext and convert it into binary.

ii. Apply XOR operation with the converted ciphertext and 8 (in binary form).

iii. After obtaining result in (ii), split the value into C1R and C1L

iv. Apply XOR operation between C1R with key2R and C1L with key2R

v. Again split the value obtained in (iv) as C2R and C2L and apply XOR between C2R with key1R and C2L with key2L

vi. Merge the result obtained in (v) and refer it as plain text

vii. Convert the binary number into decimal number in (vi)

IV. Analysis and Discussion

A. *Efficiency Parameters for Security Algorithm*

For analyzing the efficiency and complexity of the security algorithms, certain evaluation parameters were selected based on which strength of each algorithm is determined. [19] has analyzed the performance of their algorithm based on randomness, encryption time, decryption time. In this way, the researcher has also considered these parameters significant and also included other parameters for in-depth analysis. These parameters include throughput and distinctiveness

1) *Randomness*

According to [20], randomness is defined as the unpredictability in determining the nature of the keys. Concerning the proposed algorithm, it is seen that all the keys are dependent on the randomness of frame and field number. These values are randomly generated by the executed program during pin code generation and are different for every patient's entry. In this way, the keys become complex and unknown to the attacker since randomness enhance the complexity of the algorithm.

2) *Encryption Time*

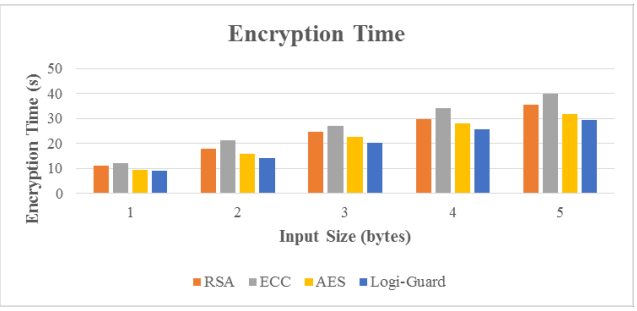

Figure 3: Comparison of Encryption Time

The above graph represents the encryption time of the security algorithms based on the size of data inputted by the patient. As the researcher has tested each of the algorithms on the same data sets, the researcher noticed different encryption times. In the first round, the size of the data was 10 bytes, and RSA encrypted the text in 10.998 seconds. Similarly, ECC encrypted the text in 11.93 seconds while AES converted the plain text into ciphertext in 9.26 seconds. However, Logi-Guard encrypted the text in 8.91 seconds. In this way, it can be seen that Logi-Guard is more efficient in performing the encryption process as compared to other conventional algorithms. Moreover, among these conventional algorithms, AES is more efficient.

If we go from left to right in analyzing the graph, it can be seen that as the data size is increasing, encryption time for every algorithm is increasing as well. By analyzing the graph, it is concluded that the proposed algorithm has taken less time to encrypt the input data as compared to existing algorithms. However, it can be seen that among the existing algorithms, AES took less time to encrypt the data while RSA took more time than the proposed algorithm and AES. Furthermore, ECC is considered to be less efficient in terms of encryption because for each input size; the algorithm took greater time to encrypt the plain text. Therefore, the encryption execution time proves that Logi-Guard performs more efficiently as compared to other conventional algorithms.

3) *Decryption Time*

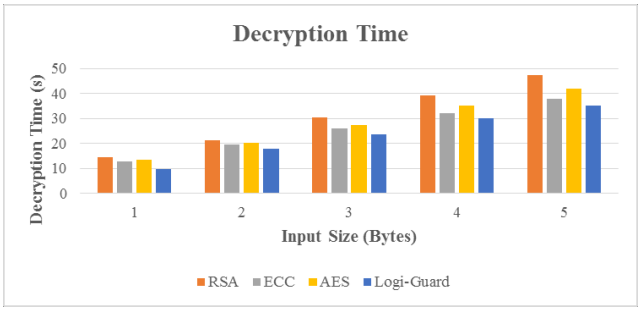

Figure 4: Comparison of Decryption Time

The above graph represents the decryption time of the security algorithms based on the ciphertext after encryption was executed. As the researcher has tested each of the algorithms on the same data sets, different execution times were noticed. In the first round, the size of the data was 10 bytes, and RSA decrypted the text in 14.33 seconds.

Similarly, ECC decrypted the text in 12.91 seconds while AES converted the ciphertext into plain text in 13.54 seconds. However, Logi-Guard decrypted the text in 9.718 seconds. In this way, it can be seen that Logi-Guard is more efficient in performing the decryption process as compared to other conventional algorithms. Moreover, among these conventional algorithms, AES is more efficient.

If we go from left to right in analyzing the graph, it can be seen that as the data size is increasing, decryption time for every algorithm is increasing as well. By analyzing the graph, it is concluded that the Logi-Guard took less time to convert the plain text into cipher text as

compared to the existing algorithms. From the graph, it can be noticed that among all the existing algorithms, AES took less time in decrypting the ciphertext, whereas ECC was noticed to perform efficiently in the same case. However, RSA is considered less efficient in the decryption process as compared to other algorithms.

4) Throughput

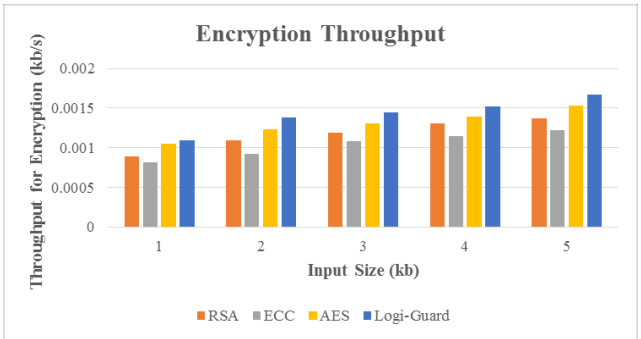

Figure 5: Throughput for Encryption Time

Figure 5 shows the throughput results of all the security algorithms implemented in the following research study based on encryption. From the trend in the graph, it is witnessed that the algorithm with the highest encryption time has the lowest throughput. This means that as Logi-Guard has encrypted all the data samples in less time as compared to other algorithms therefore, it has the highest throughput. Moreover, the graph is showing an increasing trend which means that as the data size increases, encryption time will also increase and thus, throughput value will increase. It is analyzed from the above graph that the throughput of the Logi-Guard is more than the existing algorithm and hence, the speed of the encryption is greater as compared to other security mechanisms.

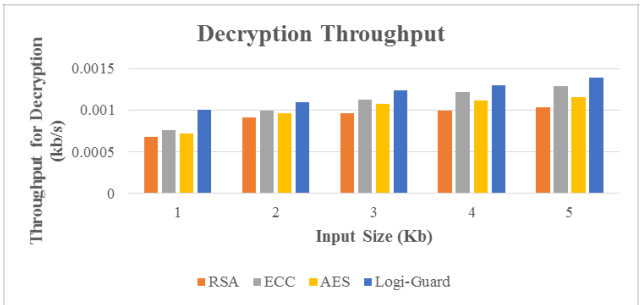

Figure 6: Throughput for Decryption

Figure 6 shows the throughput results of all the security algorithms implemented in the following research study based on decryption. From the trend in the graph, it is witnessed that the algorithm with the highest decryption time has the lowest throughput. This means that as Logi-Guard has encrypted all the data samples in less time as compared to other algorithms; therefore, it has the highest throughput. Moreover, the graph is showing an increasing trend which means that as the data size increases, encryption time will also increase and thus, throughput value will increase. It is analyzed from the above graph that the throughput of the proposed algorithm is more than the existing algorithm and hence, the speed of the decryption is greater as compared to other security mechanisms.

5) Distinctiveness

Distinctiveness in analyzing the performance of the security refers to the extent of identical keys obtained when compared with different datasets. By executing the proposed algorithm, the researcher noticed that it generated a completely different set of keys every time a new patient enters the information. This aspect also considers an element of randomness as well which enhances the distinct nature of the algorithm and also makes it more complex for the attacker to affect the integrity of the messages passed between the patient and the doctor.

B. Discussion

From the above analysis of the implemented security algorithms, it is found that the proposed algorithm is complex in terms of the functions and randomness, whereas existing algorithms are more prone to security attacks. This means that RSA, ECC, and AES are easily breakable as they lag in randomness while their distinctiveness is also partial. Similarly, when the proposed algorithm was analyzed, it was found that the algorithm comprises of more mathematical functions that are comparatively difficult to break because of their complex structure and modified mechanism incorporated in the algorithm.

[18] also evaluated their proposed algorithm in terms of determining the number of logical operators used in each phase of the security. This is because when the algorithm consists of a greater number of logical operators, its complexity increases and thus, the attacker is unable to break the algorithm. With this approach, the efficiency and complexity of the proposed algorithm are achieved.

Table 4 presents the different logical operations used in the proposed security algorithm. However, in table 5, the number of logical operations used in each phase of the security algorithm is highlighted.

Table 4 Logical Operators in Logi-Guard Algorithm

Phase of the Algorithm	Logical Operation
1. Pin Code Generation	OR
2. Key Generation	NOR, 2's Compliment, and Circular Shift
3. Encryption	XOR

4. Decryption	XOR

By looking at table 4, we can see that different logical operators were used in Logi-Guard. The main purpose of using these logical operators is that it increases the complexity of the algorithm, whereas execution is optimized. Mainly, the OR operator is used for adding the two or more values. It can be seen from the algorithm that the OR operator is used in pin code generation where patient hash ID and randomly generated frame number were passed from the following logic gate.

Similarly, NOR, 2's compliment, and circular shift operations were also used in the algorithm but the key generation phase. As we compare the following algorithm with that of the previously proposed algorithm, there is a major change in the function. Logi-Guard has adopted a different strategy, which ultimately follows the arithmetic and logical approach. In this way, the effectiveness of the algorithm is ensured as the more we add logical operators in a particular stage, the stronger the phase will be. The strength of any algorithm lies in the key generation. Therefore, Logi-Guard incorporated three different operations that increase complexity.

In order to understand the purpose of using circular shift operation in the key generation process, it is important to understand the specific traits of a secure cipher as proposed by Shannon in 1949 [21]. One of the traits of a secure cipher is confusion, which represents a complicated relationship between symmetric key and ciphertext [22]. Another trait of a secure ciphertext is diffusion, which represents the relationship between a plain text and ciphertext. In this way, bitwise shifts and rotations promote diffusions [23]. This means that when an algorithm has a circular shift operation, then it is focusing more on the relationship held between the plain text and the ciphertext.

Apart from these operators, Logi-Guard comprises of XOR operators as well. Although the previous algorithm also had a combination of XOR operators, the following algorithm is changed concerning the alignment and number of operators used in each stage. The primary purpose behind using an XOR operator in proposing a security algorithm is that it helps in achieving complexity and cryptography that is quite difficult with other logical operators. In addition, it enhances the strength of the algorithm, which means that it becomes difficult for the attacker to break the code in a few attempts.

Table 5 Total Number of Logical Operators in Each Phase

Phase of the Algorithm	Total Number of Logical Operators
1. Pin Code Generation	OR – 1 time
2. Key Generation	NOR – 1 time 2's Compliment – 1 time Circular Shift – 1 time
3. Encryption	XOR – 5 times
4. Decryption	XOR – 4 times

In this way, the key assumptions deduced from the developed study are highlighted as follows:

1. The data obtained from the patient comprises of total 8 bits
2. The algorithm determines frame number and field number randomly, which are also in 8 bits
3. Whenever BSN obtains private data using the sensors placed on the body, it undergoes different phases comprising of logical operations that are complex and difficult to break
4. Each time, the system will generate a unique key, which is dependent on the pin code
5. Pin code will be completely random due to randomly generated frame number

V. Conclusion and Future Work

The researcher explored the vulnerabilities in BSN and opted for a security procedure that best-fits in the situation where both the doctor and the patient can transfer data among each other without any security barrier. Considering the proposed work of the previous scholar, a different approach was used to develop a more enhanced version of the security algorithm that was based on the patient's ID. The purpose of using the concept was to ensure distinctiveness and that attackers cannot easily extract the information. In this way, a pin code scheme was designed, which was referred to as a unique identifier and is different for every patient. The element of randomness was also added to make the algorithm more complex and secure. Also, keys were generated using the pin code and a proposed equation, which was again a logical aspect in ensuring complexity within the algorithm. Some logical operators were also used in the security algorithm that, too, determines the complexity and makes the algorithm more stable in terms of breaking and complying with security parameters.

As there is limited research conducted in this discipline, there is a need to explore and investigate more about the security and potential measures to be taken in the healthcare domain. BSN itself is an extensive scope in healthcare; it contains specific vulnerabilities, which should be analyzed critically in order to support the

effective diagnosis and treatment of the patients. Besides, the patients are always concerned about their sensitive information that is often exploited because there is no such practical security implementation that ensures confidentiality. In this way, the policymakers should focus on implementing certain policies that are linked with effective security services and complying with the healthcare standards that ensure the patient's safety in every aspect. Other than this, the proposed algorithm can be enhanced by diversifying the concept of key management. The algorithm can be extended at key generation, encryption, and decryption phases.

REFERENCES

[1]. K. M. Cresswell and A. Sheikh, "Health information technology in hospitals: current issues and future trends," Future Hosp J, vol. 2, no. 1, pp. 50-56, Feb 2015, DOI: 10.7861/futurehosp.2-1-50

[2]. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," Security and Communication Networks, vol. 2018, pp. 1-9, 2018, DOI: 10.1155/2018/5978636.

[3]. T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy

[4]. Protection Based on IoT," IEEE, 2015, DOI: 10.1109/PAAP.2015.48.

[5]. N. S. Ali and Z. A. A. Alyasseri, "Wireless Sensor Network and Web Application Hybrid Scheme for Healthcare Monitoring," SOFT COMPUTING AND DECISION SUPPORT SYSTEMS, vol. 4, no. 5, 2017.

[6]. J. H. Y. Ng and B. H. K. Luk, "Patient satisfaction: Concept analysis in the healthcare context," Patient Educ Couns, vol. 102, no. 4, pp. 790-796, Apr 2019, DOI: 10.1016/j.pec.2018.11.013.

[7]. E. Gonzalez, R. Pena, C. Vargas-Rosales, A. Avila, and D. P. de Cerio, "Survey of WBSNs for Pre-Hospital Assistance: Trends to Maximize the Network Lifetime and Video Transmission Techniques," Sensors (Basel), vol. 15, no. 5, pp. 11993-2021, May 22 2015, DOI:10.3390/s150511993.

[8]. Mu, X. Liu, and X. Yi, "Simplified Energy- Balanced Alternative-Aware Routing Algorithm for Wireless Body Area Networks," IEEE Access, vol. 7, pp. 108295-108303, 2019, DOI: 10.1109/access.2019.2925909.

[9]. R. A. Khan and A.-S. K. Pathan, "The state-of- the-art wireless body area sensor networks: A Conference on System Sciences, 2019.

[10]. S. Majumder, T. Mondal, and M. J. Deen, "Wearable Sensors for Remote Health Monitoring," Sensors (Basel), vol. 17, no. 1, Jan 12 2017, DOI: 10.3390/s17010130.

[11]. H. Gui and J. Liu, "Latest Progresses in Developing Wearable Monitoring and Therapy Systems for Managing Chronic Diseases," 2018.

[12]. B. Antonescu and S. Basagni, "Wireless Body Area Networks: Challenges, Trends and Emerging Technologies," 2013, DOI: 10.4108/icst.bodynets.2013.253722.

[13]. Remedy for Latency Issues in Data Access from Clouds," KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, vol. 11, no. 4, pp. 2310-2345, 2017, DOI: https://doi.org/10.3837/tiis.2017.05.001

[14]. A.G.V., N. D.P., R. I.N., G. E.E., and S. M.L., Healthcare Sensing and Monitoring. In: Ganchev I., Garcia N., Dobre C., Mavromoustakis C., Goleva R. (eds) Enhanced Living Environments. Lecture Notes in Computer Science, vol 11369. Springer, Cham, 2019.

[15]. M. Ebrahim, Khan, Shujaat, and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, vol. 61, no. 20, pp. 12-19, 2013.

[16]. M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A Survey on the Cryptographic Encryption Algorithms," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, pp. 333-3444, 2017.

[17]. R. Alvarez, C. Caballero-Gil, J. Santonja, and A. Zamora, "Algorithms for Lightweight Key Exchange," Sensors (Basel), vol. 17, no. 7, Jun 27 2017, DOI: 10.3390/s17071517.

[18]. D.-e.-S. Agha, F. H. Khan, R. Shams, H. H. Rizvi, and F. Qazi, "A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications," Wireless Personal Communications, vol. 103, no. 4, pp. 2877-2890, 2018, DOI: 10.1007/s11277-018-5968-y.

[19]. Z. S. A. Shamsi, "Integration of Lightweight & Energy Efficient Cipher in Wireless Body Area Network For e-Health Monitoring," Master in Software Engineering, Software Engineering, United Arab Emirates University, 2016.

[20]. T. S.A., The Mathematical Foundations of Randomness. In: Landsman K., van Wolde E. (eds) The Challenge of Chance. The Frontiers Collection. Springer, Cham, 2016.

[21]. L. Budaghyan and P. Staˇnica, "a cryptographic Boolean function?," NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY, vol. 1, 2019, DOI: https://doi.org/10.1090/noti/1780.

[22]. M. Y. Mohamed Parvees, J. Abdul Samath, and B. Parameswaran Bose, "Cryptographically Secure Diffusion Sequences—An Attempt to Prove Sequences Are Random," 2019.

[23]. Y. Luo, L. Yao, J. Liu, D. Zhang, and L. Cao, "A Block Cryptographic Algorithm for Wireless Sensor Networks Based on Hybrid Chaotic Map," presented at the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International survey," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, 2018, DOI: 10.1177/1550147718768994.

Conference on Data Science and Systems (HPCC/SmartCity/DSS).