Implementation of Biological Key Based Security Technique in Wireless Body Area Networks

Er. Sandeep Rana, Sandeep Singh Kang

Abstract: ***These days, due to advancements in the technology, security has become the main concern in almost in every field. WBAN has appeared as a popular technologyfor controlling and monitoring the health of the patients. The information of patient's the health status is very crucial and sensitive which must be protected from any illegitimate access. In this paper, a framework is proposed for the security and privacy of medical data of patients by applying Elliptic Curve Cryptography and Diffie-Hellman key generation method for different key sizes. Biometric authentication is used in our system. The biometric images are used as secret keys which are used by the doctors to attain the patient's information. The proposed system replaces the symmetric encryption algorithms used in existing system and offers effective and better results.***

Index Terms: WBAN security, ECC, biometric authentication.

I. INTRODUCTION

As the population is getting aged, it is quite difficult to fulfill the health care needs of seniors and patients by using existing medical resources. There are limited resources and even patients are not compliant to afford the long stays in the hospitals because of financial and economic restriction or may be due to some other reasons. However, the treatment at the hospitals is much better and is done in real time. Nowadays, the technology with ubiquitous is being emerged. With this technology, maximized efficacy, precision and availability of medical treatment is provided because of the advancements in wireless technology communication as well as in electronics field. [1] It offers advanced sensors which are smaller in size and can be used around, as well as embedded on human's body. Subsequently, monitoring wireless medical systems will become part of mobile healthcare centers with real-time monitoring in the future. Wireless body area network (WBAN) has become popular techniqueespecially in such areas of health service facilities because it has a broader utility range and plays an essential role in enhancing the health of humans. The health care sector is looking forward for the systems with developing information and communication technology (ICT) for the administration of delivering heath care services in an effective manner. With the advancement in ICT systems, it become possible to provide the health care at the hospitals as well as at homes or the work place of the patients that saves the money and also offer quality life to the patients. There are many tiny sensors and gateway node comprised in WBAN for connecting it to the external database. Gateway node has responsibility of connecting the sensor nodes to telecommunication networks such as a dedicated hospital network using Wi-Fi, mobile phone network, standard telephone network. Moreover, 3G/4G data networks can be used by WBAN for transmission of the patient's data. [2] The user can store his/her personal data in any portable devices. However, WBAN becomes an exclusive ubiquitous healthcare application. Wireless Body Area Network is different from various other available WSNsas it offers some crucial features.By using identical mobility patterns, the users move with these sensor nodes in this WBAN technology. WBAN consumes less energy in its arrangement. However WBAN is cost effective as the devices used in creating this network are nor much expensive. WBAN nodes are through traditional in order to provide reliability, density and node complexity. But, security is one of the key aspects of any system. Different people have different perception regarding security and thus it has many definitions. Generally, security is safety of the entire system.

WBAN is the collaboration of such sensors which can easily communicate with other nodes as well as could be placed anywhere i.e. inside and outside of the human's body in an autonomous way. Figure 1 is demonstrating about the architecture of WBAN [6]. It comprises of almost 4 parts. The first part WBAN contains numerous sensor nodes.

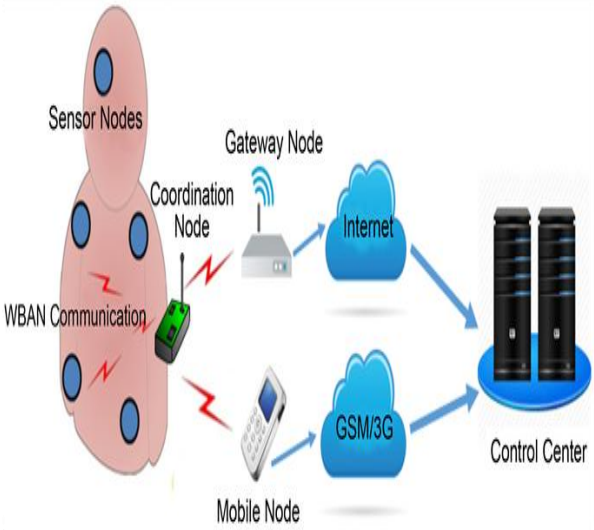


Figure 1: WBAN Architecture [6]

The second section is known as the coordination node, in this part, a coordinating node was connected to the sensor node which is usually called Central Control Unit (CCU).

Revised Manuscript Received on June 13, 2019

Er. Sandeep Rana, Computer Science Engineering,. Chandigarh University, Gharuan (Mohali), Punjab, India.

Dr. Sandeep Singh Kang, Computer Science Engineering,. Chandigarh University, Gharuan (Mohali), Punjab, India.

For the third section, gateways are required to transmit the collected data to receiving section and it is known as WBAN communication. In the last section, it offers direct communication with Mobile phone for messaging, emailing and communicating with PC and server to store the data into database made earlier.

The requirements of WBAN's safety and its acceptance are as discussed below:

1. Data Confidentiality: It represents safety of private information from contact that could be seen as the crucial problem in a Wireless Body Area Network. These nodes could be used in situations such as during emergency in medical, projected as well as dependent on the personal information of patient's health.

2. Data Integrity: It is referred to the various steps taken for protecting message's content, correctness and reliability. In this process, in order to modify the data, some fragments are integrated; data manipulation is done inside packet and is forwarded further. Therefore, the data could not be available and customized by a latent challenger with the implementation of authentication protocols.

3. Data Freshness: This technique efficiently works for the protection of reliability and privacy from captured data and replayed by an adversary through which WBAN coordinator may get confused. It ensures the accuracy of the frames.

4. Availability of the network: It shows an access of monitoring and controlling the patient to the medical practitioner.

5. Data Authentication: The application in the science field should require statistics confirmation. Therefore, WBAN nodes synchronize with the receiver to make sure that the information is received from the synced trust center only.

6.Dependability: System should be reliable and dependable. If the correct data is not fetched it might be a serious matter for the patient.

7. Accountability: It is imperative to protect the information of patient's health in the medical field.

These above stated security needs give rise to critical challenges. And these challenges are vetoed by using cryptographic techniques which includes encryption and decryption of the sensible data.

Encryption: Providentially, there is one advantage of WBAN environments that it provides secure communication if it has low range. Encryption is used to tackle with above challenges. However for encrypting the data, various algorithms are used in WBAN. And there are two popular encryption approaches used for providing communication security:

Symmetric encryption: This is an old, prominent and the simplest technique of encryption which required a secret key to decrypt and encrypt the information. It is used as a number or a word. It is a merged with the plain text in order to change the content in a specific way. The condition is that both sender as well as receiver should know the secret key so that decryption as well as encryption of data could take place. Some techniques of symmetrical encryption are: AES, RC4, Blowfish, DES, and RC5.

Asymmetrical Encryption: In this type of encryption i.e. public key cryptography, two keys are utilized for encrypting the plain text. Exchanging of the secret keys takes place over Internet. It ensures the safety of the keys. Anyone with a secret key can decipher the message and thus, asymmetrical encryption uses two related keys to boost the security. This public key can be accessible to those who want to transmit and receive message to the owner. The second key (Private Key) is kept secret.

Techniques of Encryption Algorithms:

As mentioned above, there are number of encryption techniques in order to attain the security. Most commonly used algorithms for encryption are as follows:

1. Blowfish: Blowfish act as a strong weapon against hackers and cyber-criminals. It uses an exclusive key creation. Key expansion is implemented in which a single key of up to 448 bits is converted into a table of sub keys that is 4168 bytes in size. Sub keys are helpful in making the security tighter as hacker would have to crack more than just the original key.

2. AES: It is a technique of converting raw information into something that cannot be read. Moreover, it is a reversible technique, which means the information can be converted into its real position by applying it again.

3.MD5: Produces hash value of 128 bits with the help of hash function. However, MD5 was made to be used as a cryptographic hash function and suffers extensive vulnerabilities. Data reliability is assured by checksum.

4.HMAC: It is a tool used to calculate message authentication codes using a hash function which is joined with a secret key and required to verify reliability as well as the validity of a message.

5.RSA Security: It is an asymmetric algorithm which uses two different keys. The public key may be provided to anyone and the other key should be kept private in order to maintain the security.

6. ECC: It is a technique to encode data files such that only specific individual can decode it. ECC is created on the basis of mathematics of elliptic curves and it used the location of points on an elliptic curve to cipher and decipher the information. In ECC, features of wireless security are implemented in an efficient manner, such as secure electronic mail and Web browsing.

Advantages of ECC algorithm:

- Keys, cipher texts and signatures have small sizes.
- Key is generated rapidly
- Fast signatures.
- Process encryption and decryption is fairly fast.
- Computation of signatures is done in two stages which allow lower latency as compared to inverse throughput.
- Binary curves are really fast in hardware

II. LITERATURE REVIEW

According to US department of commerce, security is a condition that is achieved after establishing and maintaining protective measures. Moreover, the issues of security the field of healthcare in sensor networks have always been part of active research. Some of the researches are mentioned below:

Amel Arfaoui et al., [2019] [3]Proposed an approach from a security perspective, which achieves confidentiality, integrity, anonymity, context-aware privacy. Performance analysis proves the efficiency and the effectiveness of the proposed scheme in contrast to benchmark schemes with respect to functional security, storage, communication, and computational cost.

Marko Kompara et al., [2019] [10]Analyzes mutual authentication scheme that already exists. This scheme was designed for two-hop WBANs with anonymous

and untraceable key establishment. Thus, author made use of authentication and key agreement approach in order to acquire the data integrity and privacy with anonymity and untrace-ability.

Selimis, G et al., [2019] [20] this security upward has effective impact on the energy diversion which is strongly related to the lifetime of the sensor, a critical aspect in wireless sensor network technology.

Pramanik, P. K. D et al., [2019] [18]Privacy and security chances in tele-health frameworks that can unfavorably influence patients' and clinicians' dimension of trust and eagerness to embrace and utilize the framework.

Peyman Dodangeh et al., [2018][4] Used biometrics for the purpose of authentication and key exchange and fulfilled the requirements in the company of energy-constraint considerations. In [5, 8], authors used the AES algorithm and biometric authentication for data transmission in WBAN to achieve the data privacy and security.

KarmakarK et al. [2018] [5]Authors used the AES algorithm and biometric authentication for data transmission in WBAN to achieve the data privacy and security

Manirabona, A et al. [2018] [7] In this paper proposes 4-levels structure for prosperity RMS to allow transportability of flexible dimensions. From one point of view, it consolidates a traffic classes mapping limit among WBAN and companion frameworks

Arfaoui, A et al., [2018] [16]The ideal vitality mindful burden adjusting of versatile down connection information traffic inside a smaller scale cell with various little cells inside its inclusion zone.

Al-Janabi et al., [2017] [17] It can be further employed in several other fields and applications such a monitoring pollution levels, physiological and medical monitoring, human computer interaction, education and entertainment. A wireless healthcare application offers and brings many benefits and challenges to healthcare sector.

Chukwunonyerem, J et al., [2016] [1] This paper study of security between hub transmission vitality for bio-sensors in a remote body territory sensor organize (WBAN) framework. Existing security arrangements in WBAN have been seen to utilize the pre-sending of static validation keys, which are unbound and vitality serious.

Ali, A et al., [2013] [14]Wireless body area networks are formed by using tiny health monitoring sensors on the human body in order to collect and communicate the human personal information. Framework that supports both intra-WBAN and inter-WBAN communications. By using multiple clusters, energy-efficiency can be ensured. These attacks pose major threats to WBAN security.

Reza Khalilian et al. [2012] [11] Proposed a system in which they utilized the scheme of random key management. In this mechanism, AES (Advanced Encryption Standard) was used for the encryption of the biometric signals

Wang, H et al., [2011] [13]In this work, we build up an incorporated security framework to verify medicinal data correspondences utilizing biometric highlights of the body in WBAN,The Wavelet area HMM confirmation process high train the Single Classification. We have a security-structure that can verify the body sensor correspondence with lower overheads by using body biometric data. The structure open another vista of incorporating biometric data into the security in remote body territory systems.

Tasubramanian, et al., [2003] [21]The sensors embedded inside the human body to screen portion of the body are called bio-sensors. These bio-sensors structure a system and all things considered screen the wellbeing state of their bearer or host. This data is of individual nature and is required to be verified. A biometric based methodology for verifying correspondence in remote systems of biosensors embedded in the human body.

III. RESEARCH GAP

From the literature survey, it was observed that the work is done on attaining the secure data transmission with the help of symmetric encryption algorithm – AES and biometric authentication. The importance of both biometric and non-biometric processes is surveyed in literature. The research gap illustrated that cost of the algorithm used key with large sizes which makes the encryption more complex. These algorithms provided data security but there are some drawbacks of using symmetric encryption algorithms. However, Symmetric encryption algorithms are not much secure. These algorithms take more time for decrypting the data. Thus, novel approach is planned for the data security in WBAN.

IV. PROBLEM FORMULATION

WBAN systems and their respective architectures are distributed allover the globe and these systems face a challenge of security of data reliability, throughput and in disparity to previousclinical system. In addition, there is a critical concern about protecting the patient. These issues provide surety and address system feasibility in the field of security, fault tolerance, consistency, reliability safety, correctness, redundancy, and various human factors. The integration services of patient and data security is required for:

1. The verification of the identity of the WBAN wearer,
2. The protection of confidentiality of the wearer,
3. Establishment and maintenance of secure links between personal WBAN and wearer as well as an individual sensor and its parent device,
4. Maintenance of the sensor data's integrity from initial achievement to final storage.
5. The protection of the access to reach stored data

V. PROPOSED WORK

The information of patient's health is very sensitive and crucial. Thus, it must be kept safe from illegitimate access because altering the health status of patients can result in life-threatening situations. Therefore, security of patient's health status has become a main concern in the hospitals and medicalclinics. Various techniques are being used to stumble upon this issue such as symmetric techniques, multi-level security approaches and biometric identification. Recently, in paper [3], author made a system utilizing both biometric authentication and AES algorithm (symmetric technique) in which key is generated with the biometric prints (thumb/palm print) of patients and doctors and MD5 is used to secure the password of both the accounts of patients and doctors. But it has some drawbacks such as decryption in AES algorithm takes four times than encryption process and the logic made by the author for key generation is not much relevant in offering the confidentiality to the

data. Thus, to overcome these limitations of traditional system [3], rather than using symmetric algorithm, asymmetric algorithm-Elliptical curve cryptography (ECC) is implemented and for key generation, Diffie-Hellman is applied into the system in order to acquire data privacy.The proposed system takes two types of users: patients and doctors. To sign up in the system, along with their personal information user image i.e. thumb/palm print is stored into the data base. These biological prints are the base of the encryption as they act as different keys to implement Diffie-Hellman algorithm for encryption and decryption of the data. The Diffie-Hellmanalgorithm used in the proposed system is as follows:

- *Public: g and p*
- *Secret key: thumb/palm print of patient A, doctor's thumb/palm print B (both in binary form)*
- *Patient send* $g^A(mod\ p)$ *and doctor send* $g^B(mod\ p)$
- *Patient computes :* $(g^B)^A = g^{BA} = g^{AB}(mod\ p)$
- *Doctor computes* $(g^A)^B = g^{AB}(mod\ p)$

The doctor will be assigned to the patient just after the registration process. Further, the patients are able to only view their health status and doctors can see and manage the information of all their patients. Thus when doctor log into the system, he/she will get the encrypted view of the selected thumb/palm print is used as the key. The access is granted to the doctors after identification of their thumb/ palm print. Encryption of the data is performed using ECC algorithm and doctor will be able to see the health status of patient.

The pseudo-code for ECC algorithm used in this proposed system is as follows:

- *Key exchange between user A and B*
- *Must first encode any message M as a point on the elliptic curve Pm*
- *Select suitable curve & point G as in D-H*
- *A chooses private key n_(A)<n*
- *To encrypt P_m to B:*
- *C_m={ kG, 〖P 〗_m+ kP_B}*
- *where k is a random positive integer chosen by A*
- *To decrypt C_m, B computes:* $P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$

VI. RESEARCH METHODLOGY

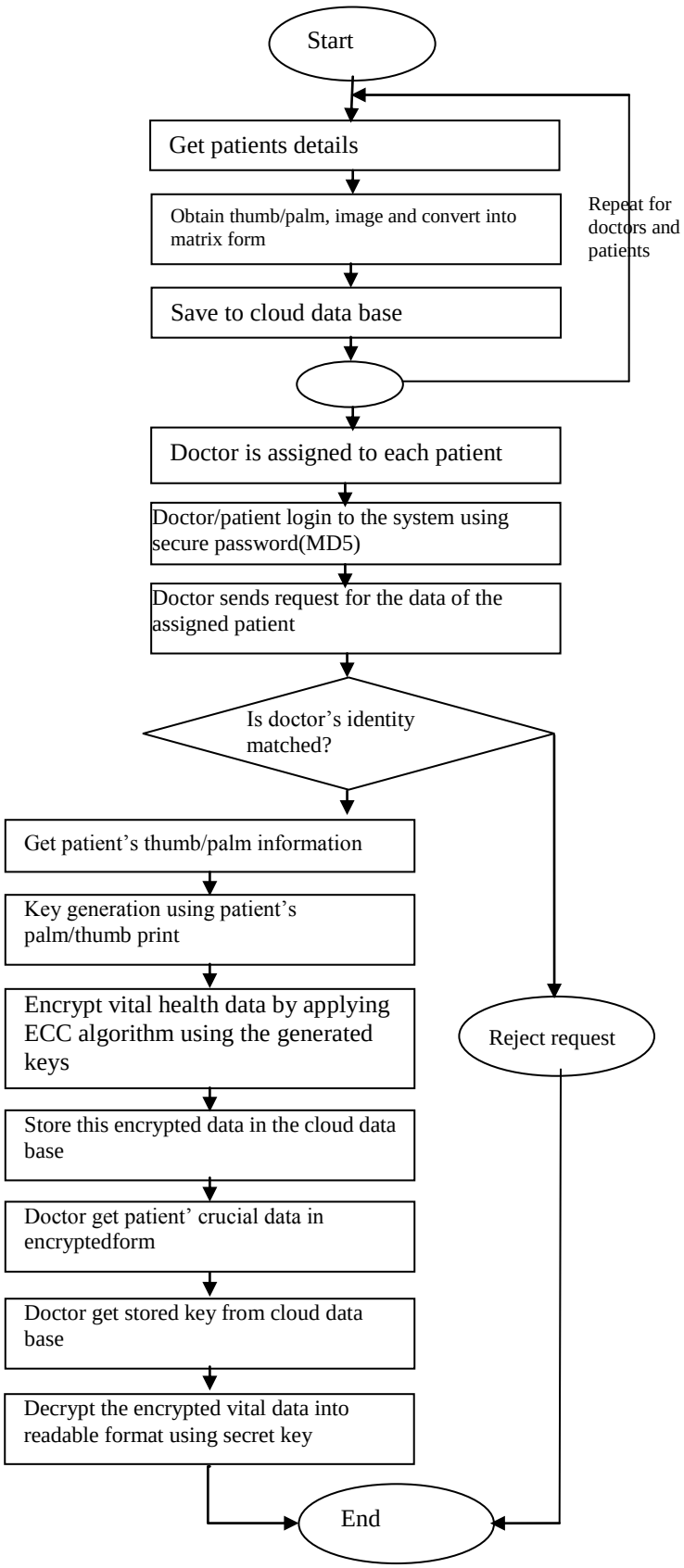
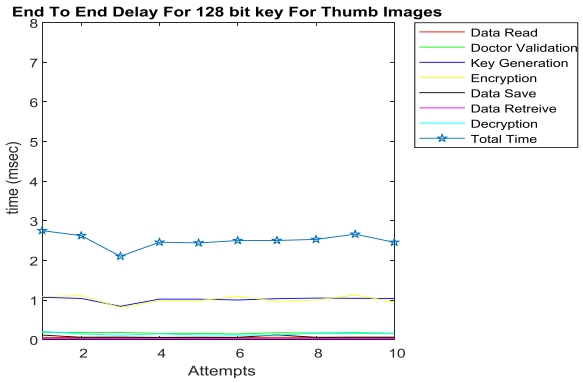


Figure 2: Workflow of proposed system

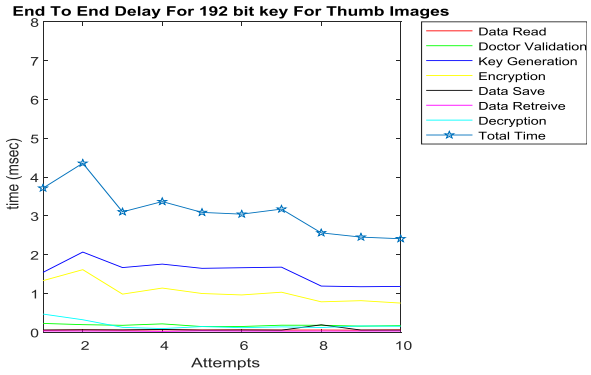
VII. EXPERIMENTAL RESULTS

We applied Elliptic Curve Cryptography (ECC) in the proposed work in which biometric authentication such as thumb/palm print is the major section for generating keys which are used in ECC. Different aspects are taken into consideration while performing the experiments. To use the images of thumb/palm print, we converted them into binary form. The system was evaluated on the basis of varying key sizes, thumb/palm prints and comparison of traditional and proposed system. Three different key sizes- 128,192 and 256 bits were considered during experimental simulation. The factors included for evaluation of the system are validation time of doctor's thumb or palm print, time to read the data, Encryption time, time to save the data, key generation time, time to retrieve data and decryption time.

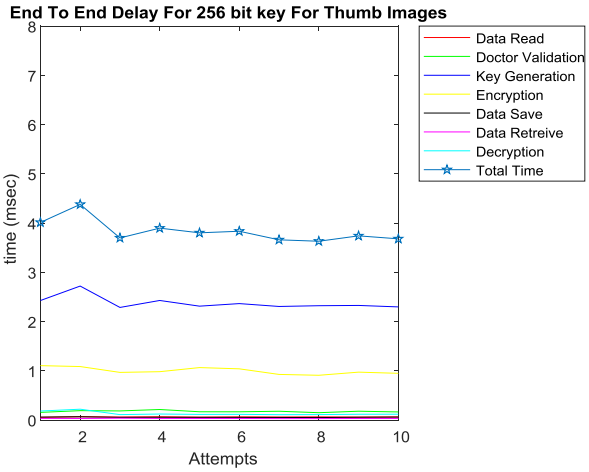
Figure 3 demonstrates the end to end lagging of safe communication of the data of patient in the traditional system using different key sizes which are obtained from patient's thumb prints. The graph is representing the time delay with respect to the number of attempts. Total 10 attempts were made to analyze the time delay. Taking into account all the mentioned factors, it takes 2 to 3 milli-seconds to perform all the processes. When 192 key bit key is used, as shown in figure (b) it took 4-5 milliseconds in the beginning and then decreased to the range 2-3 milliseconds. In figure (c), the graph represented the results using the key with 256 bits of size. Just as in the case (b), the time is increased in the initial attempts and then becomes consistent and time remains between 3-4 milli-seconds.



(a) Key size-128 bits

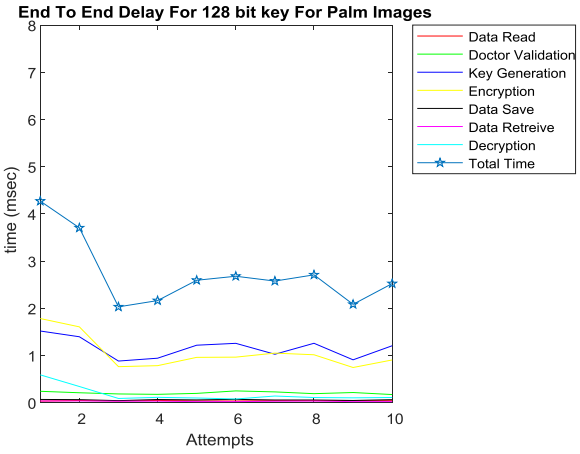


(b) Key size-192bits

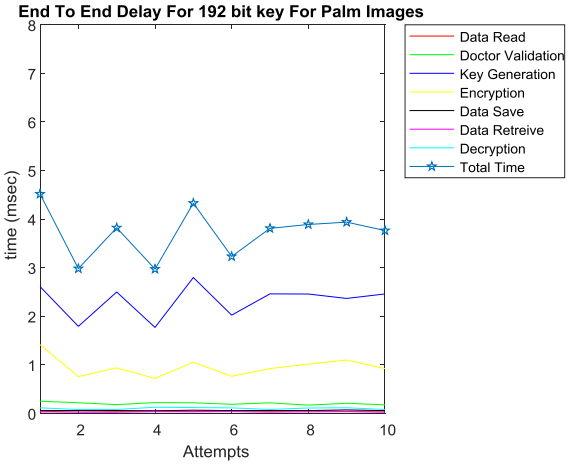


(c) Key size-256 bits

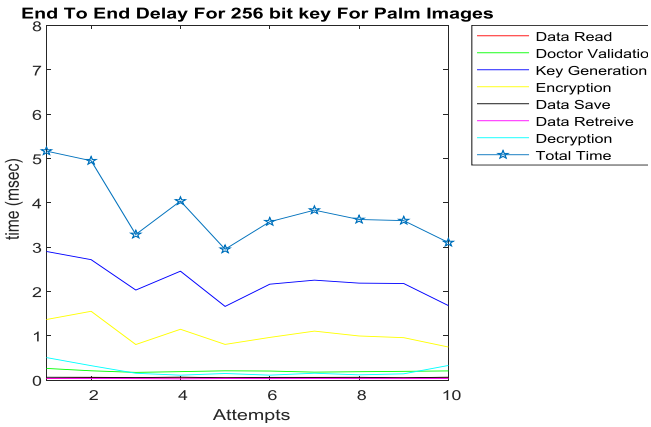
Figure 3: End-to-end delay of secure health data transmission using (a) 128 bit key (b) 192 bit key & (c) 256 bit key generated from patient's thumb image in the old system.



(a) Key size-128 bits



(b) Key size-192bits



(c) *Key size-256 bits*

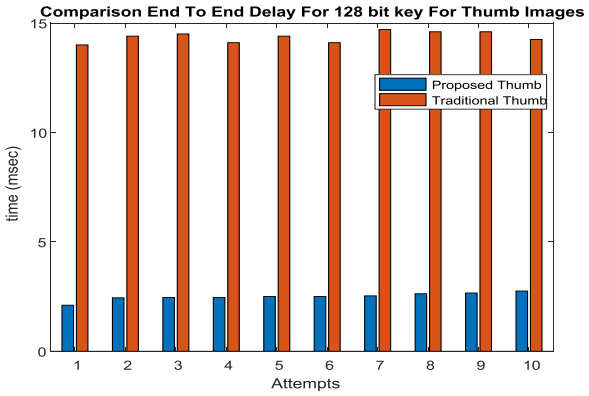
Figure 4: End-to-end delay of secure health data transmissions using (a) 128 bit key (b) 192 bit key &(c) 256 key bit generated from patient's palm image

The time lagging of traditional system using palm image is delineated in figure 4. It also represents the end-to-end time delay of different key sizes. These keys were generated from patients palm print. Time consumed for palm print is comparatively more than that of process done using thumb print. In all the cases-(a), (b) and (c), the time delay is high when initial attempts were made and it decreases as the number of attempts decreased. The time delay lies between 2-3 milli-seconds, 3-4 milli-second and nearest to 3 milliseconds when there are 128, 192as well as 256 bits of key size respectively.

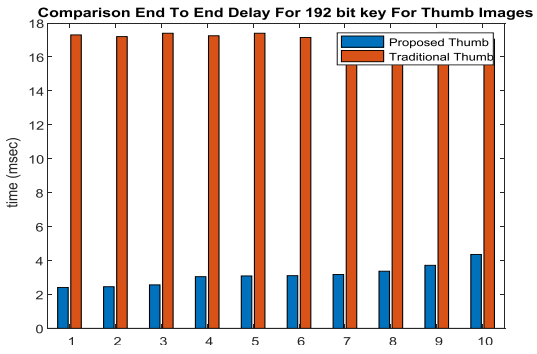
Comparison of proposed and traditional system throughout the security transmission delay using thumb and palm images with different key sizes:

After analyzing the traditional system, evaluation of the proposed system is performed and the results were compared with traditional system's outcome.

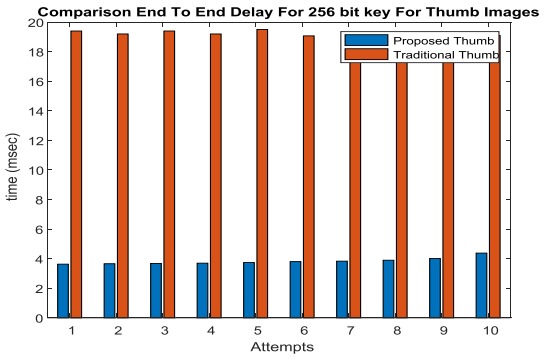
The comparative view of both proposed and conventional system is demonstrated in figure 5. The graph illustrated the end to end time delay in milliseconds among different number of the attempts.



(a) Key size-128 bits



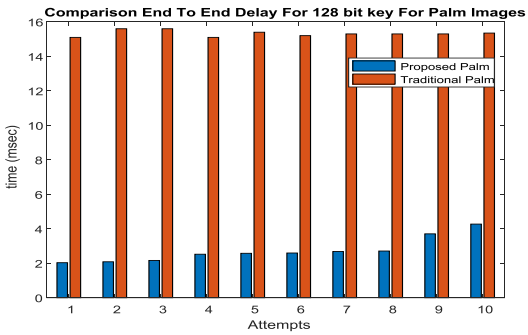
b) *Key size 192 bits*



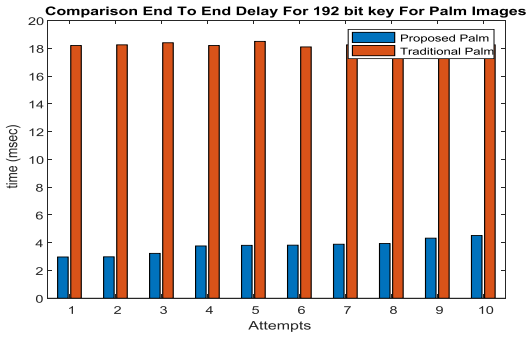
(c) *Key size-256 bits*

Figure 5: comparison of proposed and traditional work using thumb images

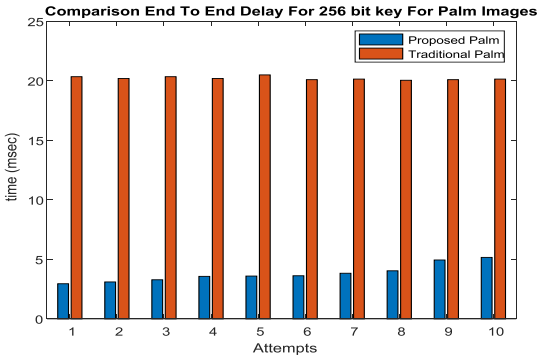
As it can be clearly seen that the time delay of traditional system is very high in all the cases, the maximum time delay in existing system is 15ms, 18ms and 20ms in 128, 192as well as 256 key size bits respectively and the proposed system has very less delay time in performing all the process.It only takes up to 3ms, 5msand 5ms for key size 128, 192 as well as 256 number of bits respectively. Thus, from this comparative analysis, the proposed system is providing secure data transmission in very les time which makes it to be used in an effective manner.



(a)*Key size-128 bits*



(b)*Key size 192 bits*



(c)*Key size-256 bits*

Figure 6: comparative analysis of traditional and proposed system using patient's palm prints for end to end encryption

The analysis of proposed system in terms of palm prints is compared with existing system. The outcome obtained is illustrated in figure 6. The time varies in all the three cases for traditional system. Time delay of existing system is much more that of proposed system. For 128 bits, 192 and 256bits key size, the maximum time used is 15ms, 18ms and 20ms respectively in traditional and maximum time for all these cases in projected work is 5ms which shows a bigger difference. Thus, lower the time delay more efficient will be the system and proposed system is also effective when palm images are used to provide data confidentiality.

The simulation results of comparative analysis are recorded and their average value is shown in the tabular form, table 1 consists of average values of both palm and thumb based data authentication for different5 key sizes those are 128,192, 256.

Table 1: Comparative analysis at different key sizes

Key Size	Traditional Palm	Proposed Palm	Traditional Thumb	Proposed Thumb
128	153.25	2.733	14.365	2.504
192	18.23	3.72	17.265	3.127
256	20.215	3.811	19.21	3.832

VIII. CONCLUSION& FUTURE SCOPE

In this paper, the work is done to achieve more data security and privacy in WBAN. Biometric authentication enhanced by using Diffie-Hellman algorithm. AES algorithm for encryption was changed with Elliptic Curve Cryptography (ECC) in which three different blocks of keys – 128, 192 as well as 256 bits were used in cryptography. From the experimental simulations, it was observed that proposed system took less time than the existing system. It provides more security to the data. Moreover, the authentication process using palm print is more effective as it is more secure. Thus, the proposed WBAN system is effective and offers stronger authentication, security, privacy to the sensible and delicate information regarding the patient's health in hospitals and medical clinics.For future perspective of this system, the data security and integrity can be enhanced and complexity can be reduced by using the hybrid model for biometric authentication system.

REFERENCES

1. Otto, C., Milenkovic, A., Sanders, C., &Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. Journal of mobile multimedia, 1(4), 307-326.
2. Khan, J. Y., &Yuce, M. R. (2010). Wireless body area network (WBAN) for medical applications. In New developments in biomedical engineering. Intech Open.
3. Arfaoui, A., Kribeche, A., &Senouci, S. M. (2019). Context-Aware Anonymous Authentication Protocols in the Internet of Things Dedicated to e-Health Applications. Computer Networks.
4. Dodangeh, P., & Jahangir, A. H. (2018). A biometric security scheme for wireless body area networks. Journal of Information Security and Applications, 41, 62-74.
5. Karmakar, K., Saif, S., Biswas, S., &Neogy, S. (2018, January). WBAN Security: study and implementation of a biological key based framework. In 2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT) (pp. 1-6). IEEE.
6. Arefin, M. T., Ali, M. H., & Haque, A. F. (2017). Wireless Body Area Network: An Overview and Various Applications. Journal of Computer and Communications, 5(07), 53.
7. Manirabona, A., &Fourati, L. C. (2018). A 4-tiers architecture for mobile WBAN based health remote monitoring system. Wireless Networks, 24(6), 2179-2190.
8. Masdari, M., Ahmadzadeh, S., &Bidaki, M. (2017). Key management in wireless body area network: Challenges and issues. Journal of Network and Computer Applications, 91, 36-51.
9. Negra, R., Jemili, I., &Belghith, A. (2016). Wireless body area networks: Applications and technologies. Procedia Computer Science, 83, 1274-1281.
10. Kompara, M., Islam, S. H., &Hölbl, M. (2019). A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. Computer Networks, 148, 196-213.
11. Raazi, S. M. K. U. R., Lee, H., Lee, S., & Lee, Y. K. (2009, December). BARI: A distributed key management approach for wireless body area networks. In 2009 International Conference on Computational Intelligence and Security (Vol. 2, pp. 324-329). IEEE.
12. Barakah, D. M., &Ammad-uddin, M. (2012, February). A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In 2012 Third International Conference on Intelligent Systems Modelling and Simulation (pp. 214-219). IEEE.
13. Wang, H., Fang, H., Xing, L., & Chen, M. (2011, June). An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN). In 2011 IEEE international conference on communications (ICC) (pp. 1-5). IEEE.
14. Ali, A., & Khan, F. A. (2013). Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. EURASIP Journal on Wireless Communications and Networking, 2013(1), 216.
15. Ali, A., & Khan, F. A. (2013). Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. EURASIP Journal on Wireless Communications and Networking, 2013(1), 216
16. Arfaoui, A., Kribeche, A., &Senouci, S. M. (2019). Context-Aware Anonymous

Authentication Protocols in the Internet of Things Dedicated to e-Health Applications. Computer Networks.
17. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., &Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2), 113-122.
18. Pramanik, P. K. D., Pareek, G., & Nayyar, A. (2019). Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. In Telemedicine Technologies (pp. 201-225). Academic Press.
19. Chukwunonyerem, J., Aibinu, A. M., Onumanyi, A. J., Ugweje, O. C., Onwuka, E. N., Alenogbena, C., &Ezechi, N. (2016). Development of key generation algorithm using ECG biometrics for node security in wireless body area sensor network. European Research in Telemedicine/La Recherche EuropéenneenTélémédecine, 5(4), 7-144.
20. Selimis, G., Huang, L., Massé, F., Tsekoura, I., Ashouei, M., Catthoor, F., ... & De Groot, H. (2011). A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. Journal of medical systems, 35(5), 1289-1298.
21. Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003, October). Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In 2003 International Conference on Parallel Processing Workshops, 2003. Proceedings. (pp. 432-439). IEEE..

AUTHORS PROFILE

Sandeep Ranais a M.E. Research Scholar at Department of C.S.E., University Institute of Engineering, Chandigarh University (CU), Gharuan (Mohali), Punjab, India. His specialization is in Software Engineering field. He received His B.Tech degree in Computer Science Engineering from Chandigarh university, Gharuan (Mohali) in the year of (2013-2017), and pursuing his M.E. in CU in present. He is doing his project in the field of Wireless, titled as, "Implementation of biological key based security technique in wireless body area networks".

Dr. Sandeep Singh Kangis working as a Professor in Computer science & Engineering at Chandigarh University Gharuan (Mohali), Punjab(India). He did his B.Tech, M.Tech and Ph.D in Computer Science and Engineering. His fields of specialization are Computer networking, network communication, Wireless sensor networks, Network Security, network simulation, software testing and steganography. He has 16 years teaching experience in the field of engineering education. He has published 70 Research papers in International/National Journals and Conferences. He has published one book on Network Security. He is the life member of ISTE.