ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Secure Data Authentication Scheme for Wban Using Fully Homomorphic Encryption Algorithm

[1] C.Rameshkumar, [2]M. Arvindhan, [3]Dr.R.Viswanathan
[1][2] Assistant Professor, [3]Associate Professor
[1][2][3] Galgotias University, Uttar Pradesh, India

Abstract: The Wireless Body Area Network (WBAN) is a type of wireless sensor network that is connected to various sensors of clothing and human body and skin planted. In organize to make sure data security; data storage in encrypted text format sink data encryption uses encrypted text attribute sensors. The major challenge of the wireless body surface is to create secure communication with the sensors and data sink data available to third parties, taking care of the current concerns about safety and information protection. There is no adequate security mechanism in the personal monitoring scheme for data security data security. This article will be developed by the algorithm of fully homomorphic encryption of communication with a secure channel between data sink and third-party access and methods for monitoring surveillance of healthcare by way of telecommunication system implantable devices to facilitate do not affect the mobility of patients. This algorithm are used to securely retrieve the sensitive data from the despreading device to data and instruction sensors wireless body surface. Ensures the authenticity of communication and impact resistance and evaluates energy consumption and calculation costs.

Keywords:Wireless body area network, Secure communication, fully homomorphic encryption.

I. INTRODUCTION

In recent years, the patient health surveillance system was an innovative wireless communication technology in modern medical devices. The wireless body is powered by leading electronics, mobile communication, wireless communication, portable batteries, and sensors. In wireless regions, network gadgets such like pacemakers, coronary heart defibers, insulin pumps, and neurostimulators. Health-related health observation nodes can be captured and implanted from the outside, which serves to monitor the oxygen saturation bioparameters in the blood. By using these biometric parameters, sensors collect personal health information used in industrial services to identify personal identification and health indicators. The real-time monitoring and reporting system of patients' health is advanced microelectronics technology [1]. The wireless network attempts to meet the requirements of miniaturization, low complexity, and energy efficiency. The wireless wireless network increases the patient's comfortable health care system to remotely monitor the health of patients and reduce the problem of cables [2].

Reliable installation of the wireless communication system in the wireless body is not currently fully protected. Data on implantable devices and sensors stored in the data logger can be easily compromised by using the cryptographic hash function, symmetric encryption algorithms, and decoding algorithms [3]. The implanted sensor collects sensitive data and important patient information that provides greater security, confidentiality, and security. The sensor collects data and entitles authorized doctors and performs secure communication channels. BAN performs a symmetric encryption system. The system is not the ideal channel. The only option for a secure communication system is the high computing cost asymmetric coding system [4].

A new fully homomorphic encryption system is recommended to solve the problem of secure communication and provide the necessary security features. These systems provide a secure data communication system for data washer and third-party access systems. The schema belongs to asymmetric encryption. The access structure provided access data to the sensors [5]. For example, by building an access structure, a physician or a specialist of a given heart surgery center may have access to the information you need. The data collected from the sensors is stored in the data channel the encrypted text. Data seal has no permission and encryption key for stored encrypted text. Our contribution can be summarized as follows:

•Only the work was done by authorized doctors and experts to have secure access to patient information
•Encrypted access control, based on roles, is encrypted and signed. The sensor can regulate authorized access rights and create an access structure for the data

•Companion data in the data channel do not show people when the data is corrupted
•Implementing the proposed system is an assessment of energy consumption and cost calculation and Evaluate doctors' access to homomorphic algorithms

The rest of the description is organized seeing that follows. Section 2 presents the motivation of the learning and summarizes the interrelated work. Section 4 introduces the system model as well as develops the basic idea of communication protocols during Section 4. Section 5 analyzes the security of the proposed protocol and presents the performance laboratory analysis described in Chapter 6.

2. MOTIVATION AND LITERATURE SURVEY

A. Motivation

The state of the system is a BAN on the storage of data assets management of data, such as PDA mobile devices should be available to a large number of third parties; senior doctors who consulted patients and doctors are required to daytime nurses can take part in the hospital. Different third User parties have different access rights when the patient sends them to another hospital. Hereafter, a mechanism BAN is a technical challenge: it needs to know how to properly keep it access rights to medical personnel while providing access to sensitive patient data. To overcome this challenge, homomorphic encoding algorithm regulates access rights to protect users and information, the sink should not risk theft or compromise control data and control access to the BANs [5].

B. Related work

In this section, we do the existing research with the appropriate problems and solutions. Different devices in the wireless sensors can be used in the BAN. It can provide communication in BAN and BAN authentication encryption. An existing security, the communication system may include data encryption; access methods and digital signatures. Attribute-based encryption can refer to electronic medical records that can provide self-sufficient protection for mobile devices and can be used for offline communication. The security and confidentiality of patient records in the data wash can easily endanger the access by third parties. Existing research can be useful for the work presented in these documents, which we handle in the field of telecommunications network security.
Chunqiang Hu et al. [6] Have shown that role-based access control allows access to the access tree for data users. For secure communication in the body area, the encrypted text attributes is based on a policy attribute that can be used for effective data communication. Their data security for data carriers require adequate and safe security and requires effective encryption approach with fewer calculations.

Halperin et al. [7] analyzed the safety and integrity of commercially available cardiovascular defibrillators (ICDs). Many radio-based attacks are identified that could endanger the patient's security and privacy.

Meng Zhang et al. [8] show that tolerance does not provide communication with the reliability of medical devices. By this method, you can have malicious attacks by increasing IWMDS programming options and network connections. Functional complexity is high within wireless communication, the high authority utilization of the MAC layer can be achieved. The results show that a low energy optimization system has been used for wireless connectivity and has developed a number of easy communication protocols.

Chan et al. [9] discovered a technique identified by the designation of q-combined keys and which provided two sensors with the consent to create only a double key if at least "q" shared keys were shared. Chana para. also extended the system with random paired keys to avoid the formation of node capture attacks

Perrig et al. [10] offer a security architecture known as SPINS and which consists of SNEP and TESLA (SNAP) protocol syntax. In this architecture, SNEP secured the confidentiality of data, while the combination of TESLA and SANP verified the broadcast data. The entire architecture is designed to allow each sensor node to share a secret key with the base station. by the Perrig structural design, two sensors cannot distribute a secret key awaiting the key is shared through the base location. The base location acts while a dependable third party among the sensors.

Traynor et al. [11] showed a likelihood of uneven distribution of keys to the networks that favor a small percentage of the sensor's ability not only to achieve the same level of security but the consequences of compromising compromises in nodes.

K. Lou and everyone. [12] A key driver for the analytical circle is a heterogeneous sensor network. The advantage of this system is as follows: (i) the minimum requirement for storage process is a key production and (ii) a small number of keys generate instead of generating a large number of random keys. Establish a Keychain using Keychain function, and then use the key tool used to collect extra circuits.

F Kausar et al. [13] proposed a procedure for key management heterogeneous sensor networks, in which a key piece is assigned to sensors H where one of the keys to this key is assigned to Sensor 1, the end result is this limited power consumption of the files and the full network connectivity. PV vary by person, which shows the uniqueness of each individual because of this fact, he has introduced for security purposes.

S.D. Bao et al. [14] proposed a technique in which PV was used to authenticate the enterprise. The main task of Bao's technique is to collect and transmit a process. The data you send will be sent to a different authentication or recognition sensor using a secure channel.

K. Venkatasubramanian et al. [15] is a technique known as the ECG-based key convention system, using FFT (Fast Fourier Transform). As the FFT calculation cost is subtracted, this is O (nlogn).

Aftab et al. [16] showed that the key generator phase of the sender is occurring before the blocks. Blocks were first cleared using SHA-256, and a watermark was placed in the splint blocks using fingerprints, as with any machine. Random numbers generate with a random machine were used as the position of watermarks happening the sender's side. The same process takes the watermark from the receiving party's blocks.

Lav Gupta et al. [17] is a powerful symmetric encryption method for the WBAN system. This method shows the poor quality of the service and the cryptographic energy cost of the elliptical curve has to be reduced. The study of the aforementioned study shows that the security and confidentiality of data communication between the third party access and data entry are ineffective. We need an effective algorithm or technique to overcome the security and confidentiality of the WBAN system data communication, homomorphic encryption is proposed. Allows you toward calculate programmed data. Your data will remain extremely confidential while doing additional operations, so you can do a useful job of staying in an untrusted environment. Performs a specific type of calculation that is executed on encrypted text and creates an encrypted result that can be decrypted according to the result of the action in the text.

3. SYSTEM MODEL

See the BAN communication system shown in Figure 1. There are four major units in the scheme: Key Generation Center (KGC), Sensor (implanted and moveable devices), Data Sink (BAN data manager or mobile device like a smartphone) and Data consumer (doctors or nurses). The following subsections summarize the fundamental functions of every component.

A.The Key Generation Center

The Key Generation Centre runs the key creation with public parameters, initializes the method, and assigns a secret key to all attributes to the user sets. Before placing the sensors in the human body, he first installed the public parameters in the sensors. The key generator generates a secret key for each attribute and the user must prove the Keyword Generation Center. The secret key will be created for the data user individually, which can be generated by random numbers to prevent secret attacks. Once the user data has to match the access tree, the secret key can encrypt the message

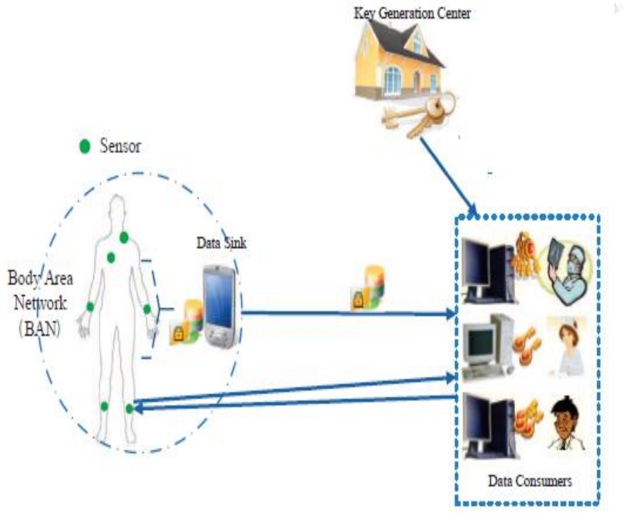

Fig. 1. A BAN architecture of a healthcare application.

B.Implanted and wearable sensors

The BANs contain wireless sensors that are used by the Body Area Network. The wearable devices can embed on the surface and embed into the deep tissue of the human body. These sensors are used to monitor body parameters and exercise and control the human body by providing vital visual and audio feedback and so on. BAS can be used in many applications, healthcare, military combat support, and athletic training.

C.Data sink

Data input is BAN or mobile device control. It is used to store patient data. Encrypted encryption is required to encrypt and store data in the data storage. The user retrieves the data and decodes the session buttons with the corresponding specified functions.

In the existing system, the data collector checks the authentication status to query the encrypted data request, which is then sent to the user. If the device is stolen or physically damaged, or a third-party attacker can download the data with memory. In the proposed scheme, the encrypted text data of the data seal enables the homomorphic encryption technique to be recorded, and the calculation is performed in encrypted data. Finally, the result is sent to the encrypted user. Using these methods, the harmful application does not affect the original data, but also the encrypted data. Based on the analysis in the study, it is assumed that the data drive is not compromised by the unauthorized access of third parties.

D.Data Users

Physicians, nurses or other experts are called data users. Data users must have the attribute that is suitable for decoding data input data. The attribute values and the secret key are collected by the key generator. Attribute values are public parameters. The secret key is randomly generated by the KGC (Key Generation Center), using the random number for each key value.

4. PROPOSED SCHEME

Homomorphic encryption is an encryption coding algorithm that allows definite calculations to be performed on ciphertexts with creating an encrypted consequence. The decoded result coincides with planetary operations. RSA can process random bits before encryption. the various public key encryptions have been proposed for homomorphic properties designed for many decades. The homomorphism is a composition that holds the record relating two algebraic structures, such like groups.assume with the aim of the public key Pkey = (x,y), the plaintexts variety a group (G1,*), and the ciphertexts form a group (G2,*),wherever * is the modular multiplication. For any two plaintexts PT1, PT2 in G1, it holds this

$$E(PT_1, P_{key}) * E(PT_2, P_{key}) = PT_1^e * PT_2^e \ (mod\ n)$$
$$= (PT_1 * PT_2)^e \ (mod\ n)$$
$$= E(PT_1 * PT_2, P_{key})$$

A.Fully Homomorphic Encryption

The first completely homomorphic encryption system, published in [5]. This concept is based on a lattice-based cryptographic system that is based on a homomorphic form, a fixed number of operations can be performed there. The open way of switching from SHE to FHE can be bootstrapping. The Gentry system proved to be ineffective in practice because of the huge costs of computing and memory.

For example, if the scheme has the following property: with

C1 = Enc(txm1) and C2 =Enc (txm2)
txm1+ txm2 = Dec (C1+ C2)

it is said to be homomorphic. Both the homomorphic scheme is called homomorphic for both dosing and multiplication.

B..Brakerski-Gentry-Vaikuntanathan homomorphic encryption scheme

This is the propose and performance of the software library system. This encryption system, along with a number of optimization techniques, launches faster evaluation methods and focuses on the effective use of text encryption techniques. Two versions of the cryptosystem deal with full vectors with the rigidity of the LWE solution and deal with the number of polynomials that depend on the rigidity of the R-LWE key. BGV is an asymmetric encryption system used to encrypt bits.

Encrypt (PlainText Mt, Public Key Pkey): CipherText Ct
Decrypt (CipherText Ct, Private Key PRkey): Plaintext Mt
Level shifting operations:
Rescale (CipherText Ct): CipherText Ct
Switch Key (Augmented CipherText Ct): CipherText Ct
Homomorphic operations:
Add (CipherText Ct1, CipherText Ct2): Cipher Text Ctsum
Mul(CipherText Ct1, CipherText Ct2): CipherText Ctcmul

5. PERFORMANCE ANALYSIS

This section presents a quantitative efficiency test. The major goal of the development is energy Consumption used to analyze as well as convey messages. Since the size of the message is directly related to the power consumption of the message transmission, which is linearly proportional to the size of the message, it begins with an analysis of the size of the message.

A.Message size

The communication protocol between the data user and the data channel when the data user and the physician first provide access to the data will receive the session key. You can then calculate the total amount of decrypting messages. Then a data transmission channel is created, the message size is 18 bytes. To establish a connection, the system requires a large message size while the message size of the communication between the user and the data sensors is low. So the size of the message is determined by the level of protection. The connection is established, the message size is independent of the level of protection.

B.Communication overhead

The data user wants to empty data to transmit stored encrypted text data. Thus, communication costs are mainly related to the amount of encrypted data. Communication is created by establishing a connection. Costs are increased by the data security level. decrease the sum of encrypted information to corresponding with communication overheads is shown in fig-2.

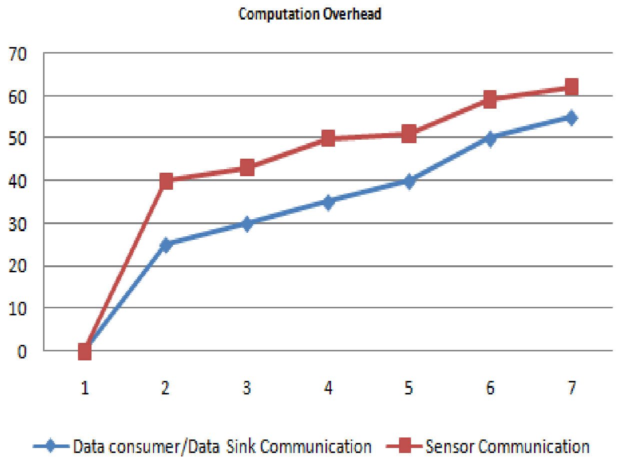

Fig : 2 Computation Over head

C.Computational Cost

In the existing method, cost calculation is primarily due to the total cost. In this proposed system, the cost of calculating communication between data consumption data and dishwashers is primarily due to the different pairing processes. After the communication connection is established, the user does not have to pair, the process closes and the new process is updated. The proposed system has low power consumption compared to other circuits. This is the most common technique method is shown in fig-3.

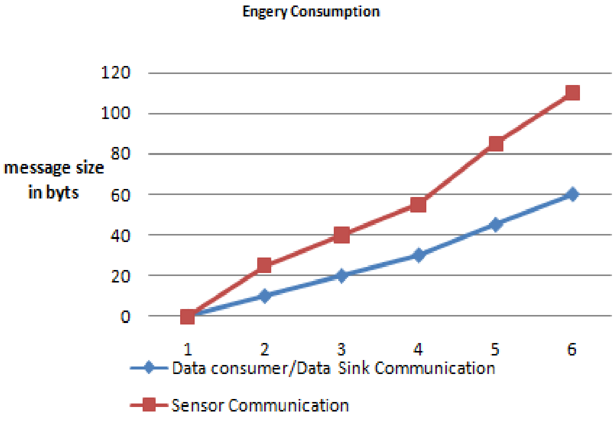

Fig 3 : Energy Consumption

6. CONCLUSION

This proposed system means developing more efficient encryption methods with less computing costs and storage requirements that would better match the practical situation of the Bulgarian Academy of Sciences. The challenge is to reduce the cost of calculating better use of the BAN. This is an effective encryption method that is used in too many encryption techniques. The data user can satisfy the access and security access required for the stored text. This article can be useful to understand that the cryptographic algorithm is used in the body network used to complete the homomorphic encryption technique to preserve privacy.

REFERENCES

[1]. S. Ali, V. Sivaraman, and D. Ostry, “Zero reconciliation secret key generation for body-worn health monitoring devices,” in ACM Wisec.ACM, 2012, pp. 39–50.

[2]. L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: body area network authentication exploiting channel characteristics," in ACM Wisec. ACM, 2012, pp. 27–38.

[3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4]. C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, “Securing communications between external users and wireless body area networks,” in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[5]. Gentry, Craig. A fully homomorphic encryption scheme. Stanford University, 2009.

[6]. Chunqiang Hu, Hongjuan Li, Yan Huo, Tao Xiang and Xiaofeng Liao "Secure and Efficient Data Communication Protocol for Wireless Body Area Networks" IEEE vol. 2, no. 2, April-June 2016.

[7]. D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[8]. Meng Zhang, Anand Raghunathan and Niraj K. Jha,"Trustworthiness of Medical Devices and Body Area Networks". Proceedings of the IEEE |Vol. 102, No. 8, August 2014.

[9]. H. Chan, A. Perrig, and D. Song,"Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy, May 2003, pp. 197–213.

[10]. A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler, "Spins Security protocols for sensor networks," in Seventh Annual Int'l Conf. on Mobile Computing and Networks, July 2001.

[11]. P. Traynor, R. Kumar, H. B. Saad, G.Cao, and T. L. Porta, "Establishing pair-wise keys in heterogeneous sensor networks," in INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, 2006, pp. 1–12.

[12]. K. Lu, Y. Qian, and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks," in IEEE International Performance Computing and Communications Conference, 2006, pp.513–519.

[13]. F Kausar et al "Key Management and Secure Routing in Heterogeneous Networks"- IEEE International Conference on, 2008 - computer.org.

[14]. S. D. Bao, Y. T. Zhang, and Y.-T.Zhang:"Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems, September 2005, pp. 2455–2458, In Proc. Of the IEEE 27th Conference on Engineering in Medicine and Biology.

[15]. K.Venkatasubramanian, G. Deng, T.Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta. Ayushman.: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed. In Distributed Computing in Sensor Systems, pages 406-407, July 2005.

[16]. Ali, Aftab, and Farrukh Aslam Khan. "An improved EKG-based key agreement scheme for body area networks." In International Conference on Information Security and Assurance, pp. 298-308. Springer, Berlin, Heidelberg, 2010.

[17]. Gowtham, M., and S. Sobitha Ahila. "Privacy enhanced data communication protocol for wireless body area network." In Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, pp. 1-5. IEEE, 2017.