DOI: https://doi.org/10.24113/ijoscience.v6i11.349

Secure Elgamal Based Authentication Scheme for Cloud Assisted IOT Based Wireless Body Area Network

Vineeta Shrivastava
M.Tech Scholar
Department of Computer Science & Engineering
Sagar Institute of Research & Technology
Bhopal, M.P, India
shrivastavavinita21@gmail.com

Mayank Namdev
Assistant Professor
Department of Computer Science & Engineering
Sagar Institute of Research & Technology
Bhopal, M.P, India

Abstract: **Now-a-days ireless Body Area Network (WBAN) is considered to be new era technique in which patient's health record are monitored remotely by using wearable sensors from anywhere in the world. In such high-level communication, there is need of security services are required to protect the data being used by healthcare professionals and patients from intruders or attackers. Therefore, many researchers are showing their keen interest for security enhancement of WBAN architecture for secure communication. In this dissertation work, different security and privacy techniques are reviewed and analysed WBAN/IoT challenges as well their limitations based on the latest standards and publications. This research also covers the state-of-art security measures and research in WBAN. This research presents an ElGamal cryptosystem and biometric information authentication scheme for WBAN/IOT applications. This work observed that most of the authentication protocols using hash function and ElGamal cryptosystem for cloud-based applications are affected by security attacks and are unable to hide the actual identities of the end users during login session. Therefore, this work has introduced a secure biometric ElGamal-based authentication as well as data sharing schemes. The result analysis shows that the proposed work is better with respect to existing work with respect to execution time and cost as well as security level.**

Keywords: Wireless Body Area Network, Data sharing, Data confidentiality, Security, ElGamal, Biometrics

I. INTRODUCTION

A Body Area Network (BAN) is a short-range wireless network consisting of devices positioned inside, above and around the body. It offers data communication over short distances, limited to distances of a few meters. Figure 1 shows the basic concept. This new type of intrinsically personal network uses portable and implanted electronic circuits. It implements extremely useful functions and capabilities in practical and discrete configurations that operate with very low energy consumption and offer exceptional security [1].

The number of technical products used by one person, a desktop computer, a laptop, a tablet, a mobile phone has increased considerably and one person often uses multiple products on a regular basis. Other products are implanted in humans to monitor various bodily functions and conditions, as well as the environment [2].

The sensor nodes are positioned directly on the body or under the skin of a person to record certain body parameters such as the electrocardiogram (ECG), the electroencephalogram (EEG), body movements, temperature, blood pressure, blood sugar, heart rate, respiratory rate, etc. [3]. These sensors are designed for specific purposes to meet the requirements. For example, an EEG sensor should monitor electrical activity in the brain. Another example is the ECG sensor, developed to monitor cardiac activity.

II. LITERATURE REVIEW

Kim et al. [4] proposed a secure and lightweight mutual authentication and key establishment scheme using wearable devices to resolve the security shortcomings. The proposed scheme can be suitable to resource-limited environments.

Jiang et al. [5] proposed an optimized system for deep distributed learning which includes a cloud server and several smartphones with IT functions. Each device is used as a personal mobile data hub to enable mobile computing while protecting data protection. The proposed system stores private data locally on smartphones, shares the settings formed and creates a global consensus model. The feasibility and usability of the proposed system are assessed through three experiments and the related discussion. Experimental results show that the proposed

distributed deep learning system can reconstruct the behaviour of centralized training.

Pandey et al. [6] presented a state-of-art survey about various features of BAN specifically communications, sensors, applications, requirements, standards & protocol, and security aspects.

Meng et al. [7] proposed a new anonymous mutual authentication and key agreement scheme, with untraceability and session key forward secrecy. The scheme uses as few hash functions and XOR operations as possible for authentication and key agreement. It is officially proven to be correct through BAN logic, and its security has been verified by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) as well.

III. OBJECTIVES

To solve the mentioned problems in previous schemes, an algorithm is proposed for secure authentication system for WBAN/IOT.

- A secure authentication and key agreement scheme for cloud-assisted WBAN/IOT system is proposed. Therefore, only authorized users have ability to access information and the proposed system can ensure user's privacy and data integrity.
- From the execution of the proposed procedures, the system reduces the burden on some computations and is suitable for implementation in the current mobile environment.

IV. PROPOSED METHODOLOGY

For secure cloud-assisted IOT application, three roles participate in this system: the user (U), the cloud-service centre (CSC) and the Authenticator (A). Before accessing the system, every participant must register with the CSC and it will issue one specific certificate to access data files in WBAN/IOT.

- Step 1. The user U goes to the Authenticator to take authentication permission to access or upload a file.
- Step 2. The user uploads his/her biometric information in encrypted form to the Authenticator (A) and A will authenticate previously registered user. If not registered then make a registration and store information.
- Step 3. A authenticate user and redirect user U to CSC.
- Step 4. The user U can either upload a new file or access existing files. For accessing other file he has to provide some accessing parameters and accessing license will be provided to the user for a specific time limit.
- Step 5. The authorized user U can access files stored in cloud center.

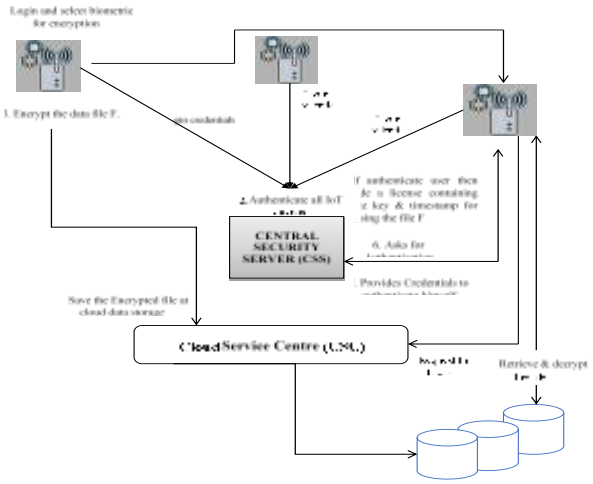

Fig. 1 Flow Chart of Proposed Work

As more and more organizations and individuals tend to outsource their data to cloud storage, the security and user privacy protection attract more attention. Encryption and decryption of data files are primarily user-centric, that only legitimate users are allowed to upload and download files, and specify whether a file can be shared to other users. There are two ends while we talk about the security of the data in a cloud environment. In order to keep securities at cloud storage following skeleton of the proposed work which is hybrid in nature containing three stages is given.

Section presents proposed security scheme which provides a complete outsourcing solution of data– not only the data confidentiality but also its authentication. Proposed security scheme consists of four stages (AuthUser, KeyGen, EncryData, DecryData). AuthUser is a stage to authenticate the iot user for secure outsourcing of data at the cloud end. KeyGen is a module that is run by cloud server to generate a public and private key that is to be used in next stage of this scheme. EncryData is a stage where data is encrypted using proposed algorithm and store it at cloud database. DecryData is stage that is used at retrieval time of data, this module decrypts the data using proposed algorithm

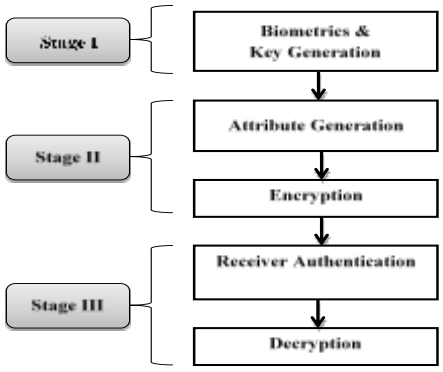

Fig. 2 Flow Chart of Stages of Proposed Work

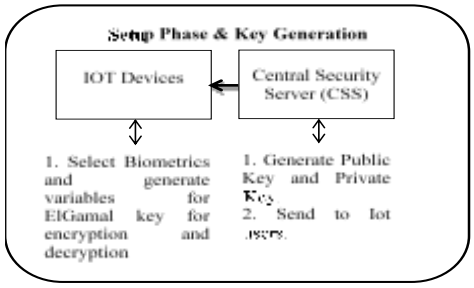

Fig. 3 Flow Chart of Stage-I Function

This is the first step of solution where the IOT user ask the CSS for authentication.

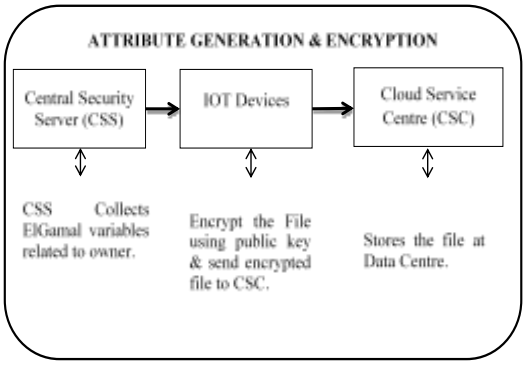

Fig. 4 Flow Chart of Stage-II Function

In the second stage, proposed work deals with new designed encryption algorithm which is based on the concept of ElGamal algorithm. In the third stage of proposed work, the phase of data file authentication and decryption, firstly the user of data file will take permission for retrieval of data file. Immediately the CSS gives license for the user authentication. Finally the user use the secrete key to retrieve the data for decryption.

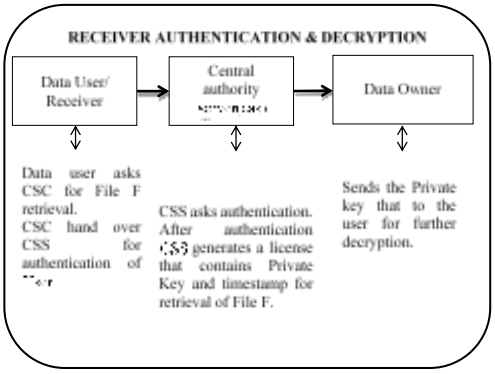

Fig. 5 Flow Chart of Stage-III Function

A. *Authentication Process Flow Chart*

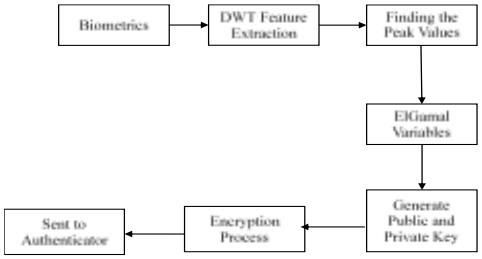

Fig. 6 Authentication Process Flow Chart

B. *Secure Data Transmission*

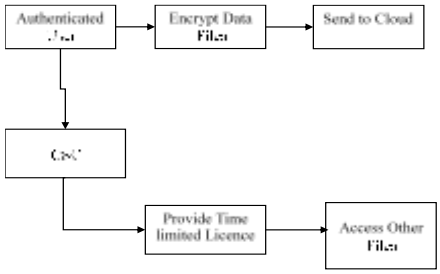

Fig. 7 Transmission Process Flow Chart

C. *Elgamal Algorithm*

ElGamal algorithm consists of three processes; there is the process of forming the key, the process of encryption and the decryption process. This algorithm is a block cipher, which was doing the encryption process on the plaintext blocks that generate ciphertext blocks then it had done the decryption process, and the results are re-combined into a whole and understandable message.

Key Formation Process

Key formation process consists of key public and private key. The process is to determine a prime number p, primitive element

α and free element a Ɛ {0,1,…,p-2}. There are three pairs of numbers in ElGamal's public key algorithm, there are:

Let E_p be an elliptic curve equation over a finite field Ep : $y^2 = x^3 + ax + b \bmod p$

where, a and b are constant

p: prime number

Coordinates (x, y) ∈ E_p follows certain additive abelian properties.

The strength of Elliptic curve analogue ElGamal encryption scheme (ECAEES) depends on Elliptic curve discrete logarithmic problem (ECDLP) which is an exponentially difficult problem with raise in key size. Performing encryption and decryption operation using ECAEES over a finite field requires computation for encoding plain data to the coordinate of the elliptic curve.

Encryption Process

$$P_c = \{kG, (P_m + kP_b)\}$$

$$P_c = \{kG, (x_c, y_c)\}$$

Where,

P_c =Cipher text

G= Key Generator

k= random integer between 1 and n − 1 where n is the cyclic order of an elliptic curve over finite field.

Pm= Plain message represented as elliptic curve coordinate using Koblitz encoding technique.

Pb= Public key of the receiver.

(x_c, y_c)= One of the point in elliptic curve after point addition of P_m and kP_b.

All the points $\{kG, P_m, kP_b, (x_c, y_c)\} \in Ep$

Decryption Process

$P_m = (x_c, y_c) - n_b kG$

where,

nb= Receiver's private key.

Koblitz encoding technique

For the Koblitz method, we choose p such that the following conditions are satisfied:

- p is a prime such that p does not divide $-16(4A^3 + 27B^2)$.
- $p \equiv 3 \bmod 4$.
- p has more than 2560 bits.
- p > m.

After converting the message to a number m, we use the following algorithm to encode the message as a point on an elliptic curve E.

- Given an elliptic curve over a finite field : Ep : $y^2 = x^3 + ax + b \bmod p$
- Represent the plain message as an integer m (where $0 \leq m < p/1000 - 1$).
- For $0 \leq j < 1000$, compute $x_j = 1000m + j$ and $s_j = x^3_j + ax_j + b \bmod p$.
- If $s^{(p-1)/2} j \equiv 1 \bmod p$, then s_j is a square mod p.
- For $p \equiv 3 \bmod 4$, $y_j \equiv s^{(p+1)/4} j \bmod p$.
- The message m is embedded as $P_m = (xj , yj)$.
- m can be recovered by a division operation on x coordinate of P_m and taking the floor value

V. RESULT ANALYSIS

According to the simulation scenario, table 1 has been given as an evidence to show that proposed cryptosystem for WBAN/IOT takes less time to execute.

Table 1: Execution Time Analysis for Biometric Authentication

Login Authentication (Biometrics)	Execution Time Analysis (in ms)
Fingerprint	0.42
Iris	0.16
Hand Gesture	1.97
Password	0.13

Table 2: Login Communication Cost for Biometric Authentication

Login Authentication (Biometrics)	Login Communication Cost (in bits)
Fingerprint	700
Iris	640

Hand Gesture	272
Password	224

According to the simulation scenario, table 2 has been given as an evidence to show that proposed cryptosystem for WBAN/IOT takes less communication cost in terms of data bits.

According to the simulation scenario, table 3 has been given as an evidence to show that proposed cryptosystem for WBAN/IOT takes less upload and download execution time in terms of data bits.

Table 3: Time Taken to Upload and Download According to File Size

File Size	Time taken in Upload (in ms)	Time taken in Download (in ms)
10 KB	0.56	.04
20 KB	0.46	.03
30 KB	0.96	.02
40 KB	1.34	1.6
50 KB	1.23	1.5
60 KB	1.89	1.7
70 KB	2.2	1.3
80 KB	2.42	1.21
90 KB	3.7	1.48
100 KB	4	1.65

A. Comparative Performance Analysis

In [1] author presented an ElGamal cryptosystem and biometric information along with a user's password-based authentication scheme for cloud-based IoT applications refereed as SAS-Cloud. This research presents an modified ElGamal cryptosystem and biometric information authentication scheme for WBAN/IOT applications for license based data sharing applications.

The table 4 shows the comparative feature analysis of proposed algorithm with existing algorithm. The table 5 and figure 8 shows the comparative performance evaluation for login as well as authentication of proposed algorithm with existing algorithm.

Table 4: Comparative Feature Analysis

Features	Existing [1]	Proposed
Authentication	Fingerprint Only	Biometric features like finger print, iris scan and hand geometry according to user choice
Secure Authentication	No	Yes
Secure Data Accessing	Yes	Yes
Secure Data Sharing	No	Yes
Integrity Checking	No	Yes
Execution Cost	Login and Authentication	Login Authentication and Encryption and License generation

Table 5: Comparative Performance Execution taken in Login and Authentication

File Size	Execution taken in Login and Authentication (in ms)
Proposed	4
Maitra et al. [1]	6
Yoon et al. [10]	7
Ramasamy and Muniyandi [9]	9
Shen et al [11]	11
Hwang and Li [12]	11
Lee et al. [8]	13

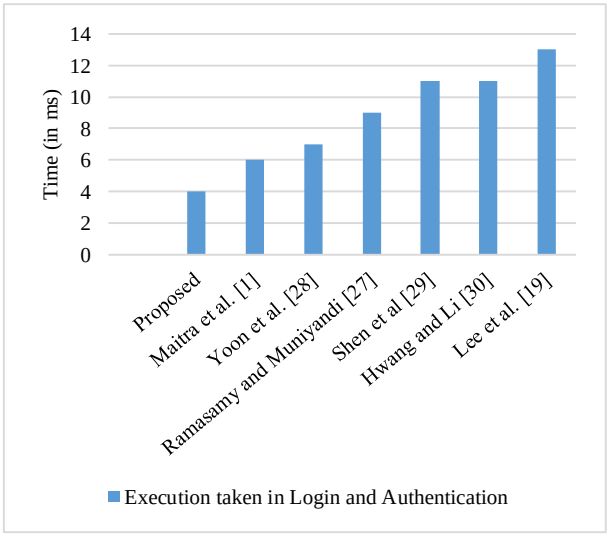

Fig. 8 Comparative Performance Execution taken in Login and Authentication

VI. CONCLUSION

The Wireless Body Area Network is a rising and future promising innovation that will change individuals' healthcare revolutionarily. Information security and protection in WBANs and WBAN-related e-healthcare frameworks is a huge

zone, and there still remain various extensive issues and challenges which is difficult to overcome. This work reviewed the deployment of WBANs in terms of security and privacy. It has also dealt with WBAN communication architecture, the security and privacy in WBAN and the threats to the integration of sensors and actuators as well as attacks to WBANs. This implies that the framework provides for the other substantive safety measures such as trust, audit, digital forensics and IDPS to guarantee compliance within the law and ethical behaviour by healthcare workers and system operators who have the access to patient records and information. These implications require the public and health care personnel to be aware of the challenges that come along with WBAN usage to ensure that the application in delivering patient's healthcare is secured at all levels. This work reviewed the deployment of WBANs in terms of security and privacy. This work observed that most of the authentication protocols using hash function and ElGamal cryptosystem for cloud-based applications are affected by security attacks and are unable to hide the actual identities of the end users during login session. Therefore, this work has introduced a secure biometric ElGamal-based authentication as well as data sharing schemes. The result analysis shows that the proposed work is better with respect to existing work with respect to execution time and cost as well as security level. In future, this work will be enhanced with some other parameters such as computational cost, storage space. This work will also be enhanced for estimating the level of security by applying different types of attacks. Somehow, it can also be enhanced while estimating the network load while transmitting over IOT.

REFERENCES

[1] Tanmoy Maitra, Mohammad S. Obaidat, Debasis Giri, Subrata Dutta, Keshav Dahal, "ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications", *IET network*, 2019, Vol. 8 Iss. 5, pp. 289-298.

[2] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen and D. Wu, "Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[3] I. Ivanciu, L. Ivanciu, D. Zinca and V. Dobrota, "Securing Health-Related Data Transmission Using ECG and Named Data Networks," *IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, Paris, France, 2019, pp. 1-6.

[4] M. Kim, J. Lee, S. Yu, K. Park, Y. Park and Y. Park, "A Secure Authentication and Key Establishment Scheme for Wearable Devices," *International Conference on Computer Communication and Networks (ICCCN)*, Valencia, Spain, 2019, pp. 1-2.

[5] H. Jiang, J. Starkman, Y. Lee, H. Chen, X. Qian and M. Huang, "Distributed Deep Learning Optimized System over the Cloud and Smart Phone Devices," *IEEE Transactions on Mobile Computing, 2019*.

[6] I. Pandey, H. S. Dutta and J. Sekhar Banerjee, "WBAN: A Smart Approach to Next Generation e-healthcare System," *International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2019, pp. 344-349.

[7] X. Meng, J. Xu, W. Liang and K. Li, "An Anonymous Mutual Authentication and Key Agreement Scheme in WBAN," *Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Washington, DC, USA, 2019, pp. 31-36.

[8] Lee, Y.C., Hsieh, Y.C., Lee, P.J., "Improvement of the elgamal based remote authentication scheme using smart cards", J. Appl. Res. Technol., 2014, 12, (6), pp. 1063–1072.

[9] Ramasamy, R., Muniyandi, A.P.: 'New remote mutual authentication scheme using smart cards', Trans. Data Privacy, 2009, 2, (2), pp. 141–152.

[10] Yoon, E.J., Ryu, E.K., Yoo, K.Y.: 'Efficient remote user authentication scheme based on generalized elgamal signature scheme', IEEE Trans. Consum. Electron., 2004, 50, (2), pp. 568–570.

[11] Shen, J.J., Lin, C.W., Hwang, M.S.: 'A modifed remote user authentication scheme using smart cards', IEEE Trans. Consum. Electron., 2003, 49, (2), pp. 414–416.

[12] Hwang, M.S., Li, L.H.: 'A new remote user authentication scheme using smart cards', IEEE Trans. Consum. Electron., 2000, 46, (1), pp. 28–30.