Lightweight PlayGamal Secure Authentication Technique with Application of Biometricsin WBAN

[1]Ashish Kumar, [2] Akhilesh Bansiya
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer Science Engineering, Vedica Institute of Technology, Bhopal, India
[2]Department of Computer Science Engineering, Vedica Institute of Technology, Bhopal, India
[1] ashu07128@gmail.com [2] akhileshbansiya@rkdf.ac.in

***Abstract:**In recent decades, Wireless Body Area Network (WBAN) is emerged as a new trend in the field of information technology that provides remote monitoring and accessing wearable sensors. While accessing remote data, there is requirement of high-level security and privacy of sensitive data over remote servers. It is therefore of great interest to discuss security and privacy issues in WBANs. In this paper, different security and privacy techniques are reviewed and analyzed WBAN/IoT challenges as well their limitations based on the latest standards and publications. This paper also covers the state-of-art security measures and research in WBAN. This work presents an PlayGamal cryptosystem and biometric information authentication scheme for WBAN/IOT applications. This work observed that most of the authentication protocols using hash function and PlayGamal 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 PlayGamal-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, PlayGamal, Biometrics.**

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].

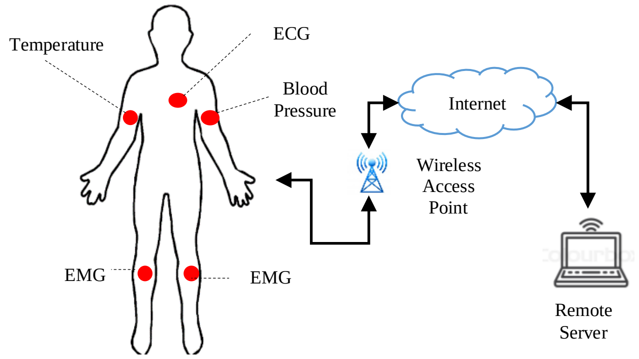

Fig. 1. WBAN Architecture

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.

These sensor nodes can be classified based on the way they are implemented into the following:

- Implant Node: These are the nodes that are placed inside the body tissues or underneath the skin.
- Body Surface Node: These are sensor nodes that are place outside the body i.e. on body surface.
- External Node: These sensor nodes are placed away from body surface about few centimeter or meter.

During distributed computing, some major concerns arise over cloud servers such as security, privacy, trust, scalability, access control, integrity etc.For these concerns many researchers are focused and developed various techniques. But still there is some limitations exists that needed modifications in it. Hence, the main goal of some researches concerning security is to improve those basic techniques to a level so that the communication security could be ensured a reasonable cost for computations in remote storage systems.

I. Literature Review

Altaf et al. [1] proposed a lightweight and secure searching scheme over encrypted data for e-Health environment. We make use of hybrid encryption scheme including symmetric encryption and optimized identity-based encryption (IBE) scheme to ensure data confidentiality over communication channel and for enhancing cloud privacy.

Jiang et al. [2] presented an optimal heart rate-based key agreement scheme to ensure secure communication between legitimate devices. The proposed key optimization scheme uses a fuzzy commitment with low latency in extracting features. In addition, the parameter optimization algorithm (PDPO) based on physiological distribution is proposed to adaptively determine the optimal protocol parameters for individuals, which ensures not only excellent and stable performance, but also safety. of the diagram. Finally, we prototype our protocol and conduct experiments on various topics to evaluate its safety and performance. Our results show that the proposed protocol negotiates the key safely and quickly, has low energy consumption and is suitable for practical applications.

Ivanciu et al. [3] proposed an original solution to protect the transmission of recorded data from sensors in a body wireless network using the ECG signal and named data networks. Our contribution is twofold: first, we use the features inherent in these networks to safely transfer sensitive health-related data (of a normal patient or driver) to the cloud, then we pass it on to stakeholders such as these such as doctors. Second, our approach uses the characteristics of the ECG signal (robustness against attack, universality and vitality detection) to encrypt this data and provide a simple and fast authentication mechanism between devices in the body area network.

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. We also measure the network traffic accumulated in different scenarios and demonstrate that the partial parameter sharing strategy not only preserves the performance of the trained model, but can also reduce network traffic.

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.

Nezhad et al. [8] proposed an approach for faulty measurements detection in order to make alarming of emergency situations more precisely. The proposed approach is based on decision tree, threshold biasing and linear regression. Our objective is to detect single and multiple faults in order to reduce unnecessary healthcare intervention. The proposed approach has been applied to real healthcare dataset. Experimental results demonstrate the effectiveness of the proposed approach in achieving high Detection Rate and low False Positive Rate. The ability of this algorithm to detect single and multiple anomalies make it more reliable for medical emergency use.

Shim et al. [9] showed that L-OOCLS is entirely broken: anyone can forge certificateless signatures on any messages for any identities from only publicly known information. Thus, the scheme is trivially insecure against the type I adversary who can replace user public keys and the type II adversary who knows the master secret key. Our result shows that their security proofs are also flawed.

II. Proposed Methodology

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.

- **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.

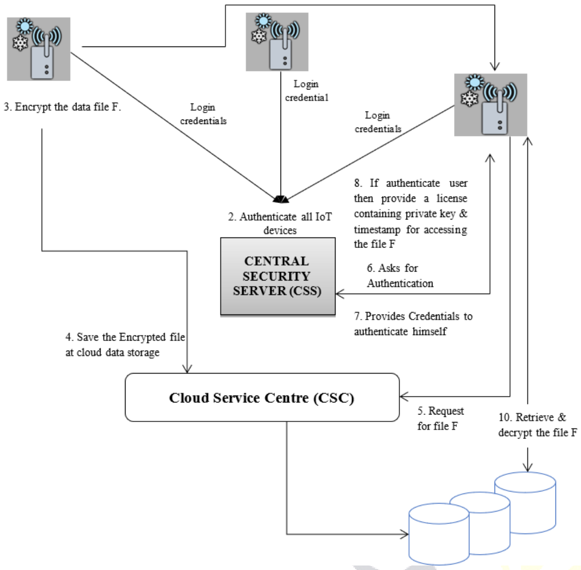
3. Encrypt the data file F.
Login credentials
Login credential
Login credentials
2. Authenticate all IoT devices
CENTRAL SECURITY SERVER (CSS)
8. If authenticate user then provide a license containing private key & timestamp for accessing the file F
6. Asks for Authentication
7. Provides Credentials to authenticate himself
4. Save the Encrypted file at cloud data storage
Cloud Service Centre (CSC)
5. Request for file F
10. Retrieve & decrypt the file F

Fig. 2. Flowchart of Work

PlayGamalalgorithm 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 message. To form the PlayGamalcryptographic system, prime numbers p and primitive group elements are needed **Z**p. There are three processes in PlayGamalAlgorithm, called the formation of keys, encryption, and a decryption step.

Key Formation Process

Key formation process consists of public key, private key and secret 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 PlayGamal**'**s public key algorithm, there are:

$$\beta = \alpha^{a} mod\, p$$

Moreover, α is the private key of the PlayGamalmethod.

So, can be obtained the public key consisting of 3 pairs of numbers there are (p, a, β) which can be published as the confidential key value.

Secret key is generated as combination of secret parameter (S_k) given by data owner and prime, q, generated by PlayGamal.

$$S_{ek} = qS_k$$

Encryption Process PlayGamal

In this process, following step of encryption is performed as:

Step 1:

- Write a message and arrange them in pairs
- Do not get the same pairs. If there are the same pairs, then paste the letter Z in the middle.
- If obtaining the odd number of letters, add the letter Z in the end.

Step 2:

Generate an encryption table of 6*6 which contains 10 numbers and 26 letters. If the generated S_{ek} is 137abc:

1	3	7	a	b	c
d	e	f	g	h	i
j	k	l	m	n	o

p	q	r	s	t	u
v	w	x	y	z	0
2	4	5	6	8	9

Messages are adjusted to this table as:

- If two letters are found in the same row of each letter is replaced with an existing letter to the right.
- If two letters are in the same key column, then each letter is replaced with the letter below.
- If two letters are not in the same row or same column, then the first letter is replaced with the first letter and second letter is replaced with the second in the square box formed due to intersection of letters.
- Repeat the steps from the start until the whole message is encrypted.
- Change the encrypted pairs into the form of a sentence or word (C_k).

Step 3:

C_k is further encrypted by following steps:

- Encryption using public key (p, α, β) and random integer number k (k Ɛ {0,1,…, p-2}) which is confidential kept by the recipient who encrypts the message. Each character in the message is encrypted using a different k number. From an integer number of ASCII that is a representation of one character that will generate code in the form of a block consisting of two values (r,t).
- Choose a character in the message to be encrypted and transform the character into the ASCII code, so the integer M is obtained.
- Calculate r value and t values with the equation

$$r = \alpha^k (mod\ p)$$
$$t = \beta^k C_k (mod\ p)$$

- Obtained ciphertext (C_{k2}) or t for the character M in blocks (r,t).
- Do the above process for all characters in the message including a space character.

Decryption Process PlayGamal

Step 1:

- The decryption from ciphertext (C_{k2}) to ciphertext (C_k) using confidential key *a*which the secrecy is kept by the recipient of the message.
- Given (p, α, β) as public keys and an as confidential key in the PlayGamal method. If it is given ciphertext (r,t), then :

$$C_k = t(r^a)^{-1} mod\ p$$

With ciphertext (C_k) with value r^a

$$(r^a)^{-1} = r^{p-1-a} mod\ p$$

Step 2:

- Create encryption table based on key S_{ek}
- Change the ciphertext (C_k) into pairs
- If two letters are on the same line of keys, each letter is replaced with a letter on the left.
- If two letters are in the same key column, then each letter is replaced with the letter above it.
- If two letters are not in the same row or same column, then the first letter is replaced with the first letter at the corner and second letter is replaced with the opposite corner of first letter in the square box formed.
- Repeat the steps from the start until the whole message is decrypted.
- Change the encrypted pairs into the form of a sentence or word (M).

III. 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	4.2
Iris	1.76
Hand Gesture	2.97
Password	1.6

According to the simulation scenario, table 2 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 2: 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	1.12	1.53
20 KB	1.74	1.98
30 KB	2.22	2.13
40 KB	2.96	2.75
50 KB	3.05	2.98
60 KB	3.54	3.14
70 KB	3.76	3.34
80 KB	4.32	3.87
90 KB	4.86	3.92
100 KB	5.65	4.63

The table 3 shows the comparative feature analysis of proposed algorithm with existing algorithm. The table 3 and figure 3 shows the comparative performance evaluation for login as well as authentication of proposed algorithm with existing algorithm.

Table 3: Comparative Performance 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	Encryption	Login Authentication and Encryption and License generation
KeyGen	20.56ms	4ms
Encrypt	7.58ms	5ms
Trapdoor	6.54ms	4ms

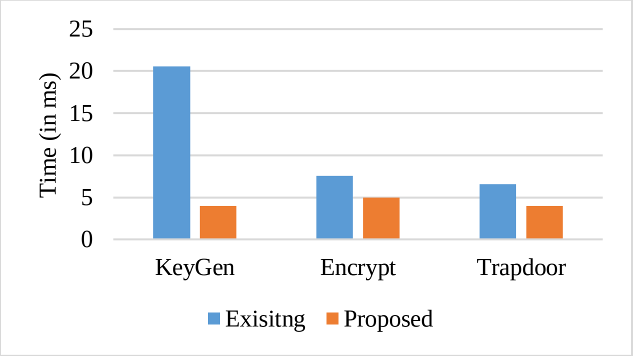

Fig. 3. Comparative Performance Analysis

IV. Conclusion

The rising and future promising innovation in the field of WBAN integrated with IoT having capabilities for changing information and technology revolutionarily. This study explores the future scope to design more secure WBAN integrated with IoT architecture with reduced complexity and enhance security level.This work observed that most of the authentication protocols using hash function and PlayGamal 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 PlayGamal-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.

REFERENCES

[1] F. Altaf, M. Aditia, E. Saini, B. Rakshit and S. Maity, "Privacy Preserving Lightweight Searchable Encryption for Cloud Assisted e-Health System," 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 2019, pp. 310-314.

[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] M. M. Nezhad and M. Eshghi, "Sensor Single and Multiple Anomaly Detection in Wireless Sensor Networks for Healthcare," *Iranian Conference on Electrical Engineering (ICEE)*, Yazd, Iran, 2019, pp. 1751-1755.

[9] K. Shim, "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211-9212, Oct. 2019.