BioGamal Based Authentication Scheme for Cloud Assisted IoT Based WBAN

Heba G. Mohamed

Abstract — Today, wireless body area networks or WBANs consist of wearable sensors that allow people to monitor their health records remotely from anywhere in the world. Healthcare professionals and patients rely on such high-level communications for their personal data to be protected from intrusions and attacks. In order to enhance the security of WBAN architecture, many researchers are showing a keen interest in it. Using the latest standards and publications, this study examines and assesses separate security and privacy techniques, analyzing WBAN/IoT challenges as well as their limitations. Additionally, this research examines the latest security practices in WBAN. For WBAN/IoT applications, we present a novel BioGamal cryptosystem and authentication method based on biometric data. It was observed that most of the authentication protocols for cloud-based applications relying on hash functions and other cryptosystems are vulnerable to security attacks and do not provide adequate security protection against revealing end-user identities. Therefore, the proposed scheme introduces both secure biometric BioGamal-based authentication and data sharing schemes. According to our analysis, this novel approach will be more effective than existing solutions in terms of execution time, cost, and security.

Keywords — BioGamal, Biometrics, Data confidentiality, Data sharing, Internet of Things, Network, Security, Wireless Body Area.

I. INTRODUCTION

In a Body Area Network (BAN), devices are located inside, above, and around the body and communicate wirelessly. Only a few meters of distance can be covered by da-ta transmission. This is illustrated in Fig. 1. Portable and implanted electronic circuits make up this new intrapersonal network. Among its many useful features and capabilities, it offers extremely low energy consumption and exceptional security [1]. There has been a dramatic increase in the number of technology products used by one person, such as desktop computers, laptops, tablets, and mobile phones. Humans are implanted with other devices to monitor their health conditions and bodily functions [2]. In addition to recording somebody's parameters directly from the surface of the skin or inside parts of a person, the sensor nodes can also record electrocardiograms (ECGs), electroencephalograms (EEGs), body movements, blood pressure, blood sugar levels, heart rates, respiratory rates, etc. [3]. Each sensor is designed specifically to meet each application's requirements. EEG sensors, for instance, should monitor brainwave activity. ECG sensors can also monitor heart rate.

A cloud-based healthcare system can handle such issues by storing patient information and their health conditions securely. However, security and privacy concerns over such data storage have become the primary concern [4], [5]. Both cloud service providers and healthcare organizations must take necessary measures to prevent unethical attackers from gaining access to patient data. Therefore, cloud-based healthcare systems must have high levels of security and assurance [6]. According to Farahani in 2014, organizations should ensure that the sensitive health reports are stored in a secure, encrypted manner on cloud services. With the growth of network size and the addition of new network devices, they lack control over the security of the data access devices used to transmit data to the network [7].

For the IoT ecosystem, the authors presented the mode of encryption and decryption for secured transmission of data in 2017 and 2020 [8], [9]. It is critical to provide encrypted and decrypted data with a key that enables access to the information in the cloud to limit unauthorized access to this information [10]. A provider selects the key (public and private) for the encryption process based on the encryption type symmetric or asymmetric [11], [12]. Authorization usually involves passing the username and password to the cloud server; based on the information provided during authorization, the patient would then be linked or tracked based on their history of access or preferences [13], [14]. There have been several types of privacy-preserving authentications for secure data transmission based on IoT, as detailed in [15], [16]. Because of this method, symmetric cryptography has a reduced processing time as compared with asymmetric cryptography. Using symmetric encryption, Gong et al. have specifically noted that their system is scalable and secure for sharing patient health data [17]. Several studies have documented cloud-based healthcare encryption protocols in which a homomorphic encryption algorithm secures the data from unauthorized access [18]-[21]. Encryption has found applications in a variety of domains with the use of cloud-based systems. Many topics have been explored in [22]-[30] regarding how health information collected from patients is encrypted before transmission through a wireless body area network (WBAN).

A secure and lightweight mutual authentication and key establishment scheme based on wearable devices were presented by Kim et al. [31]. It is suitable for resource-constrained environments. Using the cloud server and smartphones with IT functions, Jiang et al. [32] provided an
optimized system for deep distributed learning. To enable mobile computing and protect data, each device serves as a mobile data hub. As part of the proposed system, private data is stored on smartphones; sharing settings are created, resulting in a consensus model. Based on experiments, it was demonstrated that the distributed deep learning system could reconstruct the behavior of centralized training. Panday et al. [33] presented a comprehensive analysis of various BAN topics, such as communications, sensors, applications, requirements, standards, and security. Meng et al. [34], which provides untraceability for session keys, proposed a new anonymous scheme of mutual authentication and key agreement. In the scheme, authentication and key agreement are achieved by using the fewest hash functions and XOR operations possible. BAN logic, as well as the Automated Validation of Internet Security Protocols and Applications (AVISPA) have been used to verify the authenticity of the data.

With the introduction of BioGamal in [35], a security appliance that combines ElGamal digital signatures and the concept of DNA (Deoxyribonucleic Acid) encryption and decryption techniques provides an effective and comprehensive security solution for information. ElGamal digital signatures improve the authenticity of data transfers [36]. In DNA cryptography, data is encrypted using DNA sequences, which increases data security. A later extension of the DNA technique allowed researchers to both encrypt and reduce the storage size of data, providing a faster and more secure data transmission method [37], [38].

Based on BioGamal technology, we propose a secure authentication and key agreement scheme for cloud-assisted WBAN/IOT addressing the issues mentioned in previous schemes. The proposed system ensures both data integrity and privacy by limiting access to information to authorized users only. With the results of the proposed procedures, some computations can be done without incurring significant costs, making the system suitable for mobile implementation. In a summary, Section II describes the WBAN using the Internet of Things and BioGamal secure algorithm. The proposed secure healthcare system is presented in Section III, while Section IV examines both the simulation model and the overall performance of the system. The proposal concludes in Section V.

II. LITERATURE REVIEW

A. IoT Based WBAN for Healthcare Architecture

During the past few years, the Internet of Things (IoT) has gained attention from a wide range of research fields [39], [40]. It is predicted that IoT will seamlessly connect the subjects to healthcare professionals in the future [41], [42]. The wireless body area network (WBAN) is becoming an emerging research field globally with the advent of wearable sensors, low-power integrated circuits (ICs), and wireless communication technologies [43]. Wireless Body Area Networks enable the monitoring of health wherever and whenever it is required around the body [44], [45]. For example, e-health applications, including computer-assisted rehabilitation, early detection of medical issues, and emergency notification can be accessed using this platform [46]. In recent years, mobile devices have become an almost indispensable part of people's daily lives, especially smartphones. These devices can be utilized as the interface between the WBAN and the IoT cloud [47]-[49], as shown in Fig. 1.

During the development of the WBAN, wearable sensors are critical components, as they collect vital body data. Researchers have presented a variety of wearable sensor systems from diverse fields for WBAN applications. Using a wearable photoplethysmography (PPG) sensor, the authors present a method of measuring heartbeats at the earlobe [50]. The polymer-based flexible strain gauge sensor is designed in [51], as is another heartbeat sensor. During a magnetic resonance imaging (MRI) experiment, [52] presents a wearable sensor prototype that records heart rate, blood oxygen saturation, temperature, and humidity. The wearable sensors of WBAN are powered by a middleware solution based on smartphone applications proposed by Seeger et al [53].

![Fig. 1. IoT-based connected health platform with wireless body area networks.](image)

B. BioGamal Secure Algorithm

BioGamal is a combination of DNA algorithm and ElGamal cryptosystem that is used in encryption and decryption processes. A DNA cryptographic algorithm is used in the first level to scramble biometric information. During computerized coding, the states 0 or 1 are used to encode the paired digits. This forms the basis for DNA cryptography, which uses the DNA rationale word to make four nucleic acid bases A, G, C, and T representing Adenine, Cytosine, Guanine, and Thymine, respectively. Several nucleic acids are arranged in a double helix structure to form DNA. Chains T and A form paired duos, and Chains C and G form elective paired couples. By that definition, 0 and 1 are pairs of complements in a double activity, and 0 1 and 1 0 are more of a complementing pair. Table I shows that 16 key sequences can be framed using these ATGC sequences. [37], [38].

Fig. 2 shows the flowchart of the BioGamal security algorithm. This paper implements BioGamal between the user and the authenticator. It is proposed to be used as a digital signature algorithm. To shape the digest of the message, SHA is used in this phase, followed by BioGamal to encrypt the digested message. To encrypt the digested
message, DNA encryption is used, followed by ElGamal encryption. The two algorithms are combined to generate a digital signature for the message. Digital signature decryption is completed by using DNA decryption and ElGamal decryption procedures.

![Flowchart of BioGamal Algorithm for proposed security system](image)

**Table 1: DNA Key Arrangement**

| Array | Key Arrangement | Rate |
|-------|-----------------|------|
| 0000  | AA              | R0   |
| 0001  | AT              | R1   |
| 0010  | AG              | R2   |
| 0011  | AC              | R3   |
| 0100  | TA              | R4   |
| 0101  | TT              | R5   |
| 0011  | TG              | R6   |
| 0111  | TC              | R7   |
| 1000  | GA              | R8   |
| 1001  | GT              | R9   |
| 1010  | GG              | R10  |
| 1011  | GC              | R11  |
| 1100  | CA              | R12  |
| 1101  | CT              | R13  |
| 1110  | CG              | R14  |
| 1111  | CC              | R15  |

ElGamal digital signature algorithm is generated by the interplay between modular exponentiation and discrete logarithms. Ultimately, the algorithm is executed in three separate phases. The first is the generation of a key, the second is encrypting the message and the third phase is decrypting it. During key generation, a public and a private key pair are employed. Digital signatures are created using a private key, and corresponding public keys can then be used to verify the signature. As a result of digital signatures, recipients can verify the origins of the message, examine its integrity, and learn it has not been altered since it was signed. In addition, the sender cannot dishonestly claim they did not sign the message. The three phases are generated as follows:

**Phase 1: Key Generation**
- Produce an enormous prime quantity \( p \) and primitive set \( Z_p^* \) where \( Z_p^* \) are comparatively prime to \( p \).
- Create additional primitive components \( g \) and free components \( \alpha \in \{0,1,\ldots, p-2\} \) to generate a public and secret key.
- Public key is formed by three parameters as:
  \[
  \beta = g^\alpha \mod p
  \]

**Phase 2: Message Encryption**
- The system utilizes public key and unsystematic secret integer \( k, k \in \{0,1,\ldots, p-2\} \)
- Each character in the message must be encrypted with a different \( k \) number.
- Calculate \( r \) and \( t \) values as follow:
  \[
  r = g^k \mod p
  \]
  \[
  t = \beta^k M \mod p
  \]
- Cipher text completed as \((r, t)\).

**Phase 3: Message Decryption**
- Apply secret key \( \alpha \) and public keys \((p, g, \beta)\) to perform the decryption phase.
- From received cipher text \((r, t)\), plaintext is performed as:
  \[
  M = tr^{-\alpha} \mod p
  \]

**III. METHODOLOGY**

**A. Proposed Secure Cloud-Assisted IOT Application**

Authentication is one critical aspect of securing cloud assisted IoT applications. In this system, three roles are involved: the User, the cloud-service center (CSC) and the Authenticator. Users of WBAN/IoT need to register with the CSC before accessing the system then the CSC will issue them a unique certificate by the following process. The User requires first authentication permission before accessing or uploading the file. Secondly, the user encrypts his or her biometric information then uploads it to the Authenticator and the Authenticator will verify that the user has previously signed up. If there is no information the user will then be asked to register and store the user's bio-metric information.
After that, the Authenticator authenticates the User and connects him to CSC. In order to access another file, the User has to provide some accessing parameters, and a time-limited license will be provided. Once these steps are done, the authorized User can access the cloud-based files. Fig. 3 shows the flowchart of the proposed work.

Fig. 3. Flowchart of proposed IOT/WBAN.

Security and user privacy protections are becoming increasingly important as more and more people and organizations turn to cloud storage for their data. Users have primary control over the encryption and decryption of files since only authorized users can upload and download files and specify whether a file can be shared with others. In a cloud-computing environment, we have to consider two ends when it comes to security. In order to keep security at cloud storage, Fig. 4 outlines the phases of the security system, which presents the proposed security scheme that affords complete outsourcing solutions—both in terms of confidentiality as well as authentication. AuthUser, KeyGen, EncryData, and DecryData are the four phases of the security scheme. In the cloud end, AuthUser verifies the authentication of the IOT user for securing data outsourcing. Using KeyGen, the cloud server will generate public and private keys for use in the next phase of this scheme. Encrypt data and store it in a cloud database using the encrypted algorithm proposed in EncryData. During data retrieval, DecryData stage decrypts the data with the proposed algorithm; this stage is applied at data retrieval time.

From Fig. 5 there are three phases, phase one the IOT user asks the CSS for authentication. The user selects biometrics and generates variables for BioGamal key for encryption and decryption, then the CSS generates public and private keys and then sent to IOT users. In the second phase, the proposed work deals with the newly designed encryption algorithm which is based on the concept of BioGamal algorithm. The CSS collects BioGamal variables related to owners then the user encrypts his own file using the public key and sends it to CSC. The CSC store the file at the data center. In the third phase of the proposed work, the phase of data file authentication and decryption, firstly the user of the data file will take permission for retrieval of the data file. CSS asks authentication center. After verification, The CSS generates a license that contains a private key and timestamp for retrieval of the file. Finally, the user uses the secret key to retrieve the data for decryption.

Fig. 4. Flow chart of the three proposed phases Helpful Hints.

Fig. 5. Block Diagram of Phase 1, 2 and 3. (a): Setup and Key Generation, (b) Attribute Generation and Encryption, (c) Receiver Authentication and Decryption.

B. Process of BioGamal for Authentication and Data Transmission

Step 1: The IOT user presents his/her biometric to the biometric scanner.
Step 2: Features are selected or extracted from the biometric image of the user using DWT feature extraction then finding the peak values.

Step 3: Biometric template $B_T$ is generated by applying hash function $SHA256$ on the features selection $B$ as follow:

$$B_T = H(B) = \text{“34671321392033323960627213262981873026305330310549356724134919622644112251708”}$$

Step 4: Convert the biometric template output to binary number to implement BioGamal algorithm by first applying DNA encoding as follow:

$$\text{“10011001010011101100001110011001000100001110011100110001110110000110010010010101010101001010010101100110010101100101001011111010010001001111010110101010110011001011010010101100110010110111111001000010010101101010101101100110010010111110100100111101101011001110”}$$

Step 5: From Table I, assign DNA digital coding for each paring as follows:

“GTGTTACCGGAGCGATGTGAGAATCAAAAAAAAAAAAAAAAAAAAA”

Step 6: Express DNA sequence into DNA key combination as stated in Table I:

“9981481181011018111 ……… 312”

Step 7: Distinct DNA key combination by “0” or “@”between the sequences to obtain the first cipher of biometric data:

$$C_1 = \text{“9 9 8 14 8 11 1 0 1 8 11 1”}$$

Step 8: The IOT user implement ElGamal algorithm as described in section 2.2 to encrypt the first cipher of biometric data $C_1$ and then uploads it to the authenticator. He generates the key generation of ElGamal algorithm where the public key denoted by $(p, g, \beta, H)$ and the private key denoted by $(p, g, \alpha, H)$ and $H$ is a hash function $H : \{0,1\}^* \rightarrow \{1,2,...p-2\}$

Step 9: The authenticator receives the encrypted data to verify that the user has previously signed up by applying the decryption process using the public key $(p, g, \beta, H)$ of ElGamal algorithm and then recovering the hashing value using DNA decryption algorithm.

Step 10: If there is no information the user will then be asked to register and store his biometric information. After that, the authenticator authenticates the user and connects him to CSC.

Step 11: CSS generates a license that contains a private key and timestamp to access another file. Fig. 6 and 7 represent authentication and data transmission processes.

![BioGamal Authentication Process](image)

![BioGamal Secure Data Transmission](image)

IV. SIMULATION RESULTS

A. Experimental Results

These experiments were performed on a Dell computer with Windows 10, Intel Duo Core i7 @2.53 GHz, and 8 GB DDR3 RAM. It has been shown in Table II that the proposed cryptosystem for WBAN/IOT takes less time to execute.

| Biometric | Time (ms) |
|-----------|-----------|
| Fingerprint | 0.34 |
| Iris | 0.98 |
| Hand Gesture | 2.12 |
| Password | 0.10 |

Table III shows that the proposed cryptosystem for WBAN/IOT has a lower communication cost in terms of data bits in accordance with the simulation results. Table IV demonstrates that the proposed cryptosystem for BioGamal/WBAN/IOT is faster when it comes to upload and download performance.

| Biometric | Cost (bits) |
|-----------|------------|
| Fingerprint | 650 |
| Iris | 500 |
| Hand Gesture | 182 |
| Password | 167 |

| File Size (KB) | Uploading Time (ms) | Downloading Time (ms) |
|---------------|---------------------|-----------------------|
| 10 | 0.27 | 0.03 |
| 20 | 0.38 | 0.02 |
| 30 | 0.69 | 0.018 |
| 40 | 1.14 | 1.11 |
| 50 | 1.22 | 1.27 |
| 60 | 1.75 | 1.32 |
| 70 | 1.86 | 1.38 |
| 80 | 2.25 | 1.45 |
| 90 | 2.88 | 1.58 |
| 100 | 3.5 | 1.60 |
B. Simulation Performance Analysis

As part of the SAS-Cloud authentication scheme, the author in [1] presented ElGamal cryptography and biometrics information along with user passwords for cloud-based IoT applications. This paper presents a BioGamal cryptosystem for license-based data-sharing applications for WBAN/IoT. Table V compares the proposed algorithm with existing algorithms. Table VI and Fig. 8 compare the performance of the proposed algorithm with the existing algorithm for both login and authentication purposes. The results show that the proposed algorithm has a faster login and authentication time compared with other schemes.

Moreover, the report discusses WBAN communication architecture, security as well as privacy, and how sensors and actuators can be integrated to help protect WBANs from attacks. It follows that the framework ensures compliance with the law and ethical behavior by systems operators and health care workers who have access to patient records and information, through trust, audit, digital forensics, and IDPS. Public and health care workers must be aware of these implications to ensure the application in delivering patient healthcare as secure as possible. Security and privacy were assessed with regard to the deployment of WBANs. During a login session, we observe that most authentication protocols using hash functions and BioGamal cryptosystems are vulnerable to security attacks and are not capable of hiding the actual identities of end-users. As a result of this work, biometric BioGamal-based authentication and data sharing schemes were developed. In terms of both execution time and cost, as well as the level of security, the proposed work is superior to existing work. We will expand this work to include other parameters in the future, such as storage space and computational cost. Various types of attacks will be applied to this work to estimate the level of security. Additionally, it can also enhance the overall capacity of the network when transmitting over the Internet of Things.

Table V: Feature Analysis

| Features                  | [1]       | Proposed |
|---------------------------|-----------|----------|
| Authentication Secure     | Fingerprint Only | Yes |
| 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 VI: Comparison of Login and Authentication Time

| File Size | Login and Authentication Time (ms) |
|-----------|-----------------------------------|
| Proposed  | Login and Authentication Time (ms) |
| [1]       | 6                                 |
| [54]      | 13                                |
| [55]      | 9                                 |
| [56]      | 7                                 |
| [57]      | 11                                |
| [58]      | 11                                |
| [59]      | 4                                 |

Fig. 8. Comparison of Login and Authentication Time.

V. CONCLUSION AND FUTURE WORK

Wireless Body Area Networks are emerging technologies that have the ability to revolutionize the healthcare sector. Despite all the work that has been done in WBANs and WBAN-related e-healthcare frameworks, there remain numerous challenges and extensive issues which are difficult to resolve. In this study, we reviewed how WBANs are deployed from a privacy and security perspective.

REFERENCES

[1] Maitra T, Obaidat MS, Giri D, Dutta S, Dahal K. ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications. IET Netw. 2019;8(5):289–98. https://doi.org/10.1049/iet-net.2019.0004.

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

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

[4] Das Challa S. A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., & Vasilakos, A. V. “An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks” in Computers & Electrical. Eng J (NY). 2017.

[5] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wirel Commun, 2010 Feb;17(1):51–8.

[6] Zanjal SV, Talmale GR. “Medicine reminder and monitoring system for secure health using IoT”. Proc in Computer Science journal, pp. 471–476, 2016. https://doi.org/10.1016/j.procs.2016.02.090.

[7] Fairahani B, Firozzi F, Chang V, Babaraghu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. Future Gener Comput Syst. 2018;78:659–76.

[8] Yang Y, Zheng X, Tang C. Lightweight distributed secure data management system for health Internet of Things. J Netw Comput Appl. 2017;89:26–37.

[9] Alzahrani BA, Irshad A, Albeshri A, et al. A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks. Wirel Pers Commun. 2020.

[10] Abdmeziem MR, Tandjaoui D. An end-to-end secure key management protocol for eHealth applications” in Computers & Electrical. Eng J (NY). 2015; 184–97.

[11] Bokhari MU, Shalal QM, Tamandani YK. Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning. J Inst Electron Telecommun Eng. 2018 Jan.

[12] Joshi A, Mohapatra AK; Ashish Joshi & Amar Kumar Mohapatra. Authentication protocols for wireless body area network with key management approach. Journal of Discrete Mathematical Sciences and Cryptography. 2019;22(2):219–40.
Heba G. Mohamed was born in Alexandria, Egypt in 1984. She received the B.Sc., M.Sc. degrees in electrical engineering from Arab Academy for Science and Technology in 2007 and 2012, respectively, then, the Ph.D. degree in electrical engineering from the University of Alexandria, Egypt, in 2016. Starting from 2016, she was an Assistant professor at Alexandria Higher Institute of Engineering and Technology, Ministry of Higher Education, Egypt, and from 2019 and still, an Assistant professor at Faculty of Engineering, Communication department, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her research interests include cryptography, wireless communication, mobile data communication, internet of things and computer vision.