IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 23, 2021, accepted September 6, 2021, date of publication September 9, 2021,
date of current version September 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3111292

Lightweight Healthcare Wireless Body Area Network Scheme With Amplified Security

ZHENGLIANG JIANG[1], WEI LIU[1], RUIJIANG MA[1], SYED HAMAD SHIRAZI[2], AND YONG XIE[1]
[1]Department of Computer Technology and Application, Qinghai University, Xining 810016, China
[2]Department of Information Technology, Hazara University, Mansehra 21300, Pakistan

Corresponding author: Yong Xie (mark.y.xie@qq.com)

The work was supported in part by the National Natural Science Foundation of China under Grant 61862052, and in part by the Science and Technology Foundation of Qinghai Province under Grant 2019-ZJ-7065.

ABSTRACT With the rapid economic development and the increasing pressure of work and life, people are increasingly eager to obtain real-time intelligent healthcare to monitor their sub-healthy bodies. Healthcare wireless body area network (HWBAN) is one of the key infrastructures to realize intelligent healthcare. Health data is extremely private information, which makes adversaries prefer to carry out data-related interception, modification, and destruction attacks against the HWBAN system. To provide secure protection for HWBAN, many researchers have proposed various HWBAN schemes, but there are still deficiencies in security, performance, and availability. Our paper proposes a lightweight and amplified secure scheme for HWBAN by using fewer Elliptic Curve Cryptography(ECC) operations and Physically Unclonable Function(PUF) to improve security and efficiency at the same time. Furthermore, we allow users to know their health status in real-time through their mobile phones without initiating additional requests to the medical server in our system to achieve better availability. In addition, we provide strict formal security proof to demonstrate the proposed scheme meets the security and reliability requirements in this paper. The detailed comparative analysis illustrates that the proposed scheme has certain advantages in computing, communication, and security.

INDEX TERMS Healthcare wireless body area network (HWBAN), intelligent healthcare, private protection, PUF, lightweight, amplified secure.

I. INTRODUCTION

The world has entered a stage of rapid development, but it has also brought numerous crises to society. Among them, the most severe is the human health problem. For economic development, people in all walks of life have suffered overwork but ignore their health. Therefore, it is difficult for sub-health workers to spare time to check the body in time. Facing busy work, they urgently need intelligent sensors of HWBAN that can detect their health status timely. The national health problem is not only for young people, the advent of the age of the population has also presented great challenges to improve human health.

According to the research of the World Health Organization (WHO), the population of the United States over 60 years old will reach 80 million, while China will reach nearly 430 million [1], by 2050. As we all know, the growth of the elderly population is bound to increase the burden of daily healthcare and disease treatment for the elderly. Young people are busy with work day after day, making it easier for their parents to become empty nesters [2]. Without meticulous care, the healthcare of the elderly will be a huge hidden danger. Various social phenomena indicate that people now urgently need a portable intelligent medical system that can realize real-time health monitoring to relieve social pressure and protect human health.

An excellent HWBAN system must have a nice way to solve the above problems [3]. Generally, the HWBAN system uses sensors to help users detect health status timely [4] and utilizes smart mobile devices (e.g. phones) to send health information to the medical server so that doctors can grasp the health data in time and make appropriate decisions. Fig 1 is a typical HWBAN system application scenario. In recent years, many HWBAN security schemes have been designed around [5]–[9].

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

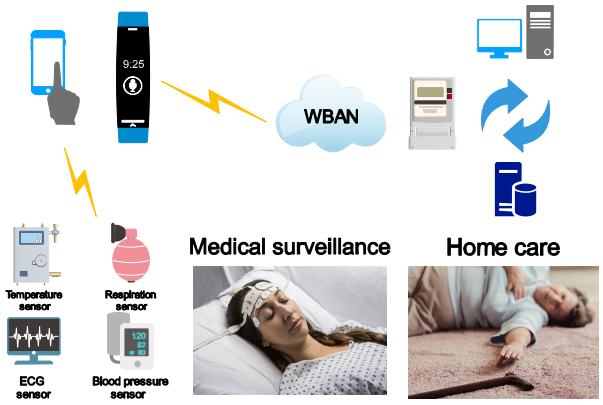

FIGURE 1. HWBAN system application scenario.

In recent years, sudden diseases have taken thousands of lives. According to medical research and analysis, all sudden diseases have related pathological symptoms before the onset. If the health status can be obtained in real-time and timely warning can significantly reduce the occurrence of sudden diseases and save the lives of countless people. Therefore, real-time perception of health data and timely delivery to patients or doctors are extremely important for the HWBAN system. To solve the issues, many researchers have imitated the design of traditional Internet of Things(IoT) security schemes in recent years, using XOR operations, hash function, and message authentication code(MAC) to construct secure communication schemes [10]. In 2020, the scheme proposed by Alzahrani *et al.* [7] wholly uses lightweight symmetric cryptographic primitives to implement a secure communication scheme between medical sensors and servers. Compared with the scheme based on public-key cryptography(PKC), the scheme has a great improvement in efficiency. The fly in the ointment is that the storage capacity of HWBAN sensors is lower [11], so it is difficult to load the storage burden of the scheme. In addition, like some similar security schemes of the IoT, it directly uses public channels to transmit the identity of the sensors, which threatens privacy [6]. Not only that, these schemes have hidden dangers of desynchronization attacks during the identity modification phase [7], [9]. Summary, the above schemes that completely use lightweight cryptographic primitives often have defects of insufficient privacy, security, and sensor storage overload.

In addition, with the continuous development of modern network technology, user privacy protection has become the main challenge. Health information is considered the most important of all private information. The leakage of personal sexual orientation, disease history, psychological and physical defects, and other information will endanger the stability of the family and even society. Therefore, a good HWBAN scheme needs to have sufficient security and reliability. To achieve this goal, some researchers have proposed a healthcare sensor network security scheme based on PKC. For example, the scheme proposed by Xie *et al.* [12] uses the ECC cryptosystem to implement secure communication between sensors and medical servers. This greatly improves the security of the traditional lightweight HWBAN schemes. However, the IEEE 802.15.6 standard proposed in 2012 strictly regulates HWBAN. It is difficult for the sensor node in the scheme to support the complex operations of PKC. Therefore, the above-mentioned scheme has insufficient usability and excessive computational costs.

The HWBAN security system in recent years has been implemented in various ways. However, most lightweight security schemes are difficult to guarantee the security of the system, and schemes that completely use public-key cryptosystems cannot guarantee the real-time of medical services. In addition, many researchers' schemes ignore the sensor's weak computing, communication, and storage capabilities, resulting in poor system practicability.

To solve the above drawbacks, our scheme combines fewer ECC point multiplication operations and lightweight cryptographic primitives to reduce computational costs while maintaining security. Specifically, medical servers and mobile phones with powerful computing power complete most calculation and communication tasks, while sensor devices are only responsible for very few lightweight calculations, and do not store any data and initiate communication requests. In order to enhance the security of the HWBAN system and reduce communication costs, the proposed scheme uses password technology and PUF to form a dual fingerprint, providing a more portable and practical authentication protocol. In order to ensure the security of the password, we propose an offline password modification protocol to further enhance the security. Aiming at improving the usability of the HWBAN system, our scheme designs a three-layer network key agreement protocol of sensor-phone-server, allowing users to obtain their health status directly through their phone. In summary, our scheme improves the security, availability, and performance of the HWBAN system, which is indispensable for the realization of intelligent medical services.

A. OUR CONTRIBUTION

Aiming at the requirements of the HWBAN system, we propose a lightweight, more secure, and more usable scheme. Our major contributions are summarized as follows:

- Firstly, we present an HWBAN scheme with amplified security and more efficient performance than traditional schemes by using PUF chip and fewer ECC operations.
- Secondly, we design a three-level communication network of sensor-phone-server that allows hospitals to obtain users' health data securely, and also users can directly understand their health status in real-time without any request to the medical server.
- Finally, we use Mao-Boyd logic to perform rigid security proof to demonstrate the proposed HWBAN scheme is provably secure and meets the security requirements of HWBAN. Moreover, we make a detailed comparative analysis with the similar schemes proposed by other researchers in recent years and illustrate our advantages.

B. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows. In Section II, we give a brief review of previous work for intelligent healthcare research. In Section III, we present the background and notations used in the paper. In Section IV, we present details of the proposed HWBAN scheme. In Sections V and VI, we perform the analysis of the security and the performance of the proposed HWBAN scheme to demonstrate its advantages compared to other similar schemes proposed in the past. Finally, we conclude the paper in Section VII.

II. RELATED WORK

In recent years, many researchers have devoted themselves to the research of health sensor networks. Ng *et al.* [13] and Stankovic *et al.* [14] described the importance and challenges of HWBAN's security mechanism and security communication scheme in detail. Then Wu *et al.* [15], Xu *et al.* [16], and Gope *et al.* [17] designed efficient security communication schemes, and achieved the real-time goal. In order to achieve reliability, Ali *et al.* [18] designed a security scheme based on bilinear pairs. Then Challa *et al.* [19] and Garg *et al.* [20] used ECC cryptographic operations to implement a more efficient and reliable HWBAN scheme.

To design an excellent HWBAN scheme, the core requirement is to protect the privacy and security of users' health data. Different from most sensor devices, HWBAN sensors have the characteristics of small size, low power, and weak computing power. In the HWBAN medical service, therefore, the traditional methods [21], [22] of direct communication between the sensor and the server or other sensors cannot be accepted. It is required to use the user's phone relay to send to the medical server. However, information is sent through public channels, which is very vulnerable to security threats such as eavesdropping, interception, and tampering. These will lead to interruption or delay of medical services, which in turn causes the HWBAN system to become unavailable. It will also cause frequent malicious attacks against the system, which will seriously endanger the reliability and security of the HWBAN system.

To achieve secure communication between sensors, mobile phones, and medical servers. Many HWBAN schemes use PKC, but they usually have huge computational burdens. Considering that the computing power of sensors is relatively lower, it is not practical to let the sensors bear the burden of public-key encryption. For example, Kumar *et al.* [23] designed a healthcare sensor network scheme utilizing bilinear pair cryptography. Later, Xie *et al.* [12] improved this algorithm by using ECC. However, the pure public-key cryptosystem exposes many efficiency problems. For example, the two HWBAN schemes mentioned above allow sensors with low computing power to undertake larger public-key cryptographic operations. However, for some critically ill users (e.g. cardiovascular and cerebrovascular diseases), time is life for them. Once the communication delay and other problems caused by low computing efficiency will be fatal.

In order to achieve a lightweight HWBAN system, Alzahrani *et al.* [7] designed a security scheme that entirely uses lightweight cryptographic primitives. Similar to many IoT security schemes, however, they have the characteristic of weaker security. For example, the schemes proposed by Lo *et al.* [6], Alzahrani *et al.* [7], and Alladi *et al.* [9] all have the risk of information leakage. Because, in their proposed scheme, the identities of all entities are publicly transmitted on public channels. Moreover, many IoT schemes have reduced availability and security in order to improve performance. Specifically, many schemes allow multiple communicating parties to store lots of shared secret values. For example, schemes such as [7], [9] will cause desynchronization attacks and other extremely serious security threats. In addition, we learn that some other HWBAN schemes [24]–[26] allow the sensor to store quantities of security parameters to achieve higher efficiency. This is very effective in some specific application scenarios, but it is not feasible under the HWBAN, because the storage capacity of the HWBAN sensor is usually weak and it is extremely easy to receive physical attacks that cause the leakage of stored information.

To balance security requirements and performance requirements, we adopt PUF chips that can provide portable authentication [27] and improve the efficiency of computing and communication [28], [29]. Not only that, but PUF chips can also achieve good physical security [30] and privacy protection [31], [32], which will improve the security and reliability of IoT devices which are exposed to the public environment.

In addition, we learn that mobile, smart phones, and smart devices are almost same have strong computing and communication capabilities, enough to bear the related operations of PKC algorithms and the costs of more communication volume. We have combined XOR operations, hash functions, and a small count of elliptic curve cryptographic primitives to design a better HWBAN security scheme. We achieve the goal of zero storage, fewer computation costs, and fewer communication costs of sensors to improve HWBAN system performance. Furthermore, we implement the entirely anonymous authentication and key agreement protocol which improves the security of traditional IoT schemes.

III. BACKGROUND AND NOTATIONS

A. PHYSICAL UNCLONABLE FUNCTION

The physical unclonable function has been usually used in the lightweight IoT security scheme. Distinct from the common mathematical function, the physical randomness of the PUF chip directly determines the mapping relationship of the PUF. Our description of PUF is as follows:

An ideal-PUF can be defined as $(l_{in}, l_{out}) - PUF : \{0,1\}^{l_{in}} \rightarrow \{0,1\}^{l_{out}}$ and it is embedded as a chip in a hardware device with the feature of efficiency, unpredictability, stability, and unforgeability. Some PUF characteristics are the basis of security of our scheme, as follows:

- **Efficiency**: The evaluation of the PUF chip is lightweight and efficient.
- **Unpredictablility**: Within the probabilistic polynomial time($\mathcal{PPT}$), even if adversary $\mathscr{A}$ gets a lot of responses of PUF through challenges other than C, the adversary cannot get the correct response $R = PUF(C)$. Thus, the response of PUF chips is unpredictable.
- **Reliability**: In any operating environment, for the same PUF, the same input will get the same output.In other words, we make $R_1 = PUF\,(C)$ and $R_2 = PUF\,(C)$, let $E(R1! = R2)$ denote the event that $R_1! = R_2$, $Pr\,[E(R1! = R2)] < \varepsilon$, ε is negligible.
- **Unforgeability**: The PUF chips are unforgeable, because their physical randomness and the length of l_{in} and l_{out} are commonly over 128 bits.

B. ELLIPTIC CURVE CRYPTOGRAPHY

Let q be a large prime number longer than 160 bits and choose an elliptic curve $E\,(a, b)$ that meets security requirements on the finite field F_q. Let G_p is a cyclic group of large prime order p and point P is the generator of the cyclic group. There are two difficult assumptions about ECC as follows [33]:

- **The ECDL assumption**: It is elliptic curve discrete logarithm(ECDL) assumption. Given the points P and cP on the elliptic curve $E\,(a, b)$, for any adversary who gets several pairs of (P, cP), adversary can not obtain c through P and cP.
- **The ECCDH assumption**: It is elliptic curve computational Diffie-Hellman(ECCDH) assumption. Given P, k_1P and k_2P, for any communicating entity that knows one of k_1 and k_2 can calculate k_1k_2P, but others must not be able to compute the k_1k_2P.

C. NETWORK MODEL

By analyzing the scheme proposed by recent scholars and our medical network sensor architecture, the network model of the PUF-based HWBAN scheme for intelligent healthcare services is shown in Fig 2. There are three types of participants with an HWBAN scheme: a sensor node $Sensor_j$, a mobile intelligent device $Phone_i$, and a medical server MS.

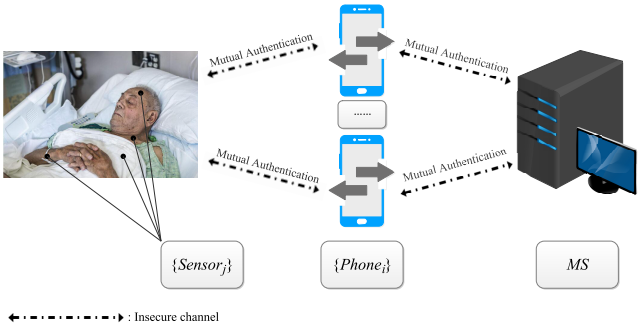

FIGURE 2. Proposed HWBAN network model.

- MS: There is a trusted medical server, which is responsible for storing the system security parameters in the scheme, including the identity of each communication entity in the scheme and the CR-pairs of every sensor node. In addition, it will authenticate and take key agreement with the $Phone_i$ for obtaining the health data securely.
- $Phone_i$: The distance between the $Phone_i$ and the HWBAN sensor node $Sensor_j$ is close. Its task is to store some parameters and users' offline passwords. In addition, it will complete authentication and key agreement with the MS and $Sensor_j$ for obtaining sensing data and transmit it securely.
- $Sensor_j$: There is an HWBAN sensor node with weak storage, communication, and computing capabilities. It will touch users directly when working. In our scheme, it is embedded with an ideal PUF chip. Will complete authentication and key agreement with the smartphone $Phone_i$ for forwarding sensing data securely.

  Data captured timely and reliably by sensor nodes is the key to various HWBAN services. Therefore, it poses a challenge to the efficiency and security of the scheme. In 2012, HWBAN was standardized as 802.15.6 by IEEE. Considering the standard as well as it commonly has the characteristics of no power supply, small size, etc., its computing, communication, and storage task needs to be thoughtfully designed.

  In the network model of this scheme, the flow of data is as follows: sensor nodes $Sensor_j$ regularly collect health data, and after authentication and key agreement are executed, health information is encrypted by the session key and transmitted to the $Phone_i$ and MS. In this way, the user can pay attention to his health information at any time, and the medical server can also analyze the user's health status in real-time and make more reasonable medical schemes.

TABLE 1. Some notations and description in our scheme.

Symbol	Description
$h\,(*)$	Secure one-way hash function
ID_i	The real identity of the mobile phone
ID_j	The real identity of the sensor node
x_s	Master key of medical server
P_{pub}	Public-key of medical server
sk_{ij}	Session key between sensor node and phone
sk_{is}	Session key between phone and medical server
(C_j, R_j), (C'_j, R'_j)	Challenge response pairs
pw_i	Password of registered user
m_i	Message of the i^{th} communication

Table 1 summarizes some of the new notations and their descriptions that appear in our scheme. And then, the next section is the proposed scheme.

IV. THE PROPOSED SCHEME

In this section, we present an exhaustive scheme that can implement privacy protection, mutual authentication, key

agreement, and offline password modification for HWBAN medical system by using ECC and PUF chips effectively. The proposed scheme consists of five phases: System initialization phase, Enrolment phase, Mutual authentication, and key agreement phase, Parameters update phase, and offline password modification phase. The symbols that appear in our scheme are listed in Table 1.

A. ASSUMPTIONS FOR THE PROPOSED SCHEME

In our proposed scheme, we make the following assumptions:

- Each sensor node $Sensor_j$ is embedded with a PUF chip. Once the PUF chip is artificially taken out or the sensor is artificially captured, it will be destroyed immediately and cannot be used.
- The medical server MS is completely credible and has sufficient data storage, computing, and strong communication capabilities. Besides, it will not have any malicious behavior. At the same time, the data in its database will not be leaked, or it will be discovered immediately after the leak.
- The smartphone $Phone_i$ after successfully completing authentication and key agreement with the medical server MS is also completely believable.

B. SYSTEM INITIALIZATION PHASE

- $Step1$: The HWBAN system will choose a secure parameter k and generate a security hash function:

$$h(\cdot) : * \rightarrow \{0, 1\}^k$$

  And publish the security hash $h(\cdot)$ to each entitiy
- $Step2$: Then the MS will select a security elliptic curve:

$$E(a, b) : y^2 = x^3 + ax + b$$

  over the finite field F_q, where the q is a large prime and the $a, b \in F_q$ satisfy $4a^3 + 27b^2 \neq 0 (modq)$, then generate an additive cyclic group with order of large prime number p and a secure generator $P \in E(a, b)$.And distribute the point P to every $Phone_i$ in the communication system.
- $Step3$: Finally, the MS will randomly chooses $x_s \in Z_p^*$ as its master key and calculate the correspondent public-key $P_{pub} = x_s P$ then publish it.

C. REGISTRATION PHASE

- $Step1$: $Sensor_j$ randomly selects a 128 bits challenge C_j and calculate the corresponding response $R_j = PUF(C_j)$ by PUF chip, and then sends $m_{rj} = \{ID_j, C_j, R_j\}$ to the $Phone_i$ through the secure channel.
- $Step2$: The $Phone_i$ selects 128 bits random numbers n_0, n_i and s. Besides, it will obtain the password when the user registered: pw_i, compute some secure parameters:

$$\begin{aligned} \alpha_i &= h(h(ID_i) \oplus h(pw_i||n_i) \, modn_0) \\ \beta_i^* &= h(s||ID_i||n_0) \\ \beta_i &= \beta_i^* \oplus h(pw_i||n_i) \end{aligned}$$

  Next, it will store the $Store_i = \{\alpha_i, \beta_i, pw_i, n_i, n_0\}$, then send $m_{ri} = \{ID_i, ID_j, \beta_i^*, C_j, R_j\}$ to MS through the secure channel.
- $Step3$: After the MS receives the message m_{ri}, it stores $Store_s = \{ID_i, \beta_i^*, ID_j, C_j, R_j\}$ in the database.

D. AUTHENTICATION AND KEY AGREEMENT PHASE

Here, we describe the key agreements between the sensor node and the smartphone and also the smartphone and the medical server. The protocol is described intuitively in Fig 3.

- $Step1$: During the validity period of the password pw_i, the $Phone_i$ gets the pw_i entered by user and its ID_i, then generate a 128 bits random number b_i and a timestamp t_i. In addition, it calculates the temporary public-key $B_i = b_i P$. Firstly, $Phone_i$ verifies that the following equation holds:

$$\alpha_i \stackrel{?}{=} h(h(ID_i) \oplus h(pw_i||n_i) \, modn_0)$$

  then computes that:

$$\begin{aligned} \beta_i' &= \beta_i \oplus h(pw_i||n_i) \oplus h(b_i P_{pub}) \\ PID_i &= ID_i \oplus h(b_i P_{pub}||B_i) \\ h_i &= h(\beta_i'||PID_i||B_i||b_i P_{pub}||t_i) \end{aligned}$$

  Lastly, $Phone_i$ sends the request message $m_1 = \{PID_i, B_i, \beta_i', t_i, h_i\}$ to medical server MS.
- $Step2$: After the MS receives the message m_1, it first verifies whether t_i is fresh. If it is not fresh, terminate the session. Otherwise, it checks the integrity of the message:

$$h_i \stackrel{?}{=} h(\beta_i'||PID_i||B_i||x_s B_i||t_i)$$

  If the above verification fails, the request will be refused, else MS completes the authentication with $Phone_i$:

$$\beta_i^* \stackrel{?}{=} \beta_i' \oplus h(x_s B_i)$$

  If the above identity verification fails, the session is terminated. Otherwise, MS calculates the ID_i of smartphone:

$$ID_i = PID_i \oplus h(x_s B_i||B_i)$$

  Then MS retrieves the parameters of $Sensor_j$ corresponding to ID_i from its database $Store_s$. Selects the timestamp t_s and random number b_s and then computes $B_s = b_s P$. To calculate:

$$\begin{aligned} PID_j &= ID_j \oplus h(b_s B_i) \\ R_j' &= R_j \oplus h(b_s B_i||t_s) \\ \beta_s &= \beta_i^*||h(x_s B_i) \\ h_s &= h(PID_j||C_j||R_j'||t_s||B_s||\beta_s) \end{aligned}$$

  Lastly, MS calculates the session key between itself and $Phone_i$: $sk_{is} = h(x_s B_i||b_s B_i)$, and then sends response $m_2 = \{B_s, t_s, C_j, R_j', PID_j, h_s\}$ to $Phone_i$.

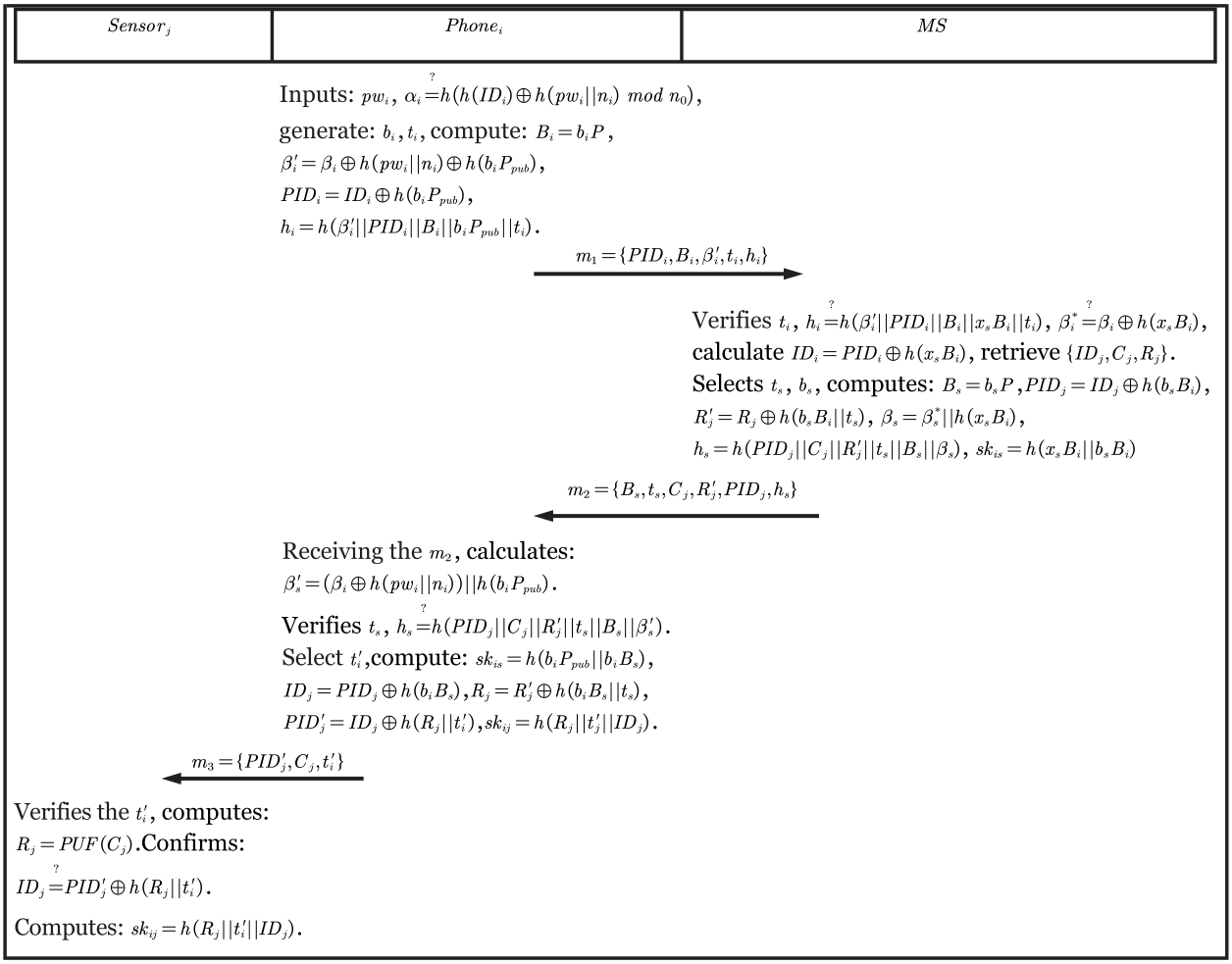

FIGURE 3. Mutual authentication and key agreement phases in the proposed scheme.

- *Step*3 : After receiving the message m_2, the $Phone_i$ immediately verifies whether the timestamp t_s is fresh, then executes identity authentication to MS and checks the integrity of the message from the MS. The next precalculates:

$$\beta'_s = (\beta_i \oplus h(pw_i||n_i))\,||h\left(b_i P_{pub}\right)$$

and then to verify:

$$h_s \stackrel{?}{=} h\left(PID_j||C_j||R'_j||t_s||B_s||\beta'_s\right)$$

If the above verification is not successful, terminate the session, otherwise calculates the session key with MS:

$$sk_{is} = h\left(b_i P_{pub}||b_i B_s\right)$$

after completing key agreement with MS, continue to calculate the sensor node's ID_j:

$$ID_j = PID_j \oplus h\left(b_i B_s\right)$$

and the response of the challenge-response pair corresponding to the ID_j:

$$R_j = R'_j \oplus h\left(b_i B_s||t_s\right)$$

Lastly, $Phone_i$ chooses a random timestamp t'_i and computes the session key between it and the $Sensor_j$:

$$sk_{ij} = h\left(R_j||t'_i||ID_j\right)$$

Then calculates the new PID'_j:

$$PID'_j = ID_j \oplus h\left(R_j||t'_i\right)$$

and then sends the message $m_3 = \left\{PID'_j, C_j, t'_i\right\}$ to $Sensor_j$.

- *Step*4 : When $Sensor_j$ receives the message from $Phone_i$, it will check the freshness of timestamp t'_i and if it does not meet the requirement aborts the session. Otherwise, $Sensor_j$ calculates the $R_j = PUF\left(C_j\right)$ corresponding to C_j by using its PUF chip. And then to verifies:

$$ID_j \stackrel{?}{=} PID'_j \oplus h\left(R_j||t'_i\right)$$

If the verification is passed, computes the session key between it and the $Phone_i$: $sk_{ij} = h\left(R_j||t'_i||ID_j\right)$, otherwise the session is aborted.

If the session key is not successfully generated, the entity without the session key will not send the message, nor can it correctly decrypt the message sent by other parties.

E. PARAMETERS UPDATE PHASE

In this subsection, we design a protocol to update the CR-pair of the HWBAN sensor nodes as follows:

- *Step*1 : $Sensor_j$ randomly selects a large integer C_j' and calculates $R_j' = PUF\left(C_j'\right)$, then encrypts message $\left\{ID_j, C_j', R_j'\right\}_{sk_{ij}}$ with its session key with $Phone_i$ and sends it to $Phone_i$.
- *Step*2 : When the $Phone_i$ received the message from $Sensor_j$, it will decrypt the message with the session key sk_{ij}. Next, it uses the session key sk_{is} to encrypt the message and sends it to the server MS.
- *Step*3 : After MS receives this message, it will utilize the session key between itself and $Phone_i$ to decrypt and update the corresponding CR-pair stored in the database according to the ID_j.

If the process of system parameter update is intercepted by any adversary, the corresponding parameters will not be updated.

F. OFFLINE PASSWORD MODIFICATION PHASE

In this subsection, we design an offline password modification protocol to achieve user-friendliness while ensuring security and improving communication efficiency. As follows:

The $Phone_i$ combines the old password entered by the user and its own ID_i, then verifies the equation:

$$\alpha_i \stackrel{?}{=} h\left(h\left(ID_i\right) \oplus h\left(pw_i||n_i\right) modn_0\right)$$

If the above equation does not hold, then rejects the password modification request. Otherwise, Waiting for the user to enter a new password pw_i' and calculates:

$$\alpha_i' = h\left(h\left(ID_i\right) \oplus h\left(pw_i'||n_i\right) modn_0\right)$$
$$\beta_i' = \beta_i \oplus h\left(pw_i||n_i\right) \oplus h\left(pw_i'||n_i\right)$$

Lastly, the $Phone_i$ replaces α_i and β_i with α_i' and β_i', respectively.

V. SECURITY ANALYSIS

In this section, we compare the proposed scheme with other relevant schemes in terms of security and functionality. Firstly, we describe Mao-Boyd logic primitives and corresponding proof rules. Next, we formally prove the security of our scheme by Mao-Boyd logic. Finally, we will analyze the security, the functionality of our scheme and compare it with the other three related schemes. For convenience, we will use I, J, and S to represent $Phone_i$, $Sensor_j$, and MS, respectively.

A. MAO-BOYD LOGIC

The seven basic modules of Mao-Boyd logic [34] are listed as follows. And the commonly used proof rules are shown in Table 2. They are necessary to understand the formal security proof of our scheme.

1) $I \models J$: The principal I completely believes the formula J to be true.
2) $I \overset{K}{\sim} M$: The principal I encrypts the massage M by utilizing the corresponding key K.
3) $I \overset{K}{\lhd} J$: The principal I can sees the message M by using the decipherment key K.
4) $I \overset{K}{\leftrightarrow} J$: Both I and J regard K as a good shared encipherment key.
5) $\#(N)$: It means that N is a fresh message, which means that it has not been seen before the current round of scheme run.
6) $sup\,(I)$: The principal I is a credible and reliable entity.
7) $I \lhd\!\| M$: The principal I cannot see the message M. This module provides basic logic primitives for the confidentiality of the scheme.

In the process of formal proof of the security of our scheme, we have repeatedly used several rules of the Mao-Boyd logic, listed in Table 2. In these rules, '$\wedge$' represents the logical *AND* operation, '$\vee$' represents the logical *OR* operation. $\{J\}^c$ means objects other than entity J. $N\mathbb{R}M$ represents the message N is transmitted at the same time as M. If two statements A and B are known, and C can be inferred from them, then it can be expressed in Mao-Boyd logic as: $\frac{A \wedge B}{C}$.

TABLE 2. MAO BOYD Logical rules.

Rule Name	Inference Method
Authentication rule	$\frac{I \models I \overset{K}{\leftrightarrow} J \ \wedge \ I \overset{K}{\lhd} M}{I \models J \overset{K}{\sim} M}$
Nonce-verification rule	$\frac{I \models \#(M) \ \wedge \ I \models J \overset{K}{\sim} M}{I \models J \models I \overset{K}{\leftrightarrow} J}$
Confidentiality rule	$\frac{I \models I \overset{K}{\leftrightarrow} J \ \wedge \ I \models S^c \lhd\!\| M \ \wedge \ I \overset{K}{\mid\sim} M}{I \models (S \cup J)^c \lhd\!\| M}$
Super-principal rule	$\frac{I \models J \models X \ \wedge \ I \models sup(J)}{I \models X}$
Intuitive rule	$\frac{I \overset{K}{\lhd} M}{I \lhd M}$
Good Key rule	$\frac{I \models \{I,J\}^c \lhd\!\| K \ \wedge \ I \models \#(K)}{I \models I \overset{K}{\leftrightarrow} J}$
Fresh rule	$\frac{I \models \#(M) \ \wedge \ I \lhd N\mathbb{R}M}{I \models \#(N)}$

B. SYSTEM SECURITY ANALYSIS

In this subsection, we combine the aforementioned Mao-Boyd logic and public-key cryptosystems to analyze the security of the system scheme and list some related cryptographic axioms, and some security lemmas and propositions that need to be proven formally.

axiom 1. According to the assumptions of the proposed scheme, the medical server S is absolutely credible and reliable. The formal description is $I \models sup\,(S)$ is true and $J \models sup\,(S)$ is true.

axiom 2. The smartphone I after successfully completing the identity authentication with the medical server is completely credible and reliable. In other words, when the scheme

progresses to the identity authentication and key agreement phase between the smartphon and sensor node, $J \models sup\,(I)$ is true.

axiom 3. The timestamp used in each round of communication must have never been used before. In other words, the timestamps appearing in this scheme must be fresh.

lemma 1: No $\mathcal{PPT}$ adversary aganist the proposed HWBAN scheme can forge a legal authentication request with a non-negligible probability.

Proof: Assuming that the adversary $\mathscr{A}$ successfully forged the authentication request m_1 sent by the mobile phone to the server, he/she must successfully forge all the contents of m_1, including: $\{PID_i, B_i, \beta_i', t_i, h_i\}$. This means that $\mathscr{A}$ must be able to forge a legal β_i'. According to the HWBAN scheme of this paper, in order to calculate β_i', b_iP_{pub} must be calculated, and according to **the ECCDH assumption** in Section III, it can be known that this is not solvable in $\mathcal{PPT}$.

lemma 2: R_j is a secure shared secret between the phone I and the sensor J.

Proof: In our HWBAN security scheme, the adversary $\mathscr{A}$ cannot forge the PUF response value R_j in the sensor entity participating in the current authentication in $\mathcal{PPT}$. First, according to the **Unpredictablility** characteristic of the PUF chip, even if the adversary $\mathscr{A}$ obtains the R_j in the past several rounds of communication, even if it is very difficult. So he/she cannot know the R_j of the current communication. According to the **Unforgeability** characteristic of PUF, the adversary cannot make a fake chip exactly the same as the PUF chip inside the current communication entity $Sensor_j$. Therefore, the attack method in any $\mathcal{PPT}$ cannot let the adversary know R_j, so R_j is a secure shared secret value between the mobile phone and the sensor.

lemma 3: $\mathcal{PPT}$ adversary aganist the proposed HWBAN scheme cannot forge a legal authentication response with a non-negligible probability.

Proof: In the proof of **lemma 1**, it can be concluded that in order to forge a legal authentication response, the entire content of the message must be forged. If adversary $\mathscr{A}$ wants to forge the response sent by the medical server to the mobile phone, he/she must forge the correct h_s. So we have to forge the correct β_s.According to the scheme, it can be known that the adversary $\mathscr{A}$ must calculate x_sB_i to forge the legal β_s. According to **the ECCDH assumption**, it can be known that this is impossible. Therefore, any adversary $\mathscr{A}$ cannot forge h_s in $\mathcal{PPT}$, so it cannot forge the correct message m_2. According to **lemma 2**, R_j is a secure shared secret value between the mobile phone and the sensor, so the adversary cannot forge PID_j'. Therefore, in $\mathcal{PPT}$, any adversary cannot forge the authentication response m_3 sent by the mobile phone to the sensor.

In our security scheme, to prove the security of the session, we need to prove the security of the session key, these are written as $S \models S \overset{sk_{is}}{\leftrightarrow} I$, $I \models S \overset{sk_{is}}{\leftrightarrow} I$, $I \models I \overset{sk_{ij}}{\leftrightarrow} J$, and $S \models I \overset{sk_{ij}}{\leftrightarrow} J$. In order to prove the security of these two keys, it is necessary to strictly prove the following six propositions.

According to the content of the scheme, in order to simplify the proof, let $sv_1 = x_sb_iP = x_sB_i = b_iP_{pub}$, and $sv_2 = b_sb_iP = b_sB_i = b_iB_s$.

- **Proposition 1.***S* believes that sv_1 is the correct shared secret value between S and I. The corresponding formal description is $S \models S \overset{sv1}{\leftrightarrow} I$
- **Proposition 2.** I believes that sv_1 is the correct shared secret value between S and I. The corresponding formal description is $I \models S \overset{sv1}{\leftrightarrow} I$
- **Proposition 3.***S* believes that sv_2 is the correct shared secret value between S and I. The corresponding formal description is $S \models S \overset{sv2}{\leftrightarrow} I$
- **Proposition 4.** I believes that sv_2 is the correct shared secret value between S and I. The corresponding formal description is $I \models S \overset{sv2}{\leftrightarrow} I$
- **Proposition 5.***I* believes that ID_j is the correct shared secret value between I and J. The corresponding formal description is $I \models I \overset{ID_j}{\leftrightarrow} J$
- **Proposition 6.***J* believes that ID_j is the correct shared secret value between I and J. The corresponding formal description is $J \models I \overset{ID_j}{\leftrightarrow} J$

C. PROVABLE SECURITY

In this subsection, we formally prove the six security propositions put forward in the previous subsection, and then demonstrate the privacy security and key security of our system.

Proposition 1: $S \models S \overset{sv_1}{\leftrightarrow} I$

Proof. To prove this proposition, we need to utilize **Good Key rule**.In other words, this proposition is equivalent to the following two subpropositions:

$$S \models \{S, I\}^c \lhd\!\| \; sv_1 \tag{1}$$

$$S \models \#\,(sv_1) \tag{2}$$

For subproposition (1), we assume that an adversary has obtained all the message in the channel. Because our scheme only sends the public-key during execution, the adversary can only obtain B_i and P_{pub}. But $sv_1 = b_iP_{pub} = x_sB_i$, so no matter how many B_i and P_{pub} the adversary has captured, as long as the adversary is not either of S or I, sv_1 cannot be calculated. Therefore, the subproposition (1) is true.

Then, in order to prove the subproposition (2), we apply the **Fresh rule**, the subproposition is equivalent to the following two subpropositions:

$$S \models \#\,(B_i) \tag{3}$$

$$S \lhd B_1 \mathbb{R} sv_1 \tag{4}$$

For subproposition (4), obviously B_i and sv_1 appear in the same round of session at the same time, so it is true. To prove the correctness of subproposition (3), we again use the **Fresh rule**, the subproposition is equivalent to the following two subpropositions:

$$S \models \#\,(t_i) \tag{5}$$

$$S \lhd B_i \mathbb{R} t_i \tag{6}$$

Because of the existence of **axiom 3**, we can obviously know that subproposition (5) is correct. And through the content of the scheme, we can know that the timestamp t_i and message B_i are sent to S together, so proposition (6) is also correct.

According to the above analysis based on Mao-Boyd logic, proposition 1 is proved to be correct. For clarity, steps prove **Proposition 1** is showed in the *Proof* (7):

$$\frac{S \models \{S,I\}^c \lhd ||sv_1 \wedge \frac{\frac{S\models\#(t_i)\wedge S\lhd B_i\mathbb{R}t_i}{S\models\#(B_i)} \wedge S\lhd sv_1\mathbb{R}B_i}{S\models\#(sv_1)}}{S \models S \overset{sv_1}{\leftrightarrow} I} \tag{7}$$

Proposition 2: $I \models S \overset{sv1}{\leftrightarrow} I$

Proof. To prove this proposition, we need to utilize **Good Key rule**. In other words, this proposition is equivalent to the following two subpropositions:

$$I \models \{S,I\}^c \lhd\!\!\| \ sv_1 \tag{8}$$
$$I \models \#(sv_1) \tag{9}$$

For subproposition (8), we can prove that it is true by using the method of proving subproposition (1) above. Now, if we want to prove the proposition 2, only need to prove subproposition (9). To prove that it is true, according to **Fresh rule**, it is equivalent to proving that the following two subpropositions are true:

$$I \models \#(b_i) \tag{10}$$
$$I \lhd sv_1\mathbb{R}b_i \tag{11}$$

The following proof of subproposition (10): according to the scheme proposed in this paper, it can be known that b_i is generated by entity I, and b_i is generated randomly in each round of communication. Then I believes b_i is fresh, so subproposition (10) is true.

According to the definition above, we know: $sv_1 = b_i P_{pub}$. Obviously, b_i and sv_1 have a one-to-one correspondence. In other words, b_i and sv_1 are a whole, then the subproposition (11) is proved to be correct. And because b_i is fresh, sv_1 is also fresh, so subproposition (9) is true. Combine subproposition (8) and subproposition (9) to know that the proposition 2 is proved to be correct. For intuitiveness, steps prove **Proposition 2** is illustrated in the *Proof* (12):

$$\frac{I \models \{S,I\}^c \lhd ||sv_1 \wedge \frac{I\models\#(b_i)\wedge S\lhd sv_1\mathbb{R}b_i}{I\models\#(sv_1)}}{I \models S \overset{sv_1}{\leftrightarrow} I} \tag{12}$$

Proposition 3: $S \models S \overset{sv2}{\leftrightarrow} I$

Proof. To prove this proposition, we need to utilize **Good Key rule**. In other words, this proposition is equivalent to the following two subpropositions:

$$S \models \{S,I\}^c \lhd\!\!\| \ sv_2 \tag{13}$$
$$S \models \#(sv_2) \tag{14}$$

The proof of subproposition (13) is similar to that of subproposition (1). Since $sv_2 = b_s B_i = b_i B_s$, and any illegal entity that is neither I nor S can not calculate sv_2 when acquiring any number of B_i and B_s. Thus, subproposition (13) is true.

To prove subproposition (14), we only need to prove the following two subpropositions:

$$S \models \#(B_i) \tag{15}$$
$$S \lhd sv_2\mathbb{R}B_i \tag{16}$$

Obviously, subproposition (15) and subproposition (3) are exactly the same, and according to the previous proof, it is also correct. Then subproposition (16) and subproposition (4) can be analogized, B_i and sv_2 are also two elements that appear at the same time in the same round of communication, so they can be regarded as a whole. So the subproposition (14) holds. Thus, subproposition (14) is true. Combining subpropositions (13) and (14), we can get that proposition 3 is proved to be correct. For convenience, steps prove **Proposition 3** is demonstrated in the *Proof* (17):

$$\frac{S \models \{S,I\}^c \lhd ||sv_2 \wedge \frac{\frac{S\models\#(t_i)\wedge S\lhd B_i\mathbb{R}t_i}{S\models\#(B_i)} \wedge S\lhd sv_2\mathbb{R}B_i}{S\models\#(sv_2)}}{S \models S \overset{sv_2}{\leftrightarrow} I} \tag{17}$$

Proposition 4: $I \models S \overset{sv2}{\leftrightarrow} I$

Proof. To prove this proposition, we need to utilize **Good Key rule**.In other words, this proposition is equivalent to the following two subpropositions:

$$I \models \{S,I\}^c \lhd\!\!\| \ sv_2 \tag{18}$$
$$I \models \#(sv_2) \tag{19}$$

According to the proof of proposition 2 above, it can be inferred that subproposition (18) is correct, and subproposition (19) can be equivalent to the following two subpropositions according to the **Fresh rule**:

$$I \models \#(b_i) \tag{20}$$
$$I \lhd sv_2\mathbb{R}b_i \tag{21}$$

According to the subpropositions (10) and (11) that have been proved above, the above two subpropositions can be proved by analogy, so proposition 4 is correct. For convenience, steps prove **Proposition 4** is showed in the *Proof* (22):

$$\frac{I \models \{S,I\}^c \lhd ||sv_2 \wedge \frac{I\models\#(b_i)\wedge S\lhd sv_2\mathbb{R}b_i}{I\models\#(sv_2)}}{I \models S \overset{sv_2}{\leftrightarrow} I} \tag{22}$$

Proposition 5: $I \models I \overset{ID_j}{\leftrightarrow} J$

Proof: To prove this proposition, we need to utilize **Good Key rule**.In other words, this proposition is equivalent to the following two subpropositions:

$$I \models \#\left(ID_j\right) \tag{23}$$
$$I \models \{I,J\}^c \lhd ||ID_j \tag{24}$$

For subproposition (23), according to our scheme, it can be known that the mobile phone I is authorized by S after

the identity authentication and key agreement of the medical server S and obtains the ID_j of the sensor. Therefore, the ID_j is completely trustworthy for the mobile phone, so subproposition (23) is true.

For subproposition (24), according to the **Confidentiality rule**, it is equivalent to the following three subpropositions:

$$I \models I \overset{R_j}{\leftrightarrow} J \tag{25}$$
$$I \models \{I\}^c \lhd ||ID_j \tag{26}$$
$$I \overset{R_j}{\mid\sim} ID_j \tag{27}$$

For the above three subpropositions, first, according to **lemma 1**, know that subproposition (25) is correct. Secondly, before entity I has completed authentication with J, I must believe that other entities cannot know ID_j, so subproposition (26) is true. Finally, according to the proposed scheme can know that I has completed the encryption of ID_j with R_j, so subproposition (27) is true. In summary, the above three subpropositions are all true, so proposition 5 is proved to be correct. For clarity, steps prove **Proposition 5** is illustrated in the *Proof* (28):

$$\frac{I \models \#\left(ID_j\right) \wedge \frac{I \models I \overset{R_j}{\leftrightarrow} J \wedge I \models \{I\}^c \lhd ||ID_j \wedge I \overset{R_j}{\mid\sim} ID_j}{I \models \{I,J\}^c \lhd ||ID_j}}{I \models I \overset{ID_j}{\leftrightarrow} J} \tag{28}$$

Proposition 6: $J \models I \overset{ID_j}{\leftrightarrow} J$

Proof: To prove this proposition, we need to utilize **Good Key rule**.In other words, this proposition is equivalent to the following two subpropositions:

$$J \models \#\left(ID_j\right) \tag{29}$$
$$J \models \{I, J\}^c \lhd ||ID_j \tag{30}$$

For entity J, ID_j is the response sent by entity I in the form of a pseudonym, so proving that subproposition (29) is equivalent to proving the following two subpropositions:

$$J \models \#\left(t_i'\right) \tag{31}$$
$$J \lhd ID_j \mathbb{R} t_i' \tag{32}$$

Referring to **axiom 3** and the previous related proofs, we can know that the above two subpropositions are obviously established, so subproposition (29) is proved to be correct.

Next, according to **Super-principal rule**, we can equivalently convert the subproposition (30) into the following two subpropositions:

$$J \models I \models \{I, J\}^c \lhd ||ID_j \tag{33}$$
$$J \models sup\,(I) \tag{34}$$

The entity I at this time has completed the identity authentication and key agreement with the medical server S. According to **axiom 2**, the entity I at this time is completely credible to J, so the subproposition (34) is obviously true. Then according to **Confidentiality rule**, proving subproposition (33) is equivalent to proving the following three subpropositions:

$$J \models I \models I \overset{R_j}{\leftrightarrow} J \tag{35}$$
$$J \models I \models \{I\}^c \lhd ||ID_j \tag{36}$$
$$J \models I \overset{R_j}{\mid\sim} ID_j \tag{37}$$

Referring to the previous analysis, subproposition (36) is obviously true. Next, prove subproposition (35). According to **Nonce-verification rule**, it is equivalent to the following two subpropositions:

$$J \models \#\left(ID_j\right) \tag{38}$$
$$J \models I \overset{R_j}{\mid\sim} ID_j \tag{39}$$

First, subproposition (38) is equivalent to subproposition (29), so it is true. Second, according to **Authentication rule**, subproposition (39) is equivalent to the following two subpropositions:

$$J \models I \overset{R_j}{\leftrightarrow} J \tag{40}$$
$$J \overset{R_j}{\lhd} ID_j \tag{41}$$

According to **lemma 2**, we can know that subproposition (40) is true. Then according to the proposed scheme, we can know that the subproposition (41) is obviously true. In summary, subproposition (39) is proved to be correct. So subproposition (35) is true.

Then the subproposition (37) is exactly the same as the subproposition (39), so the subproposition (37) is also correct. Based on the above analysis, proposition 6 is formally proved to be correct. For convenience, steps prove **Proposition 6** is demonstrated in the *Proof* (42), as shown at the bottom of the next page.

D. PERFORMANCE COMPARISONS

In this subsection, we compare the proposed HWBAN scheme with various IoT key agreements such as [6], [35], and [9] with similar network models in terms of security functions. For convenience, we mark $SF-1$, $SF-2$, $SF-3$, $SF-4$, $SF-5$, $SF-6$, $SF-7$, $SF-8$, $SF-9$, $SF-10$, $SF-11$, $SF-12$ and $SF-13$ denote Mutual Authentication, Identity Protection, Message Integrity, Low-entropy Secrets Guessing Attack, Impersonation Attack, Replay Attack, Perfect Forward Secrecy, Physical Security, Formal Security Proof, Desynchronization Attack, Offline Password Modification, Un-traceability, Intermediary device participates in secure communication respectively. The security comparisons and contrasts of the four IoT schemes are listed in Table 3.

From this section onwards, we use *Ref*. [35], *Ref*. [6] and *Ref*. [9] to replace the schemes of Alladi *et al.* [35], Lo *et al.* [6] and Alladi *et al.* [9]

TABLE 3. Comparisons and contrasts of security functions.

Functions	$Ref.$ [34]	$Ref.$ [5]	$Ref.$ [8]	Proposed scheme
SF-1	√	√	√	√
SF-2	×	×	√	√
SF-3	√	√	√	√
SF-4	√	√	√	√
SF-5	√	√	√	√
SF-6	√	×	√	√
SF-7	√	√	√	√
SF-8	√	×	√	√
SF-9	√	√	√	√
SF-10	×	√	×	√
SF-11	∅	∅	∅	√
SF-12	√	√	√	√
SF-13	∅	∅	∅	√

In the table above, the symbol √ indicates that the corresponding function is realized in the scheme, × indicates that it is not realized, and ∅ indicates that such a function is not involved.

Next, we further analyze the result of comparison of Table3. In the scheme of *Ref*. [35], the identities of sensors and access nodes are exposed on public channels. In addition, although the identity of each participant will be updated after the end of the session, but the way to update is $(ID_P)^* = H\,(ID_P||ID_W||R^c)$ and $(ID_W)^* = H\,(ID_W||ID_P||R^c)$. So any party can calculate not only its own new ID but also the IDs of other participants. Finally, but also very noteworthy is that in its identity modification phase. Once any party goes offline unexpectedly, it will not be able to update its own identity, and at this time other participants have already updated its identity. It will cause a desynchronization attack and the next round of identity authentication cannot be performed normally.

Not only that, *Ref*. [6] has some security risks. The protection of identity privacy also exists deficiencies for the same reason. However, the most important is that it can get all challenge-response pairs from PUF. However, this is very difficult. If this can be done, it means that it's PUF circuit has a relatively limited number of bits, which will have a great impact on physical security.

In the scheme of *Ref*. [9] also hidden dangers of desynchronization attacks. Assuming that in the last step, when the communicating entities are updating their own identity, the power is suddenly cut off, and the power-off entity fails to update the identity, but at this time the server has completed whose identity update. Then the next round of conversation will not be conducted.

TABLE 4. Cryptographic operations costs.

Operation	Running Times(ms)
Point Multiplication Operation	1.84
SHA256 Operation	0.006
PUF Operation	0.12
AES Operation	0.88

VI. EFFICIENCY ANALYSIS

In this section, we analyze the computing and communication costs of the proposed scheme in detail. At the same time, we also compare the computing and communication costs between our scheme and several other schemes *Ref*. [35], *Ref*. [6], and *Ref*. [9] with similar network model.

A. ANALYSIS OF COMPUTATION COST

We present the running time of various operations performed in the proposed scheme and we compare the results with those obtained from *Ref*. [35], *Ref*. [6] and *Ref*. [9] in this section. We use the following notations for the following running times in this paper:

- T_p: The running time of a operation running on the PUF chip.
- T_m: The running time of a multiplication Operation on the addition group of elliptic curve G.
- T_h: The running time of a secure SHA256 hash operation in Z_q^*.
- T_a: The running time of a secure AES operation with 256 bits.

Our experimental environment for implementing the scheme in this paper is the Windows 10 Professional operating system, with an Intel(R) Core(TM) i5-8300H central CPU, a clock frequency of 2.30 GHz, and a RAM of 8.00 GB. In order to better implement related cryptographic operations, we adopt the MIRACL library and C language to program. In order to ensure the accuracy of the experiment, we use 10,000 rounds of repeated measurements to take the average and use the high-precision timer QueryPerformanceFrequency function based on the Windows system API to repeatedly obtain the running time of each cryptographic operation. However, because the instruments and equipment that implement PUF operation are relatively rare, but from [36], it can be concluded that the running time of PUF, which is summarized in Table 4.

In addition, we assume that the running time of the *MAC* and the non-linear function $F(\cdot)$ is close to that of the secure hash SHA256 operation. In other words,

$$\frac{\dfrac{J\models\#(t_i')\wedge J\lhd ID_j\mathbb{R}t_i'}{J\models\#(ID_j)}\wedge\dfrac{\dfrac{J\models\#(ID_j)\wedge J\models I\overset{R_j}{\sim}ID_j}{J\models I\overset{R_j}{\leftrightarrow}J}\wedge J\models I\models\{I\}^c\lhd||ID_j\wedge\dfrac{J\models I\overset{R_j}{\leftrightarrow}J\wedge J\overset{R_j}{\lhd}ID_j}{J\models I\overset{R_j}{\sim}ID_j}}{J\models I\models\{I,J\}^c\lhd||ID_j}\wedge J\models sup(I)}{J\models\{I,J\}^c\lhd||ID_j}$$
$$J\models I\overset{ID_j}{\leftrightarrow}J \tag{42}$$

$T_{MAC} \approx T_F \approx T_h = 0.006ms$. Next, we will use the operating schedule of cryptographic operations obtained from the above experiment to compare and analyze the computation costs of other schemes.

By analyzing the scheme proposed of *Ref*. [35], the sensor needs to perform seven times SHA256 hash operations, once AES operation and once PUF operation. Therefore, its computation costs is $7*T_h+1*T_a+1*T_p = 1.042\ ms$. The access needs to perform twelve times SHA256 hash operations, twice AES operation and once PUF operation. Therefore, its computation costs is $12 * T_h + 2 * T_a + 1 * T_p = 1.952\ ms$. In this scheme, the server performs five times SHA256 hash operations and once AES operation, so its computation costs is $5 * T_h + 1 * T_a = 0.91\ ms$. To sum up, the computation costs of the scheme proposed by *Ref*.[35] to execute a round of key agreement is 3.904 *ms*.

Then we analyze the scheme proposed by *Ref*. [6] In its scheme, the sensor node needs to perform twice SHA256 hash operations and once PUF operation. So the computation costs of the sensor is $2*T_h+1*T_p = 0.132\ ms$. In addition, its WP node performed three times SHA256 hash operations. This WP node is equivalent to the access node in the proposed scheme by *Ref*.[35] and the entity phone of our scheme. Its run time is $3*T_h = 0.018\ ms$. The server run once SHA256 and once PUF operation, so its computation costs is $1 * T_h + 1 * T_p = 0.126\ ms$. Overall, the total computation costs of key agreement of the proposed scheme by *Ref*.[6] is 0.456 *ms*.

In the scheme of *Ref*. [9], The sensor node performs five times SHA256 and once PUF operation whose computation costs is $5 * T_h + 1 * T_p = 0.150\ ms$. The access node in the scheme has completed ten times SHA256 operations and onece PUF operation, so its run time is $10 * T_h + 1 * T_p = 0.180\ ms$. Besides, the server in the scheme of it performs five times SHA256 operations, so its computation costs is $5*T_h = 0.030\ ms$. In a nutshell, the total computation costs of key agreement of the proposed scheme by *Ref*.[9] is 0.360 *ms*.

However, in our proposed scheme, sensor node only perform twice SHA256 operations and once PUF operation. Therefore, the computation costs of the sensor is only $2*T_h+1*T_p = 0.132\ ms$. Eleven times SHA256 operations and three times point multiplication operations are performed on the smartphone. So the computation costs on the smartphone is $11 * T_h + 3 * T_m = 5.586\ ms$. The server has completed seven times SHA256 operations and three times point multiplication operations, so its computation costs is $6*T_h+3*T_m = 5.556\ ms$. In summary, the total computation costs of the scheme we propose in this paper is 11.274 *ms*.

The comparison of computation costs is demonstrated in Table 5. The computing power of sensors is relatively weak in HWBAN applications. Therefore, the practicability, reliability, and real-time of the HWBAN system largely depend on the computation costs of the sensor nodes. With this in mind, we illustrate the comparison of the computation costs of the sensor nodes of the four schemes in Fig 4. Combining Fig 4 and Table 5, we can analyze that the proposed scheme

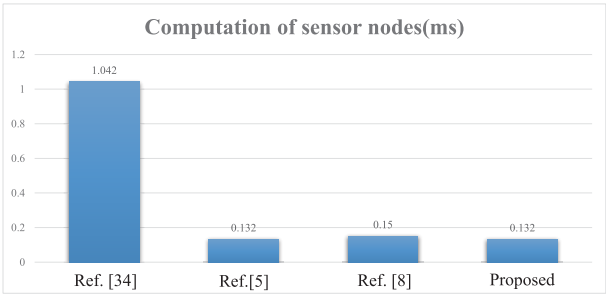

FIGURE 4. The computation costs of sensor nodes in the four schemes.

lets smartphones and servers with strong computing power bear most of the computing burden of the HWBAN system, while the costs of sensor nodes with weak computing power are tiny. Specifically, the computation costs of the sensor node of our proposed scheme is 0.222 ms, which is better than the scheme proposed by *Ref*. [35] and *Ref*. [9] It is the same as the scheme proposed by *Ref*. [6] However, the comparative analysis of security in Section V-D shows that our scheme is more secure than them.

B. ANALYSIS OF COMMUNICATION COSTS

According to the above implementation, we know that the lengths of SHA256 and the point on the elliptic curve are 256 bits and 320 bits respectively. Suppose the length of the user's identity is 64 bits and the random number is 128 bits, the timestamp is 32 bits, the PUF challenge-response pair is 128 bits. The communication costs are analyzed as follows:

In the scheme proposed by *Ref*. [35] The length of the message sent by the patient node is 384 bits in total, and the number of sending is once. Then the message sent by the wireless link node reaches 1472 bits, and the number of times the message is sent is three times. Finally, the total length of the content sent by the server is 640 bits, and the number of times the message is sent is once. Therefore, the communication costs of the entire scheme are $384 + 1472 + 640 = 2496\ bits$.

In the scheme proposed by *Ref*. [6] The length of the message sent by the sensor node is 448 bits in total, and the number of sending is twice. Then the message sent by the WP node reaches 704 bits, and the number of times the message is sent is twice. Finally, the total length of the content sent by the server is 512 bits, and the number of times the message is sent is once. Therefore, the communication costs of the entire scheme are $448 + 704 + 512 = 1664\ bits$.

In the scheme proposed by *Ref*. [9] The length of the message sent by the sensor node is 832 bits in total, and the number of sending is once. Then the message sent by the leader drone reaches 1792 bits, and the number of times the message is sent is five. Finally, the total length of the content sent by the server is 896 bits, and the number of times the message is sent is twice. Therefore, the communication costs of the entire scheme are $832 + 1792 + 896 = 3520\ bits$.

Then, in our scheme. The length of the message sent by the sensor node is 0 bits in total, and the number of sending

TABLE 5. Computation costs contrast.

schemes		*Ref*. [34]	*Ref*. [5]	*Ref*. [8]	Proposed scheme
Key Agreement Phase	Sensor Node	$7 * T_h + T_a + T_p = 1.042ms$	$2 * T_h + T_p = 0.132ms$	$5 * T_h + T_p = 0.150ms$	$2 * T_h + T_p = 0.132ms$
	Phone Node	$12 * T_h + 2 * T_a + T_p = 1.952ms$	$3 * T_h = 0.018ms$	$10 * T_h + T_p = 0.180ms$	$11 * T_h + 3 * T_m = 5.586ms$
	Medical Server	$5 * T_h + T_a = 0.91ms$	$T_h + T_p = 0.126ms$	$5 * T_h = 0.030ms$	$6 * T_h + 3 * T_m = 5.556ms$

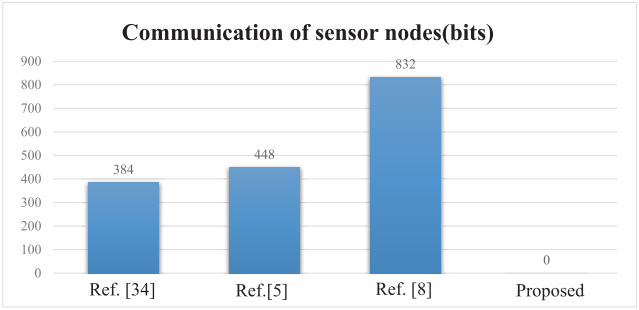

FIGURE 5. The communication costs of sending by sensor nodes in the four schemes.

is zero times. Then the message sent by the leader drone reaches 1536 bits, and the number of times the message is sent is twice. Finally, the total length of the content sent by the server is 1120 bits, and the number of times the message is sent is once. Therefore, the communication costs of the entire scheme are $0 + 1536 + 1120 = 2656\,bits$.

The communication costs of sending by sensor nodes in the four schemes is shown in Fig 5. From Fig 5 we can see that the communication costs of sending by sensor nodes in our scheme are 0 bit, which will greatly improve the battery life and stability of the HWBAN system. In addition, the communication costs by four scheme analysis, we can find the number of communications performed by our scheme is the least among other similar, which not only improves the efficiency of the HWBAN system, and more to enhance system security.

In summary, our proposed scheme has amplified security and lower computation and communication costs than the related HWBAN protocol proposed in recent years. Therefore, our HWBAN scheme is more practical for smart medical applications. In addition, the offline password modification protocol proposed by this paper ensures the security of the password and makes the system more stable and reliable.

VII. CONCLUSION

Aiming at the deficiencies of security, availability, and efficiency in the existing HWBAN system. Our paper proposes a secure and lightweight HWBAN scheme using PUF and password. The proposed scheme uses only fewer ECC point operations, XOR operations, PUF functions, and hash functions. In addition, the proposed authentication protocol uses passwords flexibly and designs corresponding offline password modification protocols, which reduces communication costs and improves security and usability. At the same time, it is also a practical HWBAN system by implementing a sensor-phone-server three-layer network security communication, allowing users to know their health status through their mobile phones at any time. Formal security proof and performance analysis demonstrate the proposed protocol meets more security and usability requirements and takes less computation and communication costs than related protocols proposed recently.

REFERENCES

[1] D. B. Baker, "The study of stress at work," *Annu. Rev. Public Health*, vol. 6, no. 1, pp. 367–381, 1985.
[2] L.-J. Liu and Q. Guo, "Life satisfaction in a sample of empty-nest elderly: A survey in the rural area of a mountainous county in China," *Qual. Life Res.*, vol. 17, no. 6, pp. 823–830, Aug. 2008.
[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, Jan. 2014.
[4] A. Milenković, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Comput. Commun.*, vol. 29, nos. 13–14, pp. 2521–2533, 2006.
[5] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.
[6] N.-W. Lo and A. Yohan, "BLE-based authentication protocol for micropayment using wearable device," *Wireless Pers. Commun.*, vol. 112, no. 4, pp. 2351–2372, Jun. 2020.
[7] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 47–69, Mar. 2021.
[8] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.
[9] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, Jul. 2020.
[10] M. Katagi *et al.*, "Lightweight cryptography for the Internet of Things," Sony Corp., 2008, pp. 7–10, vol. 2008.
[11] M. A. Hanson, H. C. P. Jr, A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor, and J. Lach, "Body area sensor networks: Challenges and opportunities," *Computer*, vol. 42, no. 1, pp. 58–65, 2009.
[12] Y. Xie, X. Li, S. Zhang, and Y. Li, "*iCLAS*: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks," *IEEE Access*, vol. 7, pp. 15170–15182, 2019.
[13] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technol. J.*, vol. 24, no. 2, pp. 138–144, Apr. 2006.
[14] J. A. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Lin, S. Son, R. Stoleru, and A. Wood, "Wireless sensor networks for in-home healthcare: Potential and challenges," in *Proc. High Confidence Med. Device Softw. Syst. (HCMDSS) Workshop*, 2005, pp. 1–4.
[15] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.

[16] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," *Future Gener. Comput. Syst.*, vol. 108, pp. 1287–1296, Jul. 2020.
[17] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.
[18] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102502.
[19] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[20] S. Garg, K. Kaur, G. Kaddoum, and M. Client, "ECC-based secure and provable authentication mechanism for smart healthcare ecosystem," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[21] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.
[22] S. Li, T. Zhang, B. Yu, and K. He, "A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT," *IEEE Sensors J.*, vol. 21, no. 4, pp. 5487–5501, Feb. 2021.
[23] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustain. Comput., Inform. Syst.*, vol. 18, pp. 80–89, Jun. 2018.
[24] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurrency Computation: Pract. Exper.*, vol. 31, no. 14, p. e5295, Jul. 2019.
[25] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 43, no. S1, pp. 619–636, Jul. 2019.
[26] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, Nov. 2019.
[27] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen, and R. Struik, "Security considerations in the IP-based Internet of Things draft-garciacore-security-06," *Internet Eng. Task Force*, 2013.
[28] M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, "A PUF based light weight protocol for secure WiFi authentication of IoT devices," in *Proc. 8th Int. Symp. Embedded Comput. Syst. Design (ISED)*, Dec. 2018, pp. 183–187.
[29] W. Liang, S. Xie, J. Long, K.-C. Li, D. Zhang, and K. Li, "A double PUF-based RFID identity authentication protocol in service-centric Internet of Things environments," *Inf. Sci.*, vol. 503, pp. 129–147, Dec. 2019.
[30] M. S. Alkatheiri, A. R. Sangi, and S. Anamalamudi, "Physical unclonable function (PUF)-based security in Internet of Things (IoT): Key challenges and solutions," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, 2020, pp. 461–473.
[31] S. Kardaş, S. Çelik, M. Yıldız, and A. Levi, "PUF-enhanced offline RFID security and privacy," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 2059–2067, 2012.
[32] S. Wook Jung and S. Jung, "HRP: A HMAC-based RFID mutual authentication protocol using PUF," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2013, pp. 578–582.
[33] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[34] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *Proc. 6th Comput. Secur. Found. Workshop*, 1993, pp. 147–158.
[35] T. Alladi, V. Chamola, and Naren, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 361–369, Feb. 2021.
[36] R. D. Smet, T. Vandervelden, K. Steenhaut, and A. Braeken, "Lightweight PUF based authentication scheme for fog architecture," *Wireless Netw.*, vol. 27, no. 2, pp. 947–959, Feb. 2021.