IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 11, 2019, accepted October 5, 2019, date of publication October 9, 2019, date of current version October 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946400

Low-Overhead Remote User Authentication Protocol for IoT Based on a Fuzzy Extractor and Feature Extraction

BAHAA HUSSEIN TAHER[1,2], SHENG JIANG[1], ALI A. YASSIN[3], AND HONGWEI LU[1]

[1]School of Computer Science, Huazhong University of Science and Technology, Wuhan 400037, China
[2]Department of Mathematics, College of Science, University of Basrah, Basrah 61004, Iraq
[3]Department of Computer Science, Education College of Pure Science, University of Basrah, Basrah 61004, Iraq

Corresponding authors: Bahaa Hussein Taher (bahaa_china@hust.edu.cn) and Sheng Jiang (jwt@hust.edu.cn)

ABSTRACT The Internet of things (IoT) is a system of smart technologies and services that mutually communicate data between users and devices or between devices via the Internet. Since data are shared between a remote user and various sensing devices over a network, it is essential to design a secure, lightweight and efficient remote user authentication protocol for the IoT environment. In the context of security and network privacy, mutual authentication is necessary for securely accessing the services of the IoT environment. However, the IoT faces substantial new challenges realizing mutual authentication due to IoT devices constraints. In this paper, we present a lightweight, robust and secure authentication protocol that satisfies constraints on IoT devices. The proposed protocol is based on level 3 feature extraction, fuzzy extraction of the user's biometrics, one-way hash functions and XOR operations and includes (1) three-factor authentication (user password, biometrics and smart devices), (2) mutual authentication, (3) a session key, and (4) key freshness. Furthermore, we have used the Burrows–Abadi–Needham logic to prove the authentication of our proposed protocol. In addition, our proposed protocol does not require additional hardware or a resource-constrained cryptosystem, and for that reason; hence, it has the lowest computational cost on the IoT nodes (0.003_ms), the lowest total computational cost (0.071_ms), and the lowest communication cost (2784 bits) compared with other relevant works. Moreover, we have conducted an informal security analysis to prove its ability to withstand well-known malicious attacks, such as replay attacks, impersonation attacks, password change attacks, man-in-the-middle (MITM) attacks, and denial of service (DOS) attacks.

INDEX TERMS BAN logic, bio-authentication, fuzzy extractor, level 3 feature extraction, IoT, key agreement.

I. INTRODUCTION

IoT is the integration of heterogeneous physical devices with embedded software, networks and information technology, with the ability to share information and provide optimal service to users without manual intervention. IoT improves our daily lives by offering highly intelligent services and facilities such as the smart home [1], smart healthcare [2], smart transportation [3], smart cities [4] and smart industries [5]. However, the technical integration of smart devices and the IoT also has adverse effects, such as threats to security and privacy due to the ability of these devices to store critical user information. The issues that are related to IoT security consist of illegal access to information, authentication, and authorization; privacy; tracking of the data stream; platform management and organization; data integrity; and data confidentiality [6], [7]. User authentication has increasingly become the most vital issue due to the growing concern with user IoT security and privacy leakage. Three major factors are used to perform authentication [8]–[10]:

- Device: what the user owns (e.g., smart card, smartphone, USB stick, or token);
- Ownership: what the user knows (e.g., PIN code, password, or TAN);
- Inherence: user authentication (e.g., iris scan, fingerprint, or typing speed).

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

Many user authentication schemes have been proposed in the literature that are based on single factors such as passwords [11]–[13]. However, such schemes are easy for attackers to breach [14]. Therefore, authentication requires an additional factor such as the user's biometrics to enhance security and to enable robust user authentication. The biometric factors have the following advantages [15]:

- Everyone possesses a universal factor;
- They never break;
- They are fixed over time;
- They are easy to measure using any available device;
- They cannot be easily guessed;
- They provide a unique identifier; and
- They cannot be lost or forgotten.

Therefore, by using the biometric factors, a strong authentication protocol can be developed and applied in many public institutions to ensure the security and privacy of sensitive information.

In this paper, based on user biometric factors, we have focused on remote user authentication, which is one of the main security issues of the IoT. Several authentication schemes have been proposed in the literature for IoT and WSN, in which the user connects to a gateway node initially so that he/she can access IoT nodes. The scenario and structure of our proposed protocol consist of three major parties: the user who requires access, the IoT nodes and the gateway node. In this case, the user can access IoT nodes and take advantage of their services.

A. MOTIVATION

The IoT has provided many opportunities for society in many areas of life, such as industry, agriculture, healthcare and warehousing, which have become accessible to all with ease and flexibility. This rapid development has led to the emergence of many challenges. Therefore, the essential motivation factors behind the design of our proposed protocol are as follows:

- The IoT sensing device operates with limiting factors such as battery, memory, and power; the authentication protocol must have low overheads in terms of computation and communication costs.
- Malicious attacks have become huge and varied in terms of methodology and severity, such as replay attacks, impersonation attacks, man-in-the-middle (MITM) attacks, and denial of service (DOS) attacks. Therefore, it is necessary to design a secure user authentication protocol for resisting such attackers.
- Moreover, due to the nature of IoT devices such as sensors and actuators, which deal with critical user data, IoT applications must be more secure.
- Several authentication protocols rely on authentication using a password, smart device or smart card, or more than one of these. However, these schemes are not sufficient for ensuring security. Therefore, authentication requires another factor for enhancing security, such as the user's biometrics, which are unique, e.g., iris scans, fingerprints and facial patterns. These biometrics are difficult to reproduce; thus, it is difficult for an attacker to steal or modify them.

B. OUR CONTRIBUTIONS

Our main contributions in this paper are as follows:

- An authentication model for the IoT environment is presented and the security challenges that are involved and their requirements are discussed.
- A low-overhead remote user authentication scheme that is based on a fuzzy extractor and feature extraction is proposed for addressing these issues.
- A formal security analysis that uses BAN logic and an informal security analysis are presented, which demonstrate that the scheme is secure.
- Finally, it is demonstrated that the protocol is more efficient in terms of communication and computational cost.

C. PAPER ORGANIZATION

The remainder of this paper is organized as follows: discussion of related work (Section II); security issues in the IoT and WSN environments (Section III); descriptions of the proposed protocol (Section IV); security analysis and discussion (Section V); performance analysis and functionality comparison (Section VI); and conclusions (Section VII).

II. RELATED WORK

Authentication and access controls play a crucial role in a secure and efficient heterogeneous network. The resources of IoT devices are characterized by being restricted; hence, substantial challenges are encountered in the design of a powerful, effective and balanced user authentication system for the IoT and WSN environments.

In 2014, Das [16] and Turkanovi? *et al.* [17] introduced user authentication schemes that were based on two and three factors for the WSN and IoT environments, respectively. However, their schemes have several security flaws, such as not providing user anonymity and being vulnerable to malicious attacks such as impersonation attacks, password change attacks, and gateway node bypassing attacks. In 2015, Porambage *et al.* [18] designed a two-group key agreement for multicasting in WSNs under constrained resources. However, the scheme has a higher security risk, does not realize most of the security features such as user anonymity, and does not secure against insider attacks, (DOS) attacks, or replay attacks [19]. In 2016, Amin *et al.* [20] and Farash *et al.* [21] presented a user-authenticated protocol for IoT networks and claimed that it was secure. However, Amin's and Farash's scheme is vulnerable to several well-known malicious attacks such as DoS attacks, off-line password guessing attack, the sensor node impersonation attack and the stolen verifier attacks, and replay attacks [22], [23]. In 2017, Dhillon and Kalra [24], and Yazdanpanah *et al.* [25] introduced multifactor authentication schemes for the IoT environment. However, these schemes are not lightweight due to their huge overheads. In 2018, many multifactor user authentication

schemes were presented (Challa *et al.* [26], He *et al.* [27], Ryu *et al.* [28], Wazid *et al.* [29], Li *et al.* [30]) for the IoT environment. Unfortunately, Wazid's scheme is suffering from security weakness [31]; while, Challa's, He's, Ryu's, and X. Li's scheme have high computation and communication overheads. Research and studies on the context of the IoT and WSNs continue to this day. In 2019, several articles and investigations emerged (Lyu *et al.* [32], Ma *et al.* [33], Martínez-Peláez *et al.* [34], Renuka *et al.* [35]). However, these contributions still have weaknesses, especially in terms of the computation and communication overheads, which are large compared to our proposed protocol.

From the literature survey that is presented in this section, we observed the following:

- Most of the protocols cannot withstand several types of malicious attacks, such as replay attacks, impersonate attack, password guessing attack, (DOS) attacks, (MITM) attacks, etc. Moreover, most of the existing protocols do not provide security features such as mutual authentication, user anonymity, forward secrecy, scalability, etc.
- The existing protocols suffer from very high computation and communication overheads.
- In addition, some of the literature was based on a single factor or two factors, such as user passwords or passwords and smart cards. Generally, such schemes risk being invaded by malicious attackers if the password is leaked or the smart card is stolen. However, in the case of a password leak or loss of a smart card, any malicious attacker can penetrate the system using powerful analysis.

To overcome the shortcomings of related works, in this paper, we have proposed a secure and efficient protocol that is based on three factors: a password, biometrics with feature extraction by a fuzzy extractor, and a smartphone. Furthermore, in our proposed protocol, there is no need for additional hardware and the user can use his smartphone to imprint and save his/her biometrics. Using those features, our proposed protocol is more secure, efficient, and suitable for the constrained resources of IoT applications.

III. SECURITY ISSUES IN IOT ENVIRONMENT

IoT security is the most critical issue that is encountered in the design of IoT applications. Therefore, providing robust security for Internet of things technologies is a major challenge and requires serious consideration. IoT has a bright future in the Internet world. Thus, security issues such as privacy and authentication are vital for the realization fo the benefits and services of modern technologies. Consequently, the following issues must be considered carefully.

A. ATTACK MODEL

Many IoT devices exist in an unattended environment and require the active investigation of all possible scenarios in which a hacker can attack the IoT system. The following are possible malicious attacks on IoT devices:

- **Denial of service attack:** This malicious attack reduces network capacity by flooding the network with many anonymous login messages, thereby making services unavailable.
- **Impersonation attack:** A malicious attacker might masquerade as a legal user or server by replying to valid request messages from a previous communication between any two legitimate objects, thereby obtaining the same authorization and service as a legitimate user or server.
- **Man in the middle attack:** In this type of attack, the attacker may attempt to secretly interrupt the communication line messages between a legitimate user and the trusted server/gateway to masquerade as a legal user or the server by using analysis attack methods.
- **Eavesdropping attack:** An adversary listens to ongoing private communication messages and launches an attack on a legitimate user later.
- **Password change attack:** An attacker might try to become a legitimate user or object by changing the user password to access IoT services. Such attacks often occur in schemes that utilize passwords as the authentication factor.
- **Parallel session attack:** An adversary listens to the communications between legitimate IoT system objects and tries to establish a parallel session to capture previous messages.
- **Stolen smart device attack:** Using s stolen smart device, an adversary can extract sensitive information, using which he/ she can impersonate himself as a legal user or object to attack the system.
- **Gateway node bypassing attack:** An attacker might try to gain full access to the IoT sensor node by bypassing the gateway node to obtain IoT services and sensitive information without gateway authentication.
- **Offline guessing attack:** A malicious attacker might try to gain access to the IoT system by guessing all possible passwords using an offline dictionary attack.

B. SECURITY FEATURE REQUIREMENTS

Several security keys must be considered in the design of any authentication protocol. In this subsection, we discuss these features.

- **Mutual authentication:** Any two parties must authenticate each other's identities at the same time mutually prior to the communication to avoid adversaries.
- **User anonymity:** The identity of a legitimate user must be safe from attempts by any adversary to obtain it by eavesdropping on messages that are exchanged legitimately at the login or authentication phase. If the user's real identity is revealed to the attacker, it can be used to launch security attacks.
- **Confidentiality:** Protection of sensitive personal user information or communication messages by making them visible only to legitimate entities.

- **Availability:** IoT resources must be available any time the user requires access to the system.
- **Forward secrecy:** Access to any protocol must be granted by providing the session key. In addition, an earlier session key must not be used to start a new session.
- **Scalability:** An authentication system must adapt to all changes that occur in the surrounding environment and allow the system objects to grow dynamically and according to the changes that occur.
- **Attack resistance:** The protocol must withstand most possible attacks such as impersonation attacks, denial of service attacks, replay attacks, and man-in-the-middle attacks.

IV. PROPOSED PROTOCOL

In this section, we present our proposed protocol for remote user authentication, which is based on three factors and consists of four phases: a registration phase, a login phase, an authentication phase and a password change phase.

A. NETWORK MODEL SCENARIO AND PROBLEM DEFINITION

The IoT applications can be accessed directly by the user anywhere and at any time using the user's smartphone. Most protocols are based on one or two factors, which will increase the security risk from, e.g., replay attacks, denial of service attacks, and impersonation attacks [36]. To overcome these shortcomings, our proposed protocol adopts a three-factor authentication protocol. The third-level features of the user's iris are encrypted, along with the anonymity of the user and the password. Then, we apply the fuzzy extractor on the encrypted template of the user's iris; this is the first factor. The second factor is the user's smartphone, while the third factor is the user's password. This is the main difference between our protocol and the traditional biometrics authentication protocols. Fig. 1 illustrates the difference between our protocol and other related protocols.

Several authentication protocols have been designed recently. Our network model is presented in Fig. 2. We have adopted the fifth model that was proposed by Xue *et al.* [37], which is in keeping with the Internet environment and WSN. Our proposed network model involves three parties: (1) the remote user U_i who aims at gaining access to the IoT application, (2) several IoT sensor-embedded devices N_k, (3) and the trusted gateway node GW. Additionally, since the IoT sources/nodes are constrained in terms of energy, memory, and battery, our proposed protocol depends on the user and utilizes distributed and embedded nodes. In this model, the user can use his/her smartphone to access IoT nodes with the help of the local Internet or cloud service provider. Meanwhile, the proposed protocol is executed among the remote user, the IoT sensor nodes, and the gateway nodes; all data passes through and is authenticated by it to establish secure communications between the user and the sensor nodes.

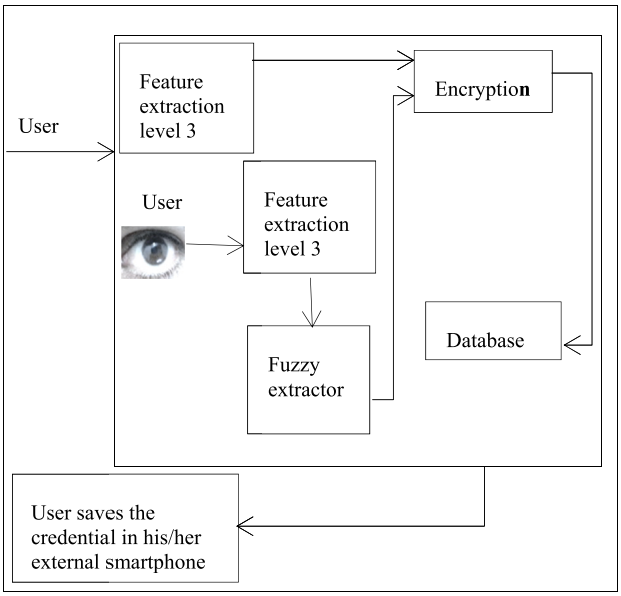

FIGURE 1. Principal difference between our authentication protocol and other related protocols.

B. NOTATIONS

The notations that are used in our proposed protocol are listed in Table 1.

C. PRELIMINARIES

1) PERCEPTUAL HASHING

The use of perceptual hashing has important benefits. The hash value is calculated for the user's biometric templates and the produced hash value, which depends on the biometric content, remains almost the same even if a modification is made to the content. The size of the hash value that can be generated via perceptual hashing varies from 64 to 128 bits. Moreover, the perceptual hash function has basic features that increase the security of the protocol [38].

2) ONE-WAY HASH FUNCTION

In this paper, we have used the one-way hash function in our proposed protocol for its basic characteristic, namely, the sensitive output of the function: the slightest change in the input affects the output. In addition, it is not possible to reverse the function; hence, there is no way to recover the input. The size of the one-way hash function is 128 bits. In Table 2, we have presented various lightweight hashing algorithms and the corresponding power consumption and technology values [39].

3) FUZZY EXTRACTOR (FE)

The FE is a new method that is applied to the user's biometrics and generates the same output string, even if there is a difference between the user's biometrics and the recorded biometric sample within the maximum permissible errors. It can convert the noise variable into a series that is stable and distributed uniformly. Furthermore, the FE includes

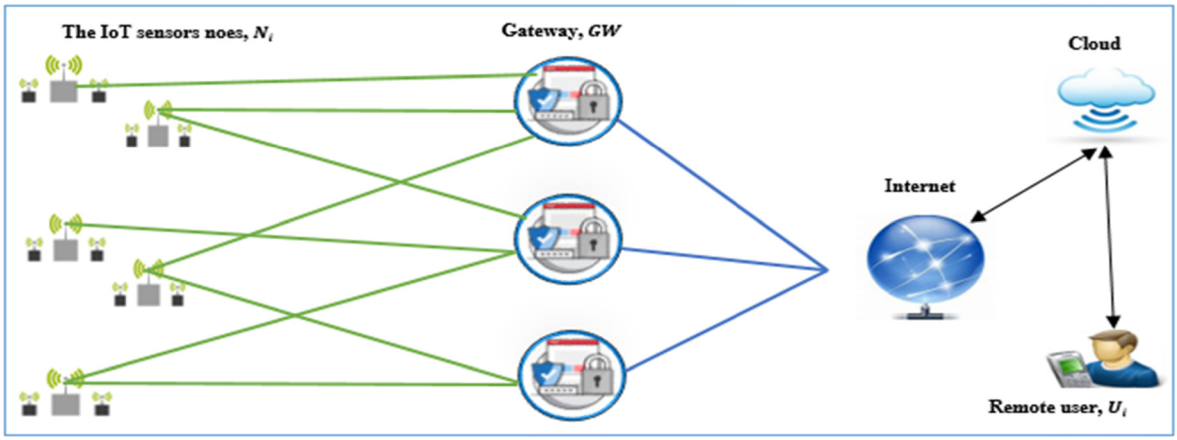

FIGURE 2. The proposed protocol scenario.

TABLE 1. Notations and their descriptions.

Notation	Description
U_i	Remote user
ID_i	Identity of the user
PW_i	The user password
IS_i	Extracting user iris
r_i, r_k	Random numbers generated by the user
Rep (.)	Fuzzy generator function
Gen (.)	Fuzzy reproduction function
R_i	Biometric secret key
P_i	Biometric public reproduction parameter
$FX3$	Feature extraction level 3
N_k	IoT sensing nodes
$X_{g_{N_k}}$	Shared secret key of the IoT nodes, generated by N_k
GW	The trusted gateway node
X_g	Secret key generated by the gateway
X_{g_u}	Secret key generated for the user
Tm_i, T	Timestamps
ΔT	Allowable transmission delaytransmission delay
SK	Shared session key
$\oplus$	XOR operation
$\|$	Concatenation operation
$H(.)$	One-way hash function
$h(.)$	Perceptual hashing function

two different algorithms: generation (Gen) and reproduction (Rep). The Gen algorithm produces output from the input of a reading (B) of the user's biometric as a public helper string (S) and an extracted string (R), namely, Gen (B) = (R, S). The Rep algorithm accepts S and the subsequent biometric reading (BL) as input and outputs R, namely, Rep (BL, S) = R. This FE is described in detail in [40-43].

4) FEATURE EXTRACTOR LEVEL 3 OF THE USER'S IRIS

Iris identification is one of the most important and vital measurements for increasing the privacy and security of the IoT and WSN. Iris identification is divided into three levels: The first level deals with the details of the identification, such as the pattern and ridgeline flow type. The second level corresponds to minute points such as bifurcations, terminations and spurs. The last level (shape) includes all the dimensional features of the ridge, such as the edge contour and sweat pores. The pores are divided into two classes: open and closed. In the open class, there is an intersection between the pores and the valley that lies between two ridges. In the closed class, a ridge surrounds the pores. Our proposed protocol focuses on the third level.

TABLE 2. Notations and their descriptions.

Algorithm	Area (GE)	Mean power (μW)	Technology (μm)
Spongent	738	1.57	0.13
Photon-80	865	1.59	0.18
Keccak	1,300	-	0.13
U-Quark	1,379	2.96	0.18
D-Quark	1,702	3.95	0.18
S-Quark	2,926	5.53	-

D. REGISTRATION PHASE

As soon as the IoT network is deployed, both the user (U_i) and the IoT sensor nodes (D_k) must register at the GW node. In this paper, the structure of our protocol consists of three objects: the remote user (U_i) who wishes to gain the services of the IoT environment, the IoT nodes (D_k), and the trusted gateway authority (GW). Therefore, there are two cases in this phase: first, the user U_i is registered in the IoT nodes and second, the IoT nodes are registered in the GW. In this section, we describe both registration phase cases.

1) CASE 1: USER AND GATEWAY NODE REGISTRATION

The user must perform a registration process at his/her gateway. The registration phase executes by extracting the features of the user's iris using a smart device such as a smartphone and applying the feature extractor level 3 on the

output template. Therefore, as a legal user, the following steps of user registration must be performed:

User Side: To complete the registration, U_i executes the following steps:

Step 1: U_i selects his/her identity (ID_i) and password (PW_i). Then, U_i extracts his iris features (IS_i) by using his smartphone.

Step 2: Next, U_i calculates the feature extraction level 3 of his/her iris ($FX3_{IS_i}$) as $FX3_{IS_i} = FeatExt(IS_i)$.

Step 3: Next, U_i computes $Gen\left(FX3_{IS_i}\right) = (R_i, P_i)$. This step overcomes the drawback of traditional biometric systems of needing to store either images or their template in the device memory.

Step 4: Then, U_i selects a random integer $r_i \in Z^+$ and computes the mask of user identity $SID_i = h(ID_i \oplus R_i \oplus r_i)$, user password $SPW_i = h(PW_i \oplus R_i \oplus r_i)$, $SFX3_{IS_i} = h(FX3_{IS_i} \oplus r_i)$ and the fuzzy extraction of the user iris $SR_i = h(R_i \oplus r_i)$.

Step 5: U_i sends the communication request message $M_1 = (SID_i, SPW_i, D^*, SFX3_{IS_i}, SR_i)$ to the GW node via a secure channel.

Gateway Side: Upon receiving the request message (M_1) from U_i, GW executes the following steps:

Step 1: GW creates secret keys X_g and X_{g_u}. Afterwards, it computes the security parameters, namely, $A_i = h(SID_i \oplus X_g)$, $B_i = h(SPW_i \oplus X_{g_u} \oplus R_i)$, and $C_i = h(SFX3_{IS_i} \oplus X_{g_u})$, for use in subsequent steps.

Step 2: Next, GW calculates $Factor = \sum_{i-1}^{L} ASCII(FX3_{IS_i} \oplus X_{g_u})$, $e_i = A_i^{Factor_i} \oplus X_{g_u}$, and $f_i = B_i^{Factor_i} \oplus X_{g_u}$.

Step 3: Afterwards, GW submits $M_2 = (SID_i, e_i, f_i, X_{g_u})$ to user U_i through a secure channel. On receiving message M_2, U_i stores it into the smartphone.

2) CASE 2: IOT NODE AND GATEWAY REGISTRATION

In this stage, every (IoT) node is registered. Any supplementary nodes can be added dynamically. This stage consists of the following steps:

IoT Node Side: During this stage, the IoT node will execute the following steps:

Step 1: N_k generates a random number $r_k \in Z_n^*$ for producing a one-time secret key and anomaly of device identity.

Step 2: N_k computes the parameters $MPW_j = h(X_{g_{N_k}} \parallel r_k \parallel ID_{N_k})$ and $MN_k = r_k \oplus X_{g_{N_k}} \oplus Factor_i$ for further use.

Step 3: Next, N_k submits MPW_j, MN_k, and the current timestamp Tm_1 to the GW via a secure channel.

Gateway Side: On receiving the registration request from IoT nodes (N_k), GW executes the following steps:

Step 1: GW will check the timestamp condition on the received Tm_1, namely, $|Tm_1 - T| < T?$, to prevent replay attacks. If the process checks are unsatisfied, then the registration phase is terminated; otherwise, GW will carry out the next step.

Step 2: GW calculates $r_k' = MN_k \oplus X_{g_{N_k}} \oplus Factor_i$.

Step 3: Based on the previous message that was received from user U_i, GW calculates $MPW_j' = h(X_{g_{N_k}} \parallel r_k' \parallel ID_{N_k^*})$.

Step 4: GW determines whether $MPW_j = MPW_j'?$ or not. If the condition is not satisfied, the node is illegitimate and the session will terminate. Otherwise, N_k is authenticated as a legal node from the network and GW performs the next step.

Step 5: GW computes the verification parameters $A_j = h(ID_{N_k^*} \parallel X_g)$, $B_j = h(MPW_j \parallel X_{g_{N_k}} \oplus Factor_i)$, and $C_j = A_j \oplus B_j$ for further use.

Step 6: Finally, GW submits A_j, C_j, and the current timestamp Tm_2 to IoT node N_k. Then, upon receiving (A_j, C_j, Tm_2) and the registration messages from GW, N_k checks the validity of the timestamp, namely, $|Tm_2 - T| < T?$, to verify for any external interference. If the condition is not satisfied, the registration messages request has been intercepted. Otherwise, N_k stores A_j, C_j, and Tm_2 into the memory and the registration phase is complete. Fig. 3 summarizes the methodology of the steps of the registration phase.

E. PRECOMPUTATION AND LOGIN PHASE

After successful registration of both U_I and N_k with the GW node, a legitimate user can access the desired node within the IoT network by logging into that node. First, U_i will be authenticated by GW and only then can it access the requested service from node N_k. In our work, we used feature extraction level 3 of the user's biometric, namely, the user's iris, for user registration and authentication. The steps for completing the login-phase process are presented as follows:

Step 1: First, U_i, as a legal user, uses his/her smartphone to open the IoT application and to enter his/her identity ID_i^* and password PW_i^*. Then, the user's smart device computes $SPW_i^* = H(PW_i \oplus R_i \oplus r_i)$ and $SFX3_{IS_i}^* = h(FX3_{IS_i} \oplus r_i)$.

Step 2: U_i computes $R_i^* = Rep(FX3_{IS_i}, P_i)$ and retrieves the original values of B_i and C_i as $B_i = h(SPW_i \oplus X_{g_u} \oplus R_i^*)$, $C_i = h(SFX3_{IS_i} \oplus X_{g_u})$.

Step 3: U_i calculates the verification parameters $B_i^* = h(A_i^{factor_i} \oplus e_i \oplus SPW_i^* \oplus X_{g_u} \oplus R_i^*)$ and $C_i^* = h(SFX3_{IS_i}{}^* \oplus b_i^{factor_i} \oplus factor_i)$. The accuracies of B_i and C_i are evaluated against B_i^* and C_i^*. If $B_i = B_i^*?$ and $C_i = C_i^*?$, then the user is verified as a legal user. Otherwise, the user has inputted incorrect identification information and the process terminates.

Step 4: On successful validation, U_i calculates $UN_K = H(X_{g_u} \parallel Tm_3 \parallel Factor_i \parallel r_i)$ and $UC_i = r_i \oplus A_i$.

Step 5: Next, U_i calculates the parameter $Factor_i^* = Factor_i \oplus Tm_3$ for an additional security check.

Step 6: U_i submits the login parameters $M_5 = (UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3)$ to the desired (IoT) node.

Upon completing Step 6, the login phase is complete and the user can select any node in the (IoT) environment.

F. AUTHENTICATION PHASE

To access and benefit from the service of any IoT node, the user $\boldsymbol{U_i}$ will try to log into the desired IoT node. Next, the IoT node redirects the user request to the gateway node. Then, the gateway node will generate the essential parameters

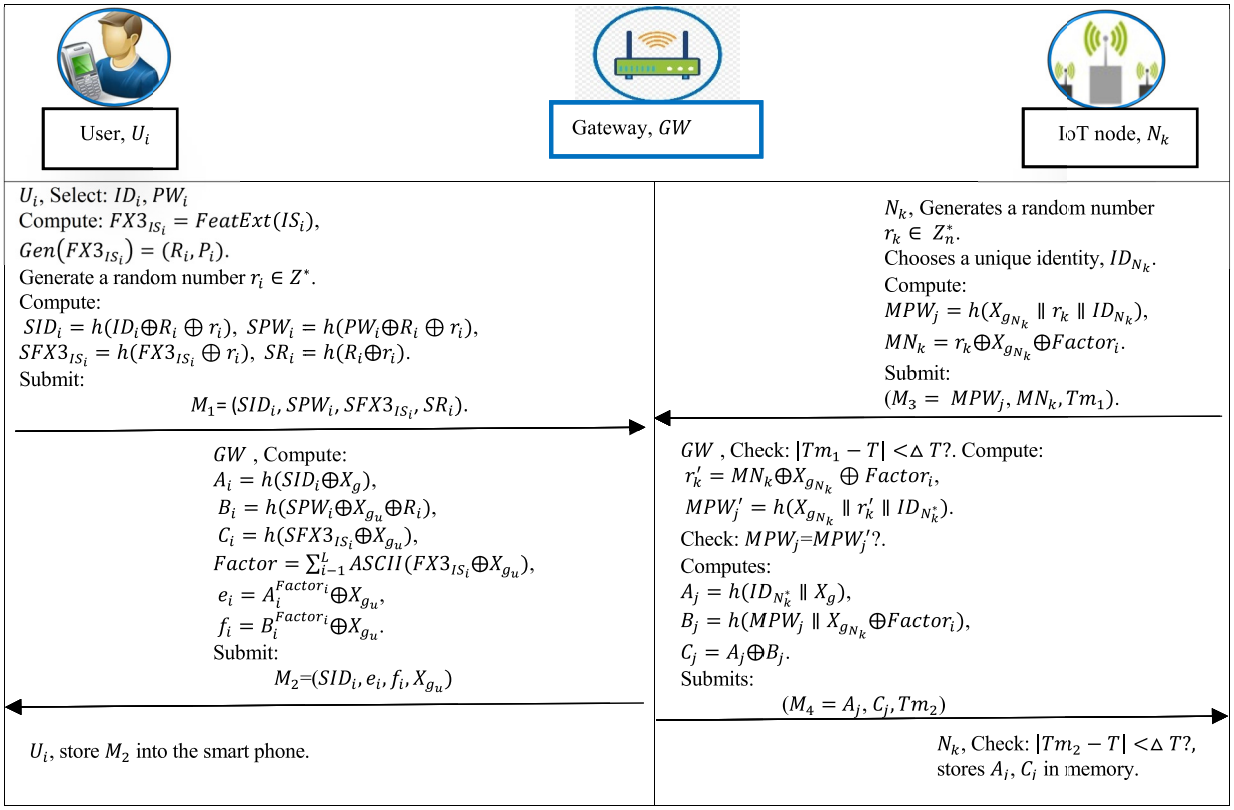

FIGURE 3. Summary of the registration phase.

or examine the authenticity of the user. On successful mutual authentication, both the user and the IoT node will generate the session key to enable them to communicate in a secure way. In this phase, the user (U_i), IoT node N_k, and the gateway node GW authenticate each other and generate a session key.

Step 1: On receiving the login message request from the user U_i, N_k checks the validity of the timestamp Tm_1, namely, whether $|Tm_3 - T| < \Delta T$, to avoid replay attacks. If the verification fails, N_k terminates the process. Otherwise, the process continues. Next, N_k retrieves the stored parameters $\langle A_j, e_j \rangle$ and calculates $B_j = A_j \oplus e_j$. Then, N_k computes the parameter $NS_j = H(X_{g_{N_k}} \| Tm_3 \| Tm_4) \oplus B_j$ for use in the mutual authentication. N_k submits the $M_5 = (UN_K, UC_i, e_i, f_i, SID_i Tm_3, Tm_4 Factor_i^*)$ message to GW.

Step 2: Upon receiving the message $M_6 = (M_5, NS_j, Tm_3, Tm_4)$ from N_k, GW will check the authenticity of U_i for N_k. Therefore, GW will examine the timestamp to determine whether the message is trustworthy or not, namely, whether $|Tm_4 - T| < \Delta T$?, and $Factor_i^* = ?Factor_i \oplus Tm_3$. If the conditions are not satisfied, the process will terminate and a termination message will be sent to N_k. Otherwise, GW proceeds to the next step.

Step 3: GW computes $A_j^* = h(ID_{N_k}^* \| X_g)$, $B_j^* = e_i \oplus A_j^*$, and $B_j = NS_j \oplus H(X_{g_{N_k}} \| Tm_3 \| Tm_4)$. Then, GW determines whether $B_j = B_j^*$. If the condition is satisfied, N_k is authenticated as a legitimate node by the network. Otherwise, GW terminates the process, thereby signaling that N_k has failed the legitimacy check.

Step 4: Once N_k has been successfully authenticated, GW computes $r_i^* = UC_i \oplus H(SID_i \oplus X_g)$ and $UN_k^* = H(X_{g_u} \| Tm_3 \| Factor_i \| r_i^*)$.

Step 5: Next, GW determines whether $UN_K = UN_k^*$. If the condition is satisfied, GW will authenticate user U_i. If not, GW terminates the process and sends an authentication failure message. Additionally, N_k will terminate the whole process and transmit a failure message to user U_i.

Step 6: On successful authentication, GW calculates $SP_{ij} = Factor_i^* \oplus r_i^* \oplus H(A_j^* \| X_{g_{N_k}})$ and $V_i = H(UN_k^* \| Tm_3 \| Tm_4 \| Tm_5 \| X_{g_u})$ and uses SP_{ij} to verify the gateway node (GW) and to avert the impersonation attack and V_i to validate both N_k and GW for the user (U_i). Then, GW submits the authentication message $M_7 = (SP_{ij}, V_i, Tm_3, Tm_4, Tm_5)$ to N_k. Having received the authentication message M_7 from GW, N_k performs the following steps:

Step 1: N_k checks the received timestamp Tm_5, namely, checks whether $|Tm_5 - T| < T$. If the check fails, N_k will terminate the process and submit a failure message to prevent replay attacks. Otherwise, N_k will check whether $SP_{ij} = Factor_i^* \oplus r_i \oplus H(A_j^* \| X_{g_{N_k}})$. If this holds, it proceeds to the next step. Otherwise, N_k terminates the process.

Step 2: Next, N_k calculates $V_i^* = H(V_i \| Tm_6 \oplus) \oplus K_i$, where K_i is a nonce random number, and calculates the session key $sk = H(r_i \oplus K_i \oplus Tm_3 \| Tm_4)$.

Step 3: N_k sends the authentication message $M_8 = (, Tm_3, Tm_4, Tm_6, V_i^*, V_i)$ to the user U_i. On receiving M_8, U_i will execute the following:

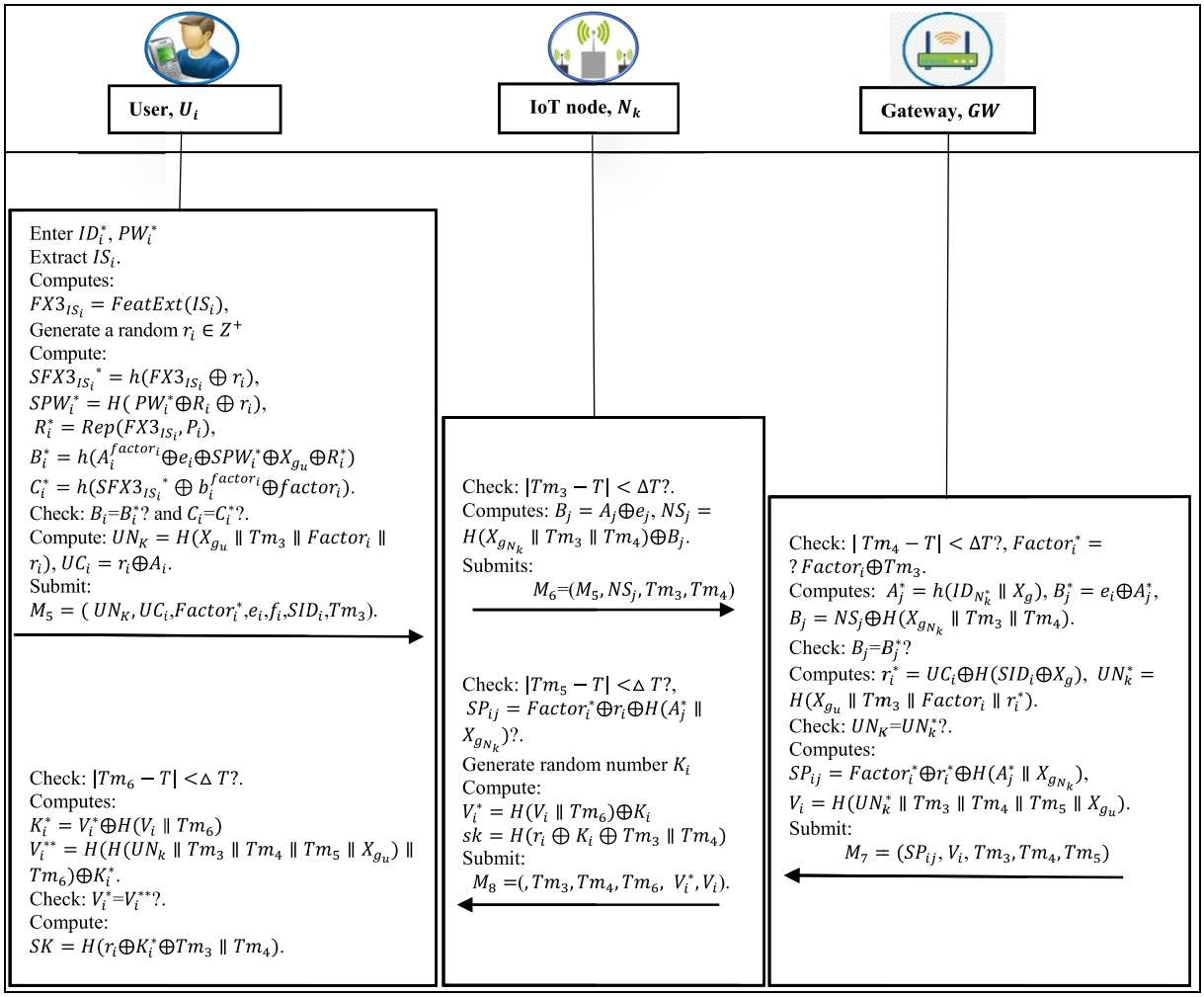

FIGURE 4. Summary of the login and authentication phase.

Step 1: U_i performs a timestamp check, namely, checks whether $|Tm_6 - T| < T$. If the condition is satisfied, U_i proceeds and calculates $K_i^* = V_i^* \oplus H(V_i \| Tm_6)$.

Step 2: Next, U_i computes $V_i^{**} = H(H(UN_k \| Tm_3 \| Tm_4 \| Tm_5 \| X_{g_u}) \| Tm_6) \oplus K_i^*)$. Then, U_i determines whether $V_i^* = V_i^{**}$?. If the verification is unsuccessful, U_i will terminate the process. Otherwise, U_i computes the session key as $SK = H(r_i \oplus K_i^* \oplus Tm_3 \| Tm_4)$ and the authentication is complete. Fig. 4 summarizes the login and authentication phases.

G. PASSWORD AND BIOMETRIC CHANGE PHASE

This phase regularly updates the password to preserve high security. Our proposed protocol enables the user to easily change his/her password. The essential steps are as follows:

Step 1: The user U_i opens his IoT application on his/her smart device and submits his/her old password SPW_i and identity ID_i and imprints his/her old biometric $FX3_{IS_i}$.

Step 2: Next, U_i computes $R_i^* = Rep(FX3_{IS_i}, P_i)$. In addition, it computes $B_i^* = h(A_i^{factor_i} \oplus e_i \oplus SPW_i^* \oplus X_{g_u} \oplus R_i^*)$ and $C_i^* = h(SFX3_{IS_i}^* \oplus b_i^{factor_i} \oplus f_i)$.

Step 3: Then, U_i retrieves the values of B_i and C_i as $B_i = h(SPW_i \oplus X_{g_u} \oplus R_i)$ and $C_i = h(SFX3_{IS_i} \oplus X_{g_u})$. Using these values, U_i will check the validity of B_i with B_i^* and C_i with C_i^*, namely, B_i =? B_i^* and C_i =? C_i^*. If the checking process fails, user U_i has inputted incorrect information - password or biometric - and the process terminates.

Step 4: If the conditions are validated, user U_i is legitimate and the device asks user U_i to enter his/her new password and new biometric. Then, U_i enters a new password NPW_i^* and imprints new biometrics IS_i^{**}.

Step 5: U_i calculates $FX3_{IS_i^{**}} = FeatExt(IS_i^{**})$, generates a new random number r_i^{**}, and computes $Gen\left(FX3_{IS_i^{**}}\right) = (R_i^{**}, P_i^{**})$, $SNPW_i^* = H(NPW_i^* \oplus R_i^{**} \oplus r_i^{**})$, $B_i'' = SNPW_i^* \oplus X_{g_u} \oplus R_i^{**}$, and $f_i'' = B_i''^{f_i} \oplus X_{g_u}$.

Step 6: Finally, U_i replaces B_i^*, f_i, and R_i from his smart device memory with B_i'', f_i'', and R_i^{**}, respectively, and the phase terminates successfully.

V. SECURITY ANALYSIS AND DISCUSSION

In this section, we conduct both informal and formal analyses of our proposed protocol. Through the informal analysis, we show how our proposed protocol satisfies the security

requirements and withstands various known attacks. We also compare our proposed protocol with related protocols in terms of security. Moreover, via formal analysis, we demonstrate that our proposed protocol provides mutual authentication and that the session key will be established mutually between the user and the IoT sensor nodes, with the assistance of the gateway node.

A. INFORMAL ANALYSIS

In this subsection, we present a security analysis of our proposed protocol and we prove that it resists various malicious attacks and can provide several security features.

1) MUTUAL AUTHENTICATION

On receiving the login request message $M_5 = (UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3)$ of U_i, N_k checks the timestamp of the requested messages ($|Tm_3 - T| < \Delta T$) and retrieves the stored parameters $\langle A_j, e_j \rangle$, which it uses to calculate $B_j = A_j \oplus e_j$. Then, N_k computes the authentication parameter $NS_j = H(X_{g_{N_k}} \parallel Tm_3 \parallel Tm_4) \oplus B_j$. Thereafter, N_k forwards the user login message and the authentication parameter $M_6 = (M_5, NS_j, Tm_3, Tm_4)$ to the GW via an insecure channel. Thus, on receiving M_6 from N_k, GW computes the authentication parameters $A_j^* = h(ID_{N_k^*} \| X_g)$, $B_j^* = e_i \oplus A_j^*$, and $B_j = NS_j \oplus H(X_{g_{N_k}} \| Tm_3 \parallel Tm_4)$. Then, GW checks if $B_j = B_j^*$ to evaluate the legitimacy of N_k. That is because only a legitimate sensing node can retrieve the correct value of NS_j. Therefore, in this step, N_k is authenticated by GW. Then, it computes the authentication parameters $r_i^* = UC_i \oplus H(SID_i \oplus X_g)$ and $UN_k^* = H(X_{g_u} \| Tm_3 \parallel Factor_i \| r_i^*)$, which are used to evaluate the legitimacy of U_i. Then, GW checks if $UN_K = UN_k^*$. That is because only a legitimate user can retrieve r_i. Then, GW calculates $V_i = H(UN_k^* \| Tm_3 \parallel Tm_4 \| Tm_5 \parallel X_{g_u})$ to validate both N_k and GW by U_i. Next, GW submits the authentication message M_7 to N_k. After that, N_k verifies the authentication parameters and computes the session key. Finally, N_k submits the authentication message M_8 to U_i. Thus, the user, the IoT node, and the gateway authenticate one another. Therefore, our proposed protocol provides mutual authentication.

2) KEY AGREEMENT

After realizing the mutual authentication, U_i and N_k establish independently a shared session key SK. Moreover, they both compute the same session key ($SK = r_i \oplus K_i^* \| Tm_3 \| Tm_4$), which is not communicated via the wireless channel. Therefore, our proposed protocol provides key agreement.

3) USER ANONYMITY AND UNTRACEABILITY

Assume that a malicious attack $\mathbb{A}$ intercepts the exchanged message parameters $\{M_5 = (UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3)\}$, $\{M_6 = (M_5, NS_j, Tm_3, Tm_4)\}$ $\{M_7 = (SP_{ij}, V_i, Tm_3, Tm_4, Tm_5)\}$, and $\{M_8 = (, Tm_3, Tm_4, Tm_6, V_i^*, V_i)\}$ during the login & authentication phases. Due to the use of the random number r_i & current timestamp Tm_3 in M_5, all parameters in this message are dynamic and unique for each session. Likewise, M_6 M_7, and M_8 are dynamic and unique due to the random numbers and the current timestamp. Moreover, the user's and IoT node's identities are not included as plaintext in previous messages. Therefore, our proposed protocol protects the user's anonymity and realizes untraceability.

4) KEY FRESHNESS

In our proposed protocol, after mutual authentication, both U_i and N_k generate the same session key SK. The established session key is based on the fresh timestamps Tm_3 and Tm_4. Moreover, the timestamps are unique for each session and ensure the uniqueness of the session key for each session. Therefore, our proposed protocol provides freshness of the session key.

5) FORWARD SECRECY AND SESSION KEY EXPOSURE

In the proposed protocol, the session key SK is computed as $SK = r_i \oplus K_i^* \parallel Tm_3 \parallel Tm_4 \parallel$ based on the random parameters (r_i, K_i, Tm_3, Tm_4). Thus, a malicious attacker ($\mathbb{A}$) cannot generate the session key SK even if secret information is compromised. Therefore, our proposed protocol provides forward secrecy and resists session key exposure.

6) RESISTANCE TO REPLAY ATTACKS

In our protocol, all the communicated messages among all involved parties U_i, N_k, and GW use the current timestamps (Tm_3, Tm_4, Tm_5, and Tm_6) with a small acceptable delay interval ΔT. Therefore, a malicious attacker $\mathbb{A}$ cannot replay the exchanged messages on which he/she has eavesdropped during the login or authentication phase. Hence, our proposed protocol resists replay attacks.

7) RESISTANCE TO IMPERSONATION ATTACKS

Assume a malicious attacker $\mathbb{A}$ tries to create a valid message from the user login request by eavesdropping on the user's login message $\{M_5 = (UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3)\}$ and altering it to $M_5' = UN'_K, UC'_i, Factor'^*_i, e'_i, f'_i, SID'_i, Tm_3\}$. For this, $\mathbb{A}$ needs to know r_i, which is a random number that is generated once by the user, and the shared secret key X_{g_u}, which will be known only to the user and the gateway node. Thus, for $\mathbb{A}$ to recreate the user login request message by eavesdropping is impossible. Therefore, our proposed protocol resists user impersonation attacks.

8) RESISTANCE TO OFFLINE PASSWORD GUESSING ATTACKS

Suppose a malicious attacker $\mathbb{A}$, by using a power analysis attack, knows all the information in the smartphone of U_i, namely, $\{SPW_i, SID_i, P_i, h(.)\}$. $\mathbb{A}$ cannot deduce the user's password PW_i or identity ID_i as they protected by a secure one-way hash function. Thus, our proposed protocol resists offline password guessing attacks.

9) RESISTANCE TO STOLEN SMART DEVICE ATTACKS

In the case of a user's smart device being stolen, all the stored information $\{SID_i, e_i, f_i, X_{g_u}, SPW_i\}$ is revealed to an

adversary $\mathbb{A}$. By using these parameters, $\mathbb{A}$ can try to access the IoT node, namely, N_k; however, $\mathbb{A}$ will fail to do so. This is because to log into the desired IoT node, $\mathbb{A}$ must compute $SPW_i^* = H(PW_i \oplus R_i \oplus r_i)$ and $SFX3_{IS_i} = h(FX3_{IS_i} \oplus r_i)$, which requires the biometric imprint and the user's password to be guessed—this is impossible.

10) RESISTANCE TO DENIAL OF SERVICE ATTACKS

This type of attack occurs when an attacker transfers an enormous number of request messages during the login and/or authentication phase to GW and N_k. In our proposed protocol, all exchanged messages are associated with timestamp values, e.g., Tm_3, Tm_4, Tm_5, and Tm_6 and are authenticated. Therefore, any invalid message or timed-out message is disclosed and is rejected. In our proposed protocol, every entity (remote user, IoT node, and the gateway node) receives a message with a timestamp check during the protocol phase, which is executed to check the validity of the message. Hence, our proposed protocol resists denial-of-service attacks.

11) RESISTANCE TO MAN-IN-THE-MIDDLE ATTACKS

Assume a malicious attacker $\mathbb{A}$ obstructs the login request message $\{M_5 = (UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3)\}$ and tries to modify this message to $\{M'_5 = UN'_K, UC'_i, Factor'^*_i, e'_i, f'_i, SID'_i, Tm'_3, Tm'_4\}$, which is another legal login request message. $\mathbb{A}$ can select a random number such as $r_i \in Z^+$ and generate the current timestamp Tm'_3. Then, $\mathbb{A}$ can calculate $Factor'^*_i$; however, $\mathbb{A}$ cannot calculate UN_K, UC_i, e_i, f_i, or SID_i without knowing the user's identity ID_i and password PW_i, and the shared secret key X_{g_u}, which is a private key that is known only to GW and the remote user. Moreover, due to the small size of the transmission delay ΔT, $\mathbb{A}$ cannot retransmit the login request message. Therefore, our proposed protocol resists man-in-the-middle attacks.

12) RESISTANCE TO PARALLEL SESSION ATTACKS

Suppose a malicious attacker $\mathbb{A}$ tries to create a parallel session of the protocol. In the proposed protocol, this case is not possible as the proposed protocol uses a unique biometric and timestamps with a small transmission delay ΔT. Therefore, $\mathbb{A}$ cannot run even one valid session to impersonate a legitimate user. Thus, our proposed protocol resists parallel session attacks.

13) RESISTANCE TO PASSWORD CHANGE ATTACKS

In the protocol, during the login phase, the user imprints his/her unique biometric $FX3_{IS_i}$, which is impossible for attacker $\mathbb{A}$ to impersonate. Moreover, if a malicious attacker tries to change the original password PW_i to a fake password PW'_i using a power analysis attack, he/she still must enter the valid biometric to log in, which is impossible. Therefore, our proposed protocol resists password change attacks.

14) RESISTANCE TO NODE COMPROMISE ATTACKS

Suppose a malicious attacker $\mathbb{A}$ captures the IoT sensing device N_k and tries to modify the exchanges message $\{UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i, Tm_3, Tm_4\}$ to $\{UN'_K, UC'_i, e'_i, f_i, SID'_i Tm'_3, Tm'_4 Factor'^*_i\}$ by extracting the stored information. $\mathbb{A}$ cannot obtain the value of SID_i as it is protected by a one-way hash function and the shared secret key Xg_{Nk}, which is only known to IoT nodeN_k. Therefore, our proposed protocol resists node compromise attacks.

15) RESISTANCE TO GATEWAY NODE BYPASSING ATTACKS

Assume a malicious attacker $\mathbb{A}$ tries to log into the desired IoT node, namely, N_k, by bypassing the gateway node GW. He/she will fail because in our proposed protocol, to use the IoT application the user must log into N_k and be authenticated by GW. Additionally, the authentication process is conducted throughGW. Therefore, no attacker can authenticate himself and bypass GW. Hence, our proposed protocol resists gateway node bypassing attacks.

16) RESISTANCE TO INSIDER ATTACKS

Suppose a privileged remote user at GW become a malicious attacker $\mathbb{A}$. Then, he/she can calculate the user information that is contained in SID_i during the registration phase. Assume $\mathbb{A}$ steals the user's smart device and retrieves all the information. However, $\mathbb{A}$ cannot guess ID_i or PW_i because they are protected by a secure one-way hash function and based on a random number. Moreover, $\mathbb{A}$ needs to know the user's biometric key R_i and to derive it, $\mathbb{A}$ must know ID_i and P_i. Thus, the proposed protocol resists insider attacks.

17) RESISTANCE TO NODE COMPROMISE ATTACKS

Assume a malicious attacker $\mathbb{A}$ captures IoT node N_k. $\mathbb{A}$ can reveal the registration request message $\{M_2 = MPW_j, MN_k, Tm_1\}$. However, $\mathbb{A}$ will fail to obtain the node identity as it is computed based on a one-way hash function and the private secret key $X_{g_{N_k}}$, which is only known to N_k. Therefore, our proposed protocol resists node compromise attacks.

B. FORMAL ANALYSIS

Here, we demonstrate the security of our proposed protocol. We have used BAN logic [44] as a formal security verification, which is more efficient than formal security proofs such as CK and BR, which do not identify errors easily. Through BAN logic, we show that our protocol is secure in the threat model of Dolev–Yao, which is widely used [45], [46]. Moreover, by using BAN logic we demonstrate that our protocol realizes secure mutual authentication among entities (user, IoT node, and the gateway node). BAN logic consists of predefined rules, which were explained by many authentication protocols. Table 3 lists the BAN logic symbols and descriptions.

1) BAN LOGIC RULES

The following are the essential postulates of BAN logic, which we have used in the mutual authentication analysis of our proposed protocol:

TABLE 3. BAN logic symbols and description.

Notations	Meaning
$P\mid\equiv X$	P believes X as a valid statement.
$P \lhd X$	Principal P sees the statement X.
$P\mid\sim X$	Principal P once said the statement X.
$\#(X)$	It means that X is fresh.
$P\overset{K}{\leftrightarrow}Q$	P and Q share a secret K, and K will never be discovered by any principal except P and Q.
$P\overset{Y}{\rightleftharpoons}Q$	P and Q share the secret key Y and only these two entities can use Y to prove its identity to each other.
$(X)_K$	Hash computation of X using the secret K.
$\langle X\rangle_Y$	Formula X combined with the formula Y.
$\{X\}_K$	Encryption of X using the secret K.

- Rule 1: Nonce-verification rule. $\frac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$. Namely, if P believes that statement X is fresh and P also believes that Q once said$X$, then P believes Q believes statement X.
- Rule 2: Jurisdiction rule. $\frac{P\mid\equiv Q\mid\Rightarrow X,,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$. Namely, if P believes that Q has jurisdiction over statement S and P believes Q believes statement$X$, then P believes statement$X$.
- Rule 3: Freshness rule. $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$. Namely, if P believes that part of statement X is fresh, then P believes that statement $\{X, Y\}$ is fresh.
- Rule 4: Belief rule. $\frac{P\mid\equiv Q\mid\equiv(X,Y)}{P\mid\equiv Q\mid\equiv X}$; $\frac{P\mid\equiv X,P\mid\equiv Y}{P\mid\equiv(X,Y)}$; $\frac{P\mid\equiv(X,Y)}{P\mid\equiv X}$; and $\frac{P\mid\equiv(X,Y)}{P\mid\equiv Y}$. Namely, if P believes that Q believes statement (X, Y), then P believes Q believes part of statement X.
- Rule 5: Message meaning rules: $\frac{P\mid\equiv P\overset{K}{\leftrightarrow}Q,P\lhd(X)_K}{P\mid\equiv Q\mid\sim X}$. Namely, if P sees a statement X that is encrypted with key K and P believes that K is a shared secret key between P and$Q$, then P believes Q once said X.

2) SECURITY GOALS

The following goals must be realized to complete the authentication proof:

- Goal 1: $U_i\mid\equiv N_k\mid\equiv\left(U_i\overset{SK}{\leftrightarrow}N_k\right)$.
- Goal 2: $U_i\mid\equiv\left(U_i\overset{SK}{\leftrightarrow}N_k\right)$.
- Goal 3: $N_k\mid\equiv U_i\mid\equiv\left(U_i\overset{SK}{\leftrightarrow}N_k\right)$.
- Goal 4: $N_k\mid\equiv\left(U_i\overset{SK}{\leftrightarrow}N_k\right)$.

Next, we present the idealized form of our proposed protocol in terms of the mutual communication messages as follows:

Mssg1:

$$U_i\overset{\text{via}N_k}{\longleftrightarrow}\text{GW}:\quad\left\{ID_i,Tm_3,(U_i\overset{ID_i}{\longleftrightarrow}N_K)\right\}_{X_{gu}}$$

Mssg2:

$$U_i\overset{\text{via}N_k}{\longleftrightarrow}\text{GW}:\quad\left\{UN_K,UC_i,Factor_i^*,e_i,Tm_3f_i,\ SID_i(U_i\overset{ID_i}{\longleftrightarrow}N_K),(U_i\overset{X_{gu}}{\longleftrightarrow}N_K)\right\}_{X_{gu}}$$

Mssg3:

$$N_k\longrightarrow GW:\quad\left\{SID_i,Tm_4,Factor_i,N_k\overset{SID_i}{\longleftrightarrow}\text{GW}\right\}_{X_{gN_k}}$$

Mssg4:

$$N_k\longrightarrow GW:\quad\left\{UN_K,UC_i,e_i,f_i,Tm_3,Tm_4Factor_i^*,\ N_k\overset{r_i}{\longleftrightarrow}\text{GW},N_k\overset{SID_i}{\longleftrightarrow}\text{GW}\right\}_{X_{gN_k}}$$

Mssg5:

$$GW\longrightarrow N_k:\quad\left\{Tm_5,(N_k\overset{X_{gN_k}}{\longleftrightarrow}GW)\right\}_{X_{gN_k}}$$

Mssg6:

$$GW\longrightarrow N_k:\quad\left\{Tm_3,Tm_4,Tm_5,SP_{ij},(N_k\overset{X_{gN_k}}{\longleftrightarrow}GW),\ (N_k\overset{r_i^*}{\longleftrightarrow}GW)\right\}_{X_{gN_k}}$$

Mssg7:

$$U_i\overset{\text{via}GW}{\longleftrightarrow}N_k:\quad\left\{Tm_5,r_i^*,(N_k\overset{SID_i}{\longleftrightarrow}\text{GW}),\ (N_k\overset{r_i^*}{\longleftrightarrow}GW)\right\}_{X_{gN_k}}$$

Mssg8:

$$\text{GW}\overset{\text{via}N_k}{\longleftrightarrow}U_i:\quad\left\{Tm_5,r_i^*,(U_i\overset{ID_i}{\longleftrightarrow}\text{GW}),\ (U_i\overset{r_i^*}{\longleftrightarrow}GW)\right\}_{X_{gN_k}}.$$

Mssg9:

$$N_k\longrightarrow U_i:\quad\left\{Tm_3,Tm_4,Tm_5,,Tm_6,V_i^*,V_i,\left(N_k\overset{SID_i}{\longleftrightarrow}\text{GW}\right),r_i^*,(U_i\overset{K_l}{\longleftrightarrow}G)\right\}_{SK}$$

3) SUPPOSITIONS

Now, we will specify the initial state suppositions for our proposed protocol, as follows:

- Sup1: $GW\mid\equiv(U_i\overset{X_g}{\longleftrightarrow}GW)$
- Sup2: $GW\mid\equiv\#(Tm_3)$
- Sup3: $GW\mid\equiv U_i\mid\Longrightarrow(U_i\overset{ID_i}{\longleftrightarrow}GW)$
- Sup4:$GW\mid\equiv(U_i\overset{SID_i=h(ID_i\oplus R_i\oplus r_i)}{\longleftrightarrow}GW)$.
- Sup5: $GW\mid\equiv\#(r_i)$

- Sup6: $GW| \equiv U_i| \Longrightarrow (U_i \overset{r_i}{\longleftrightarrow} GW)$
- Sup7: $GW| \equiv (U_i \overset{X_{gu}}{\longleftrightarrow} GW)$
- Sup8: $GW| \equiv \#(Tm_4)$
- Sup9: $GW| \equiv N_k| \Longrightarrow (N_k \overset{SID_i}{\longleftrightarrow} GW)$
- Sup10: $GW| \equiv (N_k \overset{X_{gN_k}}{\longleftrightarrow} GW)$
- Sup11: $GW| \equiv \#\left(r_i^*\right)$
- Sup12: $GW| \equiv N_k| \Longrightarrow (N_k \overset{r_i^*}{\longleftrightarrow} GW)$
- Sup13: $N_k| \equiv (N_k \overset{X_{gN_k}}{\longleftrightarrow} GW)$
- Sup14: $N_k| \equiv \#(Tm_5)$
- Sup15: $GW| \equiv N_k| \Longrightarrow (N_k \overset{X_g}{\longleftrightarrow} GW)$
- Sup16: $N_k| \equiv \#\left(r_i^*\right)$
- Sup17: $N_k| \equiv GW| \Longrightarrow (N_k \overset{r_i^*}{\longleftrightarrow} GW)$
- Sup18: $N_k| \equiv U_i| \Longrightarrow (N_k \overset{r_i^*}{\longleftrightarrow} GW)$
- Sup19: $U_i| \equiv ((U_i \overset{SID_i=h(ID_i \oplus R_i \oplus r_i)}{\longleftrightarrow} GW)$
- Sup20: $U_i| \equiv \#(K_i)$
- Sup21: $U_i| \equiv GW| \Longrightarrow (U_i \overset{K_i}{\longleftrightarrow} GW)$
- Sup22: $U_i \equiv \#(Tm_6)$
- Sup23: $U_i| \equiv N_k| \Longrightarrow (U_i \overset{K_i}{\longleftrightarrow} GW)$

Considering the basic assumptions, logical postulates, rules, and idealized forms, we will demonstrate that the proposed protocol realizes the above four objectives (Goal 1, Goal 2, Goal 3, and Goal 4).

From ***Mssg1***, we get:

$$GW \triangleleft \langle ID_i, Tm_3, (U_i \overset{ID_i}{\longleftrightarrow} N_K)\rangle_{X_g} \tag{1}$$

From **(1)**, ***Sup1***, and Rule (1), we get:

$$GW| \equiv \sim\sim \langle ID_i, Tm_3, (U_i \overset{ID_i}{\longleftrightarrow} N_K)\rangle_{X_g} \tag{2}$$

Now, from ***Sup2,*** and Rule (1), we get:

$$GW| \equiv \#\langle ID_i, Tm_3, (U_i \overset{ID_i}{\longleftrightarrow} N_K)\rangle_{X_g} \tag{3}$$

From **(2)** & **(3),** and Rule (2):

$$GW| \equiv U_i| \equiv \langle ID_i, Tm_1, (U_i \overset{ID_i}{\longleftrightarrow} N_K)\rangle_{X_g} \tag{4}$$

From **(4)** and Rule (5), we get:

$$GW| \equiv U_i| \equiv (U_i \overset{ID_i}{\longleftrightarrow} \text{GW}) \tag{5}$$

From **(5),** ***Sup3***, Rule(3), we can get:

$$GW| \equiv (U_i \overset{ID_i}{\longleftrightarrow} \text{GW}) \tag{6}$$

From ***Mssg2***: we get:

$$GW \triangleleft \langle UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i(U_i \overset{ID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gu}} \tag{7}$$

From **(7)**, ***Sup4***, and Rule (1),

$$GW| \equiv U_i| \sim \langle UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i(U_i \overset{ID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gu}} \tag{8}$$

From ***Sup2***, ***Sup5***, and Rule (4),

$$GW| \equiv \#\langle UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i(U_i \overset{ID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gu}} \tag{9}$$

From (8) & (9), and Rule (2),

$$GW| \equiv U_i| \equiv \langle UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i(U_i \overset{ID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gu}} \tag{10}$$

From **(5)**, **(6)**, **(10)**, and Rule (5),

$$GW| \equiv U_i| \equiv (U_i \overset{r_i}{\longleftrightarrow} \text{GW}) \tag{11}$$

From **(11)**, ***Sup6***, Rule (3),

$$GW|(U_i \overset{r_i}{\longleftrightarrow} \text{GW}) \tag{12}$$

From ***Mssg3***,

$$GW \triangleleft \langle SID_i, TS_2, Factor_i, N_k \overset{SID_i}{\longleftrightarrow} GW\rangle_{X_{gN_k}} \tag{13}$$

From (13), ***Sup7***, and Rule (1),

$$GW| \equiv N_k| \sim \langle UN_K, UC_i, Factor_i^*, e_i, f_i, SID_i(U_i \overset{ID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gN_k}} \tag{14}$$

From ***Sup7***, and Rule (4),

$$GW| \equiv \#\langle UN_K, UC_i, e_i, f_i, SID_i(U_i \overset{MID_i}{\longleftrightarrow} N_K), (U_i \overset{X_{gu}}{\longleftrightarrow} N_K)\rangle_{X_{gN_k}} \tag{15}$$

From **(14)**, **(15)**, and Rule (2),

$$GW| \equiv N_k| \equiv \langle SID_i, TM_2, Factor_i(N_{k_i} \overset{MID_i}{\longleftrightarrow} \text{GW})\rangle \tag{16}$$

From **(16)**, and Rule (5), we get:

$$GW| \equiv N_k| \equiv (N_{k\,i} \overset{MID_i}{\longleftrightarrow} \text{GW}) \tag{17}$$

From **(17)**, ***sup9***, and Rule (3),

$$GW| \equiv (N_{k\,i} \overset{MID_i}{\longleftrightarrow} \text{GW}) \tag{18}$$

From ***Mssg4***,

$$GW \triangleleft \langle UN_K, UC_i, e_i, f_i, Tm_3, Tm_4, (N_k \overset{r_i}{\leftrightarrow} \text{GW}), (N_k \overset{SID_i}{\longleftrightarrow} \text{GW})\rangle_{X_{gN_k}} \tag{19}$$

From **(19)**, ***sup10***, and Rule (1),

$$GW| \equiv N_k| \sim \langle UN_K, UC_i, e_i, f_i, Tm_3, Tm_4, (N_k \overset{r_i}{\leftrightarrow} \text{GW}), (N_k \overset{SID_i}{\longleftrightarrow} \text{GW})\rangle_{X_{gN_k}} \tag{20}$$

From ***sup8***, ***sup11***, Rule (4),

$$GW| \equiv \#\langle UN_K, UC_i, e_i, f_i, Tm_3, Tm_4, (N_k \overset{r_i}{\leftrightarrow} \text{GW}), (N_k \overset{SID_i}{\longleftrightarrow} \text{GW})\rangle_{X_{gN_k}} \tag{21}$$

From (20), (21), and Rule (2),

$$GW| \equiv N_k| \equiv \langle UN_K, UC_i, e_i, f_i, Tm_3, Tm_4, (N_k \overset{r_i}{\leftrightarrow} \text{GW}), (N_k \overset{SID_i}{\longleftrightarrow} \text{GW})\rangle_{X_{gN_k}} \tag{22}$$

From **(17), (18)**, **(22),** and Rule(5), we get:

$$GW| \equiv N_k| \equiv (N_k \overset{r_i}{\longleftrightarrow} \text{GW}) \tag{23}$$

From **(23)**, ***sup12***, and Rule(3), we get:

$$GW| \equiv (N_k \overset{r_i}{\longleftrightarrow} \text{GW}) \tag{24}$$

From **Mssg5**, we get:

$$N_k \lhd \langle Tm_3, (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{25}$$

From **(25)**, ***sup13***, and Rule 1,

$$N_k| \equiv GW| \sim \langle Tm_3, (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{26}$$

From ***sup14***, Rule 4,

$$N_k| \equiv \#\langle Tm_3, (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{27}$$

From **(26)**, **(27)**, and Rule 2, we get:

$$N_k| \equiv GW| \equiv \langle Tm_3, (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{28}$$

From **(28)**, Rule 5, we get:

$$N_k| \equiv GW| \equiv (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW) \tag{29}$$

From **(29)**, ***sup15***, and Rule 3, we get:

$$N_k| \equiv (N_k \overset{X_{g_{N_k}}}{\longleftrightarrow} GW) \tag{30}$$

From ***Mssg6***,

$$N_k \lhd \langle Tm_3, Tm_4, Tm_5, SP_{ij}, (N_k \overset{X_{g_{N_k}}}{\leftrightarrow} GW), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{31}$$

From (30), (31), ***sup13***, and Rule 1,

$$N_k| \equiv GW| \sim \langle Tm_3, Tm_4, Tm_5, SP_{ij}, (N_k \overset{X_{g_{N_k}}}{\leftrightarrow} GW), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{32}$$

From **sup*14***, ***sup16***, and Rule 4,

$$N_k| \equiv \#\langle Tm_3, Tm_5, SP_{ij}, (N_k \overset{X_{g_{N_k}}}{\leftrightarrow} GW), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{33}$$

From **(32)**, **(33)**, Rule (2),

$$N_k| \equiv GW| \equiv \langle Tm_3, Tm_4, Tm_5, SP_{ij}, (N_k \overset{X_{g_{N_k}}}{\leftrightarrow} GW), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{34}$$

From **(17)**, **(18)**, and **(34)**,

$$N_k| \equiv GW| \equiv (N_k \overset{r_i^*}{\longleftrightarrow} GW) \tag{35}$$

From **(35)**, ***sup17***, and Rule 3, we get:

$$N_k| \equiv (N_k \overset{r_i^*}{\longleftrightarrow} GW) \tag{36}$$

From **Mssg7**,

$$N_k \lhd \langle Tm_5, r_i^*, (N_k \overset{SID_i}{\leftrightarrow} \text{GW}), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{37}$$

From **(37)**, ***sup13***, and Rule1,

$$N_k| \equiv U_i| \sim \langle Tm_5, r_i^*, (N_k \overset{SID_i}{\leftrightarrow} \text{GW}), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{38}$$

From ***sup14***, ***sup16***, and Rule 4,

$$N_k| \equiv \#\langle Tm_5, r_i^*, (N_k \overset{SID_i}{\leftrightarrow} \text{GW}), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{39}$$

From **(38)**, **(39)**, and Rule 2,

$$N_k| \equiv U_i| \equiv \langle Tm_5, r_i^*, (N_k \overset{SID_i}{\leftrightarrow} \text{GW}), (N_k \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{40}$$

From **(17)**, **(18)**, **(35)**, and Rule 5, we get:

$$N_k| \equiv U_i| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} N_k) \qquad \textbf{\textit{(Goal 4)}}$$

From **(36)**, ***sup18***, ***Goal 4***, and Rule (3) we get,

$$N_k| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} N_k) \qquad \textbf{\textit{(Goal 3)}}$$

From ***Mssg8***, we get:

$$U_i \lhd \langle Tm_5, r_i^*, (U_i \overset{ID_i}{\leftrightarrow} \text{GW}), (U_i \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{41}$$

From **(41)**, ***sup19***, and Rule (1),

$$U_i| \equiv GW| \sim \langle Tm_5, r_i^*, (U_i \overset{ID_i}{\leftrightarrow} \text{GW}), (U_i \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{42}$$

From sup***20***, and Rule 4, we get:

$$U_i| \equiv \#\langle Tm_5, r_i^*, (U_i \overset{ID_i}{\leftrightarrow} \text{GW}), (U_i \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{43}$$

From **(42)**, **(43)**, and Rule (2),

$$U_i| \equiv GW| \equiv \langle Tm_5, r_i^*, (U_i \overset{ID_i}{\leftrightarrow} \text{GW}), (U_i \overset{r_i^*}{\longleftrightarrow} GW)\rangle_{X_{g_{N_k}}} \tag{44}$$

From **(5)**, **(6)**, **(44)**, and Rule 5,

$$U_i| \equiv GW| \equiv (U_i \overset{r_i^*}{\longleftrightarrow} GW) \tag{45}$$

From **(45)**, ***sup21***, and Rule (3), we get:

$$U_i| \equiv (U_i \overset{r_i^*}{\longleftrightarrow} GW) \tag{46}$$

From ***Mssg9***,

$$U_i \lhd \langle Tm_3, Tm_4, Tm_5, , Tm_6, V_i^*, \left(N_k \overset{SID_i}{\leftrightarrow} GW\right), r_i^*(U_i \overset{K_l}{\longleftrightarrow} GW)\rangle_{SK} \tag{47}$$

From **(47)**, ***sup9***, and Rule (1),

$$U_i| \equiv\sim \langle Tm_3, Tm_4, Tm_5, , Tm_6, V_i^*, \left(N_k \overset{SID_i}{\leftrightarrow} GW\right), r_i^*(U_i \overset{K_l}{\longleftrightarrow} GW)\rangle_{SK} \tag{48}$$

TABLE 4. Comparison of functionality features of the proposed protocol with related protocols.

S.F	[18]	[20]	[21]	[29]	Our
A1	✗	✗	✗	✓	✓
A2	✓	✗	✓	✓	✓
A3	✓	✓	✓	✓	✓
A4	✗	✗	✗	✓	✓
A5	✗	✓	✓	✓	✓
A6	✗	✗	✓	✓	✓
A7	✓	✗	✓	✓	✓
A8	✗	✓	✓	✓	✓
A9	✗	✗	✓	✓	✓
A10	✓	✗	✓	✓	✓
A11	✓	✗	✓	✓	✓
A12	✗	✓	✓	✓	✓
A13	✓	✓	✓	✗	✓
A14	✓	✓	✓	✓	✓
A15	✗	✗	✓	✗	✓
A16	✓	✗	✓	✓	✓

From ***sup20***, ***sup22***, and Rule (4),

$$U_i| \equiv \#\langle Tm_3, Tm_4, Tm_5, , Tm_6, V_i^*, \left(N_k \overset{SID_i}{\leftrightarrow} GW\right), r_i^*(U_i \overset{K_l}{\longleftrightarrow} GW)\rangle_{SK} \quad (49)$$

From **(48)**, **(49)**, and Rule (2),

$$U_i| \equiv N_k| \equiv \langle Tm_3, Tm_4, Tm_5, , Tm_6, V_i^*, \left(N_k \overset{SID_i}{\leftrightarrow} GW\right), r_i^*(U_i \overset{K_l}{\longleftrightarrow} GW)\rangle_{SK} \quad (50)$$

From **(45)**, **(50)**, and Rule (5),

$$U_i| \equiv N_k| \equiv (U_i \overset{SK}{\longleftrightarrow} N_k) \qquad \textbf{\textit{(Goal 2)}}$$

From **(46)**, ***sup23***, ***(Goal 2)***, and Rule (3),

$$U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} N_k) \qquad \textbf{\textit{(Goal 1)}}$$

As a result, Goal 1, Goal 2, Goal 3, and Goal 4 collectively ensure the mutual authentication between user U_i and IoT node N_k.

VI. PERFORMANCE ANALYSIS AND FUNCTIONALITY COMPARISON

In this section, we compare our proposed protocol with other relevant protocols in terms of security functionalities, computational cost, and communication cost.

A. SECURITY ATTACK COMPARISONS

In this subsection, we compare our proposed protocol in terms of security and functionality with related authentication protocols for the IoT environment and wireless sensor networks.

TABLE 5. Execution time and description of cryptographic operation [29].

Notation	Approx. computation time (ms)	Description (time to compute)
T_h	0.0005	Hash function operation
T_{ecm}	0.0087	Encryption/decryption symmetric cryptographic
T_{fe}	0.063075	Fuzzy extraction operation
T_E	0.063075	ECC point multiplication

Table 4 lists the availability of the functionalities in the protocols of Porambage *et al.* [18] Amin *et al.* [20], Farash *et al.* [21], and Wazid *et al.* [29], compared with the proposed protocol.

The proposed protocol provides all the required functionalities, while other protocols are lacking in key areas such as providing security against impersonation, man-in-the-middle attacks, and offline password guessing attacks, and providing user anonymity.

B. COMPUTATIONAL OVERHEAD COMPARISONS

Here, we compare the proposed protocol with those of Challa *et al.* [19], He *et al.* [27], Challa *et al.* [26], Renuka *et al.* [35], Ma *et al.* [33], Lyu *et al.* [32], Martínez-Peláez *et al.* [34], Wazid *et al.* [29], and Ryu *et al.* [28] during the login and authentication phases. The approximate execution times that are required for the operations are based on the experimental results of [29], as presented in Table 5. The XOR and concatenation operations have much shorter execution times than the other three operations; therefore, these are considered negligible and are omitted from the analysis of the computational cost. Table 6 compares our protocol with relevant recent protocols in terms of computational overhead. In our proposed protocol, we have used lightweight operations (a one-way hash function, a fuzzy extractor, and the XOR operation) compared with other operations that have slightly higher overheads, such as public-key cryptographic functions and symmetric-key encryption/decryption.

According to Table 7, the computation time for the IoT node/sensor node in the proposed protocol is 0.003 ms, which is 95.42%, 97.68%, 98.82%, 97.03%, 91.84%, 85.64%, 88.92, 91.95%, and 97.66% lower than the computation times in the protocols of Challa *et al.* [19], He *et al.* [27], Challa *et al.* [26], Renuka *et al.* [35], Ma *et al.* [33], Lyu *et al.* [32], Martínez-Peláez *et al.* [34], Wazid *et al.* [29], and Ryu *et al.* [28], respectively. Therefore, our proposed protocol is more efficient and more suitable for constrained sensor devices in the IoT environment. Table 8 presents the improvements of our proposed protocol over other existing protocols in terms of computational cost of the IoT nodes. Moreover, Table 8 presents the improvements of our proposed protocol over other protocols in terms of the computational costs to the user, the IoT node, and the gateway node.

TABLE 6. Comparison of computation overheads of our protocol with related protocols.

Protocol	User side, U_i	Sensor device/ sensor side N_k	Gate way side, GW	Total operations	Total overhead/ In second
Challa et al. [26]	$2T_E + 10T_h + 1T_{fe}$ ms	$1T_E + 5T_h$ ms	$5T_h$ ms	$3T_{ecm} + 19T_h + 1T_{fe}$ ms	0.262 ms
He et al. [27]	$11T_h + 2T_E$ ms	$7T_h + 2T_E$ ms	$9T_h$ ms	$18T_h + 4T_E$ ms	0.26 ms
Challa et. al [19]	$\mathbf{6T_h + 5T_E}$ ms	$\mathbf{4T_h + 4T_E}$ ms	$\mathbf{4T_h + 5T_E}$ ms	$\mathbf{14T_h + 14T_E}$ ms	0.89 ms
Renuka et al. [35]	$5T_h + 4T_{ecm}$ ms	$11T_h + 11T_{ecm}$ ms	$11T_h + 11T_{ecm}$	$27T_h + 26T_{ecm}$ ms	1.65 ms
Ma et al. [33]	$4T_h + 3T_{ecm}$ ms	$4T_h + 4T_{ecm}$ ms	$11T_h + 10T_{ecm}$ ms	$19T_h + 17T_{ecm}$ ms	1.081 ms
Lyu et al. [32]	$11T_h + 2T_{ecm}$ ms	$7T_h + 2T_{ecm}$ ms	$8T_h + 2T_{ecm}$ ms	$26T_h + 6T_{ecm}$ ms	0.23 ms
Peláez et al. [34]	$4T_h + 3T_{ecm}$ ms	$2T_h + 3T_{ecm}$ ms	$21T_h + 2T_{ecm}$ ms	$48T_h + 8T_{ecm}$ ms	0.093 ms
Wazid et al. [29]	$13T_h + 1T_{fe} + 2T_{ecm}$ ms	$5T_h + 4T_{ecm}$ ms	$4T_h + 2T_{ecm}$ ms	$22T_h + 1T_{fe} + 8T_{ecm}$ ms	0.578 ms
Li et al. [30]	$12T_h + 1T_{fe} + 3T_E$ ms	$5T_h + 2T_E$ ms	$12T_h + 1T_E$ ms	$29T_h + 1T_{fe} + 6T_E$ ms	0.445 ms
Our Protocol	$8T_h + 1T_{fe}$ ms	$6T_h$ ms	$8T_h$ ms	$22T_h + 1T_{fe}$ ms	0.071 ms

C. COMMUNICATION OVERHEAD COMPARISON

In this subsection, we compare our proposed protocol with those of Dhillon and Kalra [24] (2017), Dammak *et al.* [31] (2019), He *et al.* [27] (2018), Farash *et al.* [21] (2016), Li *et al.* [30] (2018), Lyu *et al.* [32] (2019), Ma *et al.* [33] (2019), and Wazid *et al.* [29] (2018) in terms of the communication cost. For simplicity and conventional comparison, we have assumed that the output sizes of the hash function, the identity *ID*, and ECC point multiplication are 160 bits. Similarly, we assume that the output sizes of the random number and the timestamp are 32 bits and 128 bits for the secret key. In our proposed protocol, there are four messages (M_5, M_6, M_7, and M_8) during the prelogin and authentication phases. The communication cost of message M_5 is 1056 bits, M_6 1120 bits, M_7 384 bits, and M_8 224 bits. As a result, the communication cost of the proposed protocol is 2784 bits. Our protocol is compared with other protocols in Table 9, where the message content is excluded. Hence, our proposed protocol has a lower communication overhead compared with other related protocols.

TABLE 7. Improvement and the computation cost of the IoT node.

Protocol	Computation cost of IoT node/ms	Improvement %
Challa et al. [26]	0.066 ms	95.42
He et al. [27]	0.129 ms	97.68
Challa et. al [19]	0.254 ms	98.82
Renuka et al. [35]	0.101 ms	97
Ma et al. [33]	0.036 ms	91.84
Lyu et al. [32]	0.021 ms	85.64
Peláez et al. [34]	0.027 ms	88.92
Wazid et al. [29]	0.037 ms	91.95
Li et al. [30]	0.128 ms	97.66

TABLE 8. Improvement of our proposed protocol over other protocols in terms of computation cost.

Protocol	Improvement %
Challa et al. [26]	72.93
He et al. [27]	72.69
Challa et. al [19]	92
Renuka et al. [35]	95.7
Ma et al. [33]	93.4
Lyu et al. [32]	69.13
Peláez et al. [34]	24.14
Wazid et al. [29]	88.17
Li et al. [30]	84
Our Protocol	90

TABLE 9. Comparison of communication overhead of our protocol with related protocols.

Protocol	Message size (bits)
Dammak et. al. [31]	3104
Renuka et. al. [35]	3168
Ma et al. [33]	3712
Lyu et al. [32]	4160
Li et al. [30]	2880
Dhillon et al. [24]	4032
Farash et al. [21]	3552
Our protocol	2784

VII. CONCLUSION

This paper proposes a lightweight secure biometrics-based key agreement user authentication protocol for the

IoT environment, where fuzzy extraction and a level 3 feature extractor are used to handle the user's biometric information. The informal security analysis results demonstrate that our protocol can withstand most known malicious attacks and provides most of the required functionalities such as mutual authentication, key agreement, user anonymity and untraceability, and key freshness. Additionally, we have proved the mutual authentication of our protocol between the remote user and the accessed sensing IoT device using the widely accepted BAN logic. Moreover, through the informal security analysis we have proved the security of the proposed protocol and we show that the proposed protocol can resist various known malicious attacks. Furthermore, the proposed protocol is more efficient in terms of computational and communication costs compared with other protocols. Therefore, our protocol has high security, is more efficient in terms of computational and communication costs, and has additional functionalities. Hence, our proposed protocol is more suitable for applications in the IoT environment compared to other related protocols.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for providing constructive and generous feedback.

REFERENCES

[1] D. Pal, B. Papasratorn, W. Chutimaskul, and S. Funilkul, "Embracing the smart-home revolution in Asia by the elderly: An end-user negative perception modeling," *IEEE Access*, vol. 7, pp. 38535–38549, 2019.

[2] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy ensured *e* -healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.

[3] X. Luo, D. Li, and S. Zhang, "Traffic flow prediction during the holidays based on DFT and SVR," *J. Sensors*, vol. 2019, Jan. 2019, Art. no. 6461450.

[4] V. Petrov, K. Mikhaylov, D. Moltchanov, S. Andreev, G. Fodor, J. Torsner, H. Yanikomeroglu, M. Juntti, and Y. Koucheryavy, "When IoT keeps people in the loop: A path towards a new global utility," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 114–121, Jan. 2019.

[5] F. Tao and Q. Qi, "New IT driven service-oriented smart manufacturing: Framework and characteristics," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 1, pp. 81–91, Jan. 2019.

[6] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[7] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[8] M. T. Arafin, M. Gao, and G. Qu, "VOLtA: Voltage over-scaling based lightweight authentication for IoT applications," in *Proc. 22nd Asia South Pacific Design Automat. Conf. (ASP-DAC)*, Jan. 2017, pp. 336–341.

[9] S. Choudhary and A. Oberoi, "Quality improvement by enhancement techniques (QIET) on low quality fingerprint image," *Int. J. Eng. Innov. Technol.*, vol. 3, no. 2, pp. 300–305, Aug. 2013.

[10] M. Sarvabhatla and C. S. Vorugunti, "A secure biometric-based user authentication scheme for heterogeneous WSN," in *Proc. 4th Int. Conf. Emerg. Appl. Inf. Technol.*, vol. 5, Dec. 2014, pp. 367–372.

[11] B.-L. Chen, W.-C. Kuo, and L.-C. Wuu, "Robust smart-card-based remote user password authentication scheme," *Int. J. Commun. Syst.*, vol. 27, no. 2, pp. 377–389, Feb. 2014.

[12] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, 2012.

[13] B.-L. Chen, W.-C. Kuo, and L.-C. Wuu, "A secure password-based remote user authentication scheme without smart cards," *Inf. Technol. Control*, vol. 41, no. 1, pp. 53–59, Apr. 2012.

[14] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[15] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 12, no. 1, pp. 43–59, 2019.

[16] A. K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377–1404, 2015.

[17] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[18] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.

[19] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[20] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, Jun. 2016.

[21] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[22] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[23] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Humanized Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017.

[24] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 34, pp. 255–270, Jun. 2017.

[25] H. Yazdanpanah, M. H. Ahangar, M. Azizi, and A. Ghafouri, "A secure user authentication and key agreement scheme for HWSN tailored for the Internet of Things environment," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 574, Jun. 2017.

[26] 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.

[27] J. He, Z. Yang, J. Zhang, W. Liu, and C. Liu, "On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 1, 2018, Art. no. 1550147718756311.

[28] J. Ryu, H. Lee, H. Kim, and D. Won, "Secure and efficient three-factor protocol for wireless sensor networks," *Sensor*, vol. 18, no. 12, p. 4481, 2018. doi: 10.3390/s18124481.

[29] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[30] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

[31] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–4.

[32] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely access 'my' smart home in private: An anti-tracking authentication and key agreement scheme," *IEEE Access*, vol. 7, pp. 41835–41851, 2019.
[33] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. L. Choo, "An efficient and provably-secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2019.2902840.
[34] R. Martínez-Peláez , H. Toral-Cruz , J. R. Parra-Michel, V. García, L. J. Mena, V. G. Félix, and A. Ochoa-Brust, "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances," *Sensors*, vol. 19, no. 9, p. 2098, May 2019.
[35] K. M. Renuka, S. Kumari, D. Zhao, and L. Li, "Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems," *IEEE Access*, vol. 7, pp. 51014–51027, 2019.
[36] S. F. Aghili, H. Mala, and P. Peris-Lopez, "Securing heterogeneous wireless sensor networks: Breaking and fixing a three-factor authentication protocol," *Sensors*, vol. 18, no. 11, p. 3663, 2018.
[37] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, Jan. 2013.
[38] L. Kotoulas and I. Andreadis, "Colour histogram content-based image retrieval and hardware implementation," *IEE Proc.-Circuits, Devices Syst.*, vol. 150, no. 5, pp. 387–393, Oct. 2003.
[39] A. K. Manjulata, "Survey on lightweight primitives and protocols for RFID in wireless sensor networks," *Int. J. Commun. Netw. Inf. Secur.*, vol. 6, no. 1, p. 29, Apr. 2014.
[40] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.
[41] W. Li, L. Xuelian, J. Gao, and H. Y. Wang, "Design of secure authenticated key management protocol for cloud computing environments," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2019.2909890.
[42] R. Mariño, F. H. Álvarez, and L. H. Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Inf. Sci.*, vol. 195, pp. 91–102, Jul. 2012.
[43] M. Zhang, J. Zhang, and Y. Zhang, "Remote three-factor authentication scheme based on Fuzzy extractors," *Secur. Commun. Netw.*, vol. 8, no. 4, pp. 682–693, Mar. 2015.
[44] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[45] P. Maene, J. Götzfried, R. De Clercq, T. Müller, F. Freiling, and I. Verbauwhede, "Hardware-based trusted computing architectures for isolation and attestation," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 361–374, Mar. 2017.
[46] A. Agrawal, C. M. Ahmed, and E.-C. Chang, "Poster: Physics-based attack detection for an insider threat model in a cyber-physical system," in *Proc. Asia Conf. Comput. Commun. Secur.*, Jun. 2018, pp. 821–823.

BAHAA HUSSEIN TAHER received the bachelor's degree from the Department of Mathematics, College of Pure Science, University of Basrah, Iraq, the bachelor's degree from the Computer Science Department, Science College, University of Basrah, and the master's degree in computer science from the Computer Science Department, Pune University, India. He is currently pursuing the Ph.D. degree in computer science and technology with the Huazhong University of Science and Technology, Wuhan, China. He has nine years of teaching experience and was with the Science College, University of Basrah, before taking study leave and coming to China. His research interest includes security and privacy issues in the IoT and cloud computing.

SHENG JIANG received the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2009, where he is currently a Lecturer with the School of Computer Science and Technology. His current research interests include data mining and natural language processing.

ALI A. YASSIN received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, Hubei, China. He is currently an Assistant Professor with the Computer Science Department, Education College for Pure Science, University of Basrah. His research interests include security of cloud computing, image processing, pattern recognition, biometric, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing.

HONGWEI LU received the B.Sc., M.Sc., and Ph.D. degrees from the Huazhong University of Science and Technology (HUST), Wuhan, China, where he is currently a Professor with the School of Computer Science and Technology. His research interests include security and privacy in ubiquitous computing and electronic commerce, with a focus on security protocol analysis, access control, and trust negotiation.