Hindawi
Journal of Sensors
Volume 2021, Article ID 8871204, 18 pages
https://doi.org/10.1155/2021/8871204

Research Article

A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications

Bahaa Hussein Taher,[1,2] **Huiyu Liu**,[1] **Firas Abedi**,[3] **Hongwei Lu**,[1] **Ali A. Yassin**,[4] **and Alzahraa J. Mohammed**[4]

[1]*School of Computer Science, Huazhong University of Science and Technology, Wuhan, 400037 Hubei, China*
[2]*Department of Mathematics, College of Science, University of Basrah, 61004, Iraq*
[3]*Medical Instrumentation Engineering Techniques Department, Al-Mustaqbal University College, 51001 Hillah, Babil, Iraq*
[4]*Department of Computer Science, Education College of Pure Science, University of Basrah, 61004, Iraq*

Correspondence should be addressed to Huiyu Liu; liuhuiyu@hust.edu.cn

Received 22 August 2020; Revised 24 October 2020; Accepted 28 November 2020; Published 28 April 2021

Academic Editor: ahmed alkhayyat

With the booming integration of IoT technology in our daily life applications such as smart industrial, smart city, smart home, smart grid, and healthcare, it is essential to ensure the security and privacy challenges of these systems. Furthermore, time-critical IoT applications in healthcare require access from external parties (users) to their real-time private information via wireless communication devices. Therefore, challenges such as user authentication must be addressed in IoT wireless sensor networks (WSNs). In this paper, we propose a secure and lightweight three-factor (3FA) user authentication protocol based on feature extraction of user biometrics for future IoT WSN applications. The proposed protocol is based on the hash and XOR operations, including (i) a 3-factor authentication (i.e., smart device, biometrics, and user password); (ii) shared session key; (iii) mutual authentication; and (iv) key freshness. We demonstrate the proposed protocol's security using the widely accepted Burrows–Abadi–Needham (BAN) logic, Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool, and the informal security analysis that demonstrates its other features. In addition, our simulations prove that the proposed protocol is superior to the existing related authentication protocols, in terms of security and functionality features, along with communication and computation overheads. Moreover, the proposed protocol can be utilized efficiently in most of IoT's WSN applications, such as wireless healthcare sensor networks.

1. Introduction

The IoT has been a trend in the last few years, and it is expected to be so in the future [1]. In an IoT system, information is being sensed/collected by IoT sensing devices such as embedded systems, Radio Frequency Identification (RFID), wearable devices, and low powered IEEE 802.15.4 devices before being sent to another intermediary device/node (e.g., edge or fog computing node), IoT device, or to the cloud, via the Internet. In IoT, many devices can interact with each other over the Internet. A lot of IoT applications, already, have been deployed such as healthcare systems, smart cities, smart industrial, transportation systems, and smart homes [2, 3]. In these IoT applications, WSNs are most necessary and important [4]. The use of WSNs has greatly increased in providing services to activities and monitoring environments due to its low costs, ease of deployment, a wide range of applications, and flexibility [5]. Therefore, security and privacy are a significant challenge in any consumer technology deployment [6]. For example, let us highlight on an IoT healthcare application [7] as shown in Figure 1. In this scenario, the quality of healthcare service can be enhanced by allowing a medical practitioner to direct access to data that have sensed by the medical sensor nodes deployed in his patient's body. This information can involve current vital reading such as blood pressure, cholesterol, C-reactive protein, and blood sugar level. Accordingly, based on this private and secret current information, a decision can be taken

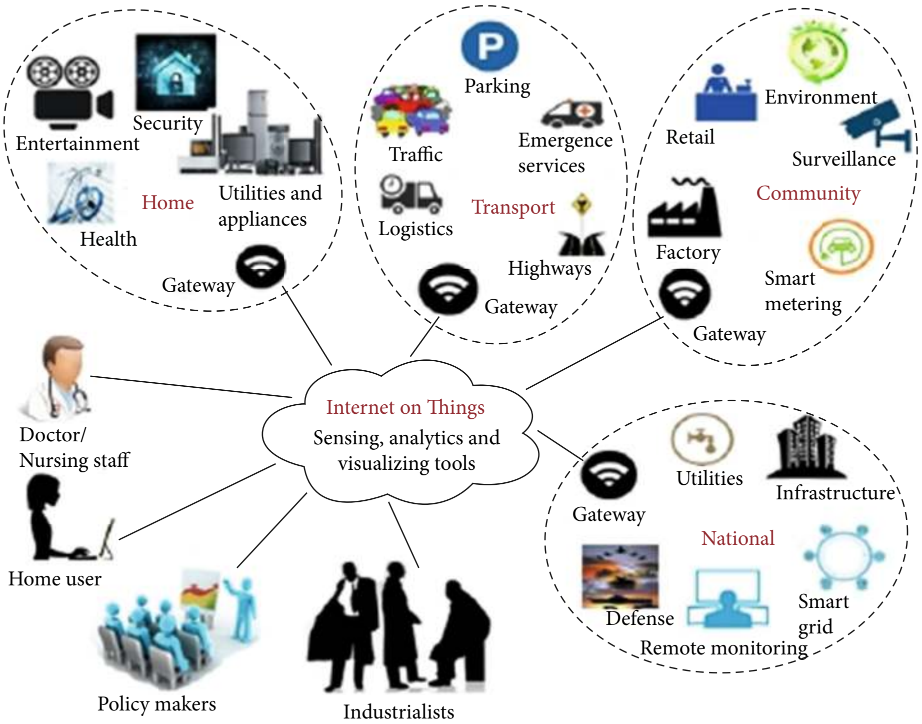


Figure 1: Authentication model for future IoT WSN applications [7].

regarding the patient's health condition to provide necessary remedial actions.

In IoT, the sensor node/devices in WSN face a significant security challenge. Usually, those sensor nodes are deployed in places that are easy for people to touch. Nowadays, one of the most possible critical security attacks that easily happen is a node captured attack where the authentication information that is inside the sensor node is revealed by physical crack [8]. Furthermore, new remote user authentication that is also possible could be vulnerable to this attack because the malicious attacker possibly obtained all sensitive authentication information through this attack. Thus, the security issues in IoT WSN applications are significant and catch more attention. To satisfy this goal, we proposed a secure and lightweight remote user authentication and key agreement protocol to operate in an IoT WSN application environment.

1.1. Motivation. The IoT WSN has opened up many opportunities in various walks of life and particularly in healthcare, shipping, warehousing, and logistics, which have facilitated processes for consumers and businesses. This wide-ranging and rapid development has led to the emergence of great challenges that require the design of high-security protocols for IoT applications in order to preserve the sensitive information of users. Security is now the primary challenge facing the IoT WSN environment. In an IoT WSNs, remote users can access data from IoT sensor nodes via the Internet. Researchers have developed effective mechanisms to integrate wireless networks into the Internet of things environments [9, 10]. Sensor nodes are inherently resource-constrained devices in terms of limited processing capability, constrained communication bandwidth, and very low storage capacity due to the physical size and limited energy [11]. Therefore, designing a secure and efficient remote user authentication protocol for IoT WSN environments is a nontrivial challenge. In IoT environments, the security efficiency of remote user authentication is an important issue for transmitting information securely [12–14]. In addition, energy consumption and computational and communication efficiency are crucial due to the WSN resources energy limitation. Also, due to constrained sensors, adding resourceful gateway nodes can support the sensors, can provide quick on-demand delivery of information, and take care of most of the processing. The authentication of users or devices is a critical issue that must be considered in the context of IoT security. Most of the traditional authentication protocols are based on a password, a smart card, or both. These protocols are ineffective at present since attackers have modified the methodology of their attacks on IoT devices. The need for biometric-based approaches that are difficult to reproduce, such as those involving fingerprints, iris scanning, and facial patterns, has emerged as an additional factor that can enhance the security of Internet applications.

1.2. Attack Model. In our proposed protocol, we follow the widely accepted and more realistic Dolev-Yao threat (DY) model [15]. In this model, the communication between two entities is accomplished over a public (open) channel. Also, an adversary *MA* will have full control over the communication channel. Therefore, *MA* can alter, eavesdrop, insert, and delete forgery messages that are being transmitted during communication. In addition, it is assumed that MA can physically capture one or more IoT sensing nodes in IoT and can steal all sensitive information stored in the captured sensing nodes which utilize the strength analysis attacks.

1.3. Our Contribution. The main contributions of our proposal are as follows:

(1) We proposed a lightweight and secure remote user authentication protocol based on feature extraction of the user fingerprint and one-way hash function for IoT WSN applications which is suitable to use in wireless healthcare application. The proposed protocol is three factors: user password, smartphone, and biometrics to achieve our goal. We used biometrics to increase the security of the protocol due to difficulty to forge or steal or forget biometrics

(2) Level 3 feature extraction is done to overcome the problem of noise in fingerprint images in existing authentication schemes

(3) We prove our protocol secure using informal and formal security analysis through BAN logic and random oracle model

(4) We simulate the proposed protocol using the popular and widely accepted tool called AVISPA and demonstrate that the protocol is perfectly secure against active and passive attacks

(5) Comparative evaluation of our protocol with related protocols in terms of communication and computational overheads was performed

2. Related Work

The general security requirements needed to secure an IoT WSN environment are authentication, integrity, confidentiality, availability, nonrepudiation, authorization, freshness, forward, and backward secrecy. Therefore, a remote user authentication scheme designed for an IoT WSN environment should be designed in a way that ensures it will withstand many attacks such as man-in-the-middle, online/offline guessing, replay, privileged insider, stolen/lost smart card, password change, and sensing device capture. Also, the designed scheme should reduce computation and communication costs and include the password/biometric update phase. Presume a scenario for a medical practitioner wandering the medical IoT environment. In such an assumption, we need to preserve certain information about this user such as achieving anonymity preservation to prevent other parties (users) from revealing the patient's critical privacy information while he/she joins the system sessions. By way of explanation, user anonymity is one of important key features in the user authentication protocol [16]. Also, the untraceability feature is important in the IoT WSN applications to prevent an attacker from tracing a user during a session [17]. WSNs have become an important and necessary network infrastructure after modernization, and they can be generally used in many modern fields such as health monitoring, environments, and smart homes [18–21]. To gratify the security requirements of the IoT WSN environment, numerous user authentication protocols have been proposed. Shi and Gong [22] proposed a new user-authentication scheme using ECC for the WSNs. Unfortunately, the storage and computational overhead are relatively high so it is not applicable for healthcare application systems [23–25].

Usually, the real-time users adopt to use easy-to-memorialize parameters, such as secret keys and identities, for their convenience, as explain in [23–25]; hence, user anonymity is not provided. For the enhancement security of IoT WSNs, studies in [26–30] presented lightweight remote user authentication schemes. Nonetheless, these contributions have need of improvements to resist attacks while persevering optimum communication and computation performance. In 2016, Arasteh et al. [31] proposed an authentication scheme for an IoT network that aimed to overcome the weaknesses of a scheme designed by Amin et al. [32]. In 2017, Dhillon and Kalra's [33] proposed a lightweight 3FA scheme using a user password, biometric, and a mobile device. They pointed out that their scheme is secure against well-known attacks such as a denial of service, impersonation, offline password guessing, and stolen mobile device attacks. However, their scheme is still insecure against the mentioned attacks and does not afford a session key agreement. In the same year, Li et al. [34] and Zhang et al. [35] presented their authentication schemes with key agreement. They showed that their scheme was lightweight and appropriate for constrained IoT environments. In 2018, several studies were published on remote user authentication for the IoT environment [36–41]. The author in [36] presented an authentication scheme for ad hoc WSN to improve the security weakness of the scheme in [42] using ECC cryptograph. In Cyber-Physical Systems (CPS) and IoT, Lu et al. [37] presented a mutual authentication proposed scheme with user anonymity. Xu et al. [38] proved that Srinivas et al.'s [43] authentication schemes are vulnerable by many attacks and did not achieve user anonymity features. Moreover, Ryu et al. [39] reviewed Wu et al.'s [44] scheme and pointed out that Wu et al.'s scheme has two security weaknesses against outsider attackers. A new user authentication scheme was presented by Wazid et al. [40] for a hierarchical IoT network. These authors observed that their scheme involved lower computation and communication costs. Moreover, Chen et al. [41] presented an authentication scheme based on the fuzzy extractor. Nonetheless, the overhead in Chen's scheme is costly.

More recently, in 2019, articles on this subject were published by Dammak et al. [45], Gupta et al. [46], Lyu et al. [47], Ma et al. [48], Renuka et al. [49], and Li et al. [50]. However, these schemes still have weaknesses, particularly in terms of the computation and communication overheads, which are highly compared to those of our proposed scheme. In summary, most remote user authentication protocols either fail to achieve IoT WSN environment security requirements or they do not provide security functionality features such as dynamic anonymity and untraceability and biometric and password change procedures. To overcome the aforementioned weaknesses, we proposed a lightweight remote user authentication protocol suited for the IoT WSN application, which achieves user anonymity and untraceability.

3. Basic Preliminaries

In this section, we briefly discuss the properties of the one-way hash function, perceptual hashing, and level 3 feature extraction.

(i) Level 3 feature extraction of fingerprint: a fingerprint is the pattern of ridges and valleys on the outer surface of the fingertip, and each individual has unique fingerprints. Fingerprint identification involves three levels: the first level includes details such as thr pattern type and ridge-line flow; the second involves minutiae points for instant bifurcations, spurs, and terminations; and the third relates to the dimensional properties of a ridge, such as incipient ridges, creases, pores, and edge contours The third level contains all the dimensional properties of a ridge for instant sweat pores, initial ridges, edge, and the crispiness. Our proposed protocol therefore adopts the third level, since it is unique, unalterable, and perpetual. More detail can be found in [51].

(ii) One-way hash function: one-way hash function (1HF) is a mathematical function that is broadly used in many applications, such as disclose data integrity during transmission, generating message authentication codes (MAC), and digital forensic investigations. Cryptographic 1HF is highly sensitive to even small perturbations to the input. The 1HF is impossible to invert, i.e., it is difficult to regain the original text from the hash value. It produces hash values of 128 bits and higher. Generally, 1FH is used to generate digital signatures, which are used to recognize and authenticate the sender [52].

(iii) Perceptual hashing: when using biometrics for user authentication schemes, the standard encryption or hashing algorithms cannot be used to encrypt the biometric template. The biometric data such as fingerprint and voice. change with time and environment. Therefore, in designing a user authentication protocol using biometrics, the hashing or encryption algorithms cannot be utilized to encrypt the biometric template. To deal with this issue, researchers have proposed using perceptual hashing (p-hash) [53]. The advantage of using p-hash is capability tolerant to unimportant variation in the quality and format of the input. The hash value size that is generated by perceptual hashing differs from 64 to 128 bits [54]. In this paper, we adopted the perceptual hashing function proposed by Jie [55] in a previous study. The authors in [56] merge the image blocks which have low-frequency DCT coefficients and the color histogram as a perceptual feature, and this perceptual feature then compressed as interfeature with PCA and threshold the interfeature to generate a strong hash. Figure 2 shows the process of perceptual hashing

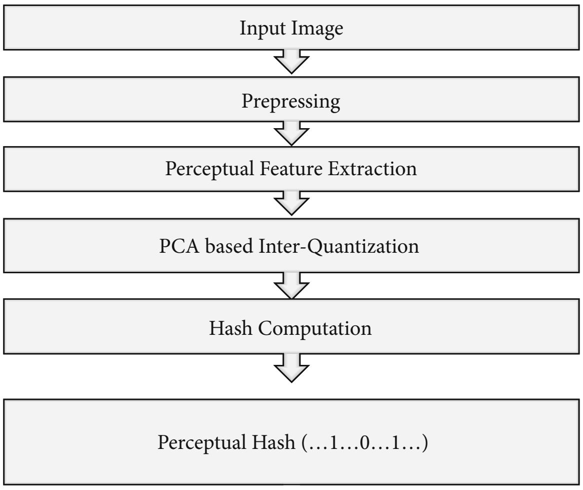

Input Image
Prepressing
Perceptual Feature Extraction
PCA based Inter-Quantization
Hash Computation
Perceptual Hash (…1…0…1…)

Figure 2: Perceptual hashing based on block-DCT and PCA based image.

4. The Proposed Protocol

In this section, we propose an efficient and secure user authentication protocol for IoT WSN applications using the network model scenario presented in Figure 1. We also mention that the proposed protocol is designed to be generic enough for most IoT WSN applications that require user authentication. A summary of the symbols used in this paper is given in Table 1. In this work, we utilize the current timestamps to ensure flexibility to replay attacks. In this work, we utilize the current timestamps to ensure flexibility to replay attacks. Consequently, the clocks of all protocol objects are assumed to be synchronized which is a typical assumption in the literature [7, 44, 57]. Our authentication protocol based on three factors, namely, password, user's biometric, and smartphone focuses on the user in order to reduce the costs to the IoT nodes. Using a smart device such as a smartphone, the user can easily access the IoT nodes and the services they provide.

The proposed protocol contains three participants: a remote user (U_i) who aims to maximize the services in the environment, a set of IoT sensor nodes (D_k), and a trusted home authority/gateway (GW). Our work consists of four phases: registration, precomputation, authentication and key agreement, and password change phase. The registration phase was performed once, while the precomputation, authentication, and password change phase are executed whenever a remote user wishes to login or change his/her password. The proposed protocol enables the remote users to freely update his password and/or biometric information with the help of the smartphone without further involving GW.

4.1. Remote User Registration Phase. User side: at this stage, U_i who aims to access IoT resources must initially register in the GW. To complete the registration, U_i executes the following steps:

(Step 1) The U_i selects his identity (ID_i) and password(PW_i). Afterwards, U_i inputs his/her fingerprint(FP_i)

Table 1: Symbols used.

Notation	Description
U_i	Remote user
ID_i	Identity of the user
$PW_i \mathrm{IS}_i$	The user password Extracting user iris
R_i,R_k	Random numbers generated by the user
FP_i	The fingerprint of the user
$FX3$	Feature extraction level 3
D_k	IoT sensing nodes
$X_{g_{D_i}}$	The shared secret key of the IoT devices, generated by D_k
GW	The trusted gateway node
X_g	A secret key generated by the gateway
X_{g_u}	A secret key generated for the user
TS_1, TS_2, TS_3, TS_4, T	Timestamps
SK	Shared session key
$\bigoplus$	XOR operation
$\|$	Concatenation operation
$H(.)$	One-way hash function

(Step 2) The U_i computes level 3 feature extraction of the fingerprint as follows: $FX3_{FP_i} = \mathrm{FeatExt}(FP_i)$

(Step 3) The U_i selects a random integer $R_i \in Z_n^+$ and computes a mask for the user's identity, password, and fingerprint as follows: identity mask: $MID_i = H(ID_i \bigoplus R_i)$, password mask: $MPW_i = H(PW_i \bigoplus_i R_i)$, and fingerprint mask: $MFP_i = h(FX3_{FP_i})$

(Step 4) The U_i sends MID_i, MPW_i, MFP_i, and $FX3_{FP_i}$ to the GW as a communication request to the GW node through a secure channel

Gateway side: on receiving a request message from U_i, the GW performs the following steps.

(Step 1) GW generates secret keys X_g and X_{g_u}. Following this, GW computes the security parameters $a_i = H(MID_i \bigoplus X_g)$, $b_i = H(MPW_i \bigoplus X_{g_u})$, and $c_i = H(FX3_{FP_i} \bigoplus X_{g_u})$, prior to use

(Step 2) GW calculates $\mathrm{Factor} = \sum_{i=1}^{L} ASCII(FX3_{FP_i})$, $e_i = a_i^{f_i} \bigoplus X_{g_u}$, and $f_i = b_i^{f_i} \bigoplus X_{g_u}$

(Step 3) The GW node submits $M_1 = MID_i$, e_i, f_i, X_{g_u}, and MFP_i to U_i. On receiving M_1, U_i saves it in the memory of the device. Figure 3 summarizes the different processing steps followed during this phase

4.2. IoT Sensor Node Registration. In this stage, each IoT sensor node is a registry. Any supplementary nodes can be added dynamically. This stage consists of the following steps.

IoT node side:

(Step 1) D_k generates a random number $R_k \in Z_n^+$. D_k known the shared secret $X_{g_{D_k}}$ of the GW and has a unique identity $ID_{D_k}^*$

(Step 2) D_k computes the parameters $MPW_j = h(X_{g_{D_k}} \| R_k \| ID_{D_k}^*)$ and $MD_k = R_k \bigoplus X_{g_{D_k}} \bigoplus \mathrm{Factor}_i$ for further calculation

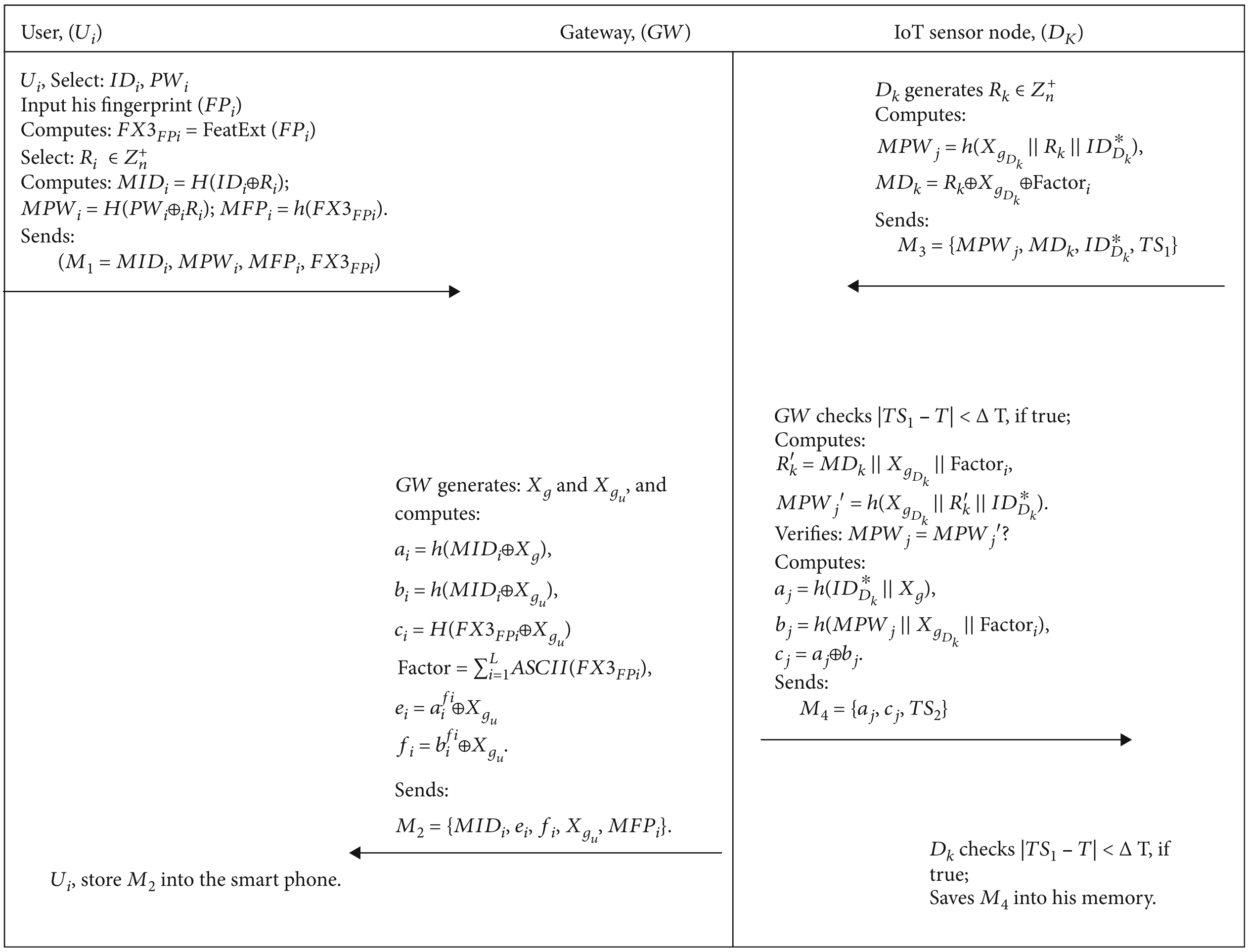
(Step 3) D_k sends MPW_j, MD_k, $ID_{D_k}^*$, and TS_1 to the GW through a secure channel

GW node side: upon receiving the registration request from IoT sensor nodes D_k, the Gw calculates the following steps.

(Step 1) Checks the timestamp condition $|TS_1 - T| < \triangle T$. If the condition is unsatisfied, then the registration phase is terminated; otherwise, the GW executes the next step

(Step 2) Computes $R_k' = MD_k \bigoplus X_{g_{D_k}} \bigoplus \mathrm{Factor}_i$, and MPW_j' on the basis of the previous message received from U_i as $MPW_j' = h(X_{g_{D_k}} \| R_k' \| ID_{D_k}^*)$

(Step 3) Verifies whether $MPW_j = MPW_j'$ or not. Therefore, if they are not unequal, the node is not



U_i, Select: ID_i, PW_i
Input his fingerprint (FP_i)
Computes: $FX3_{FPi}$ = FeatExt (FP_i)
Select: $R_i \in Z_n^+$
Computes: $MID_i = H(ID_i \oplus R_i)$;
$MPW_i = H(PW_i \oplus_i R_i)$; $MFP_i = h(FX3_{FPi})$.
Sends:
$(M_1 = MID_i, MPW_i, MFP_i, FX3_{FPi})$

D_k generates $R_k \in Z_n^+$
Computes:
$MPW_j = h(X_{g_{D_k}} \,||\, R_k \,||\, ID^*_{D_k})$,
$MD_k = R_k \oplus X_{g_{D_k}} \oplus \text{Factor}_i$
Sends:
$M_3 = \{MPW_j, MD_k, ID^*_{D_k}, TS_1\}$

GW checks $|TS_1 - T| < \Delta$ T, if true;
Computes:
$R'_k = MD_k \,||\, X_{g_{D_k}} \,||\, \text{Factor}_i$,
$MPW_j{}' = h(X_{g_{D_k}} \,||\, R'_k \,||\, ID^*_{D_k})$.
Verifies: $MPW_j = MPW_j{}'$?
Computes:
$a_j = h(ID^*_{D_k} \,||\, X_g)$,
$b_j = h(MPW_j \,||\, X_{g_{D_k}} \,||\, \text{Factor}_i)$,
$c_j = a_j \oplus b_j$.
Sends:
$M_4 = \{a_j, c_j, TS_2\}$

GW generates: X_g and X_{g_u}, and computes:
$a_i = h(MID_i \oplus X_g)$,
$b_i = h(MID_i \oplus X_{g_u})$,
$c_i = H(FX3_{FPi} \oplus X_{g_u})$
Factor $= \sum_{i=1}^{L} ASCII(FX3_{FPi})$,
$e_i = a_i^{fi} \oplus X_{g_u}$
$f_i = b_i^{fi} \oplus X_{g_u}$.
Sends:
$M_2 = \{MID_i, e_i, f_i, X_{g_u}, MFP_i\}$.

U_i, store M_2 into the smart phone.

D_k checks $|TS_1 - T| < \Delta$ T, if true;
Saves M_4 into his memory.

FIGURE 3: Summarize of the user registration phase.

illegitimate, and the GW terminates the session. Otherwise, GW executes the next step

(Step 4) Computes the following parameters for further use, $a_j = h(ID^*_{D_k} \| X_g)$, $b_j = h(MPW_j \| X_{g_{D_k}} \|$ Factor$_i)$, and $c_j = a_j \bigoplus b_j$

(Step 5) Then, GW sends a_j, c_j, and TS_2 to D_k. Upon receiving the registration messages (a_j, c_j, and TS_2) from the GW, D_k checks the timestamp condition $|TS_2 - T| < \triangle T$ to verify for any external interference. If the condition is unsatisfied, then the session is terminated; otherwise, D_k saves the parameters a_j, c_j. and TS_2 into his device memory. Finally, the user registration phase is accomplished. Figure 3 shows the steps of the IoT sensor node registration phase

4.3. Precomputation and Login Phase. Once the registration is accomplished successfully, an authorized user U_i can access any desired sensor node within the IoT network through the authentication phase. To start with the authentication phase, U_i must login to the selected IoT service application, following the login steps that are implemented during this phase.

(Step 1) First, the user U_i uses the smartphone to open the applications and enters his/her password PW_i and level 3 feature extraction $FX3_{FP_i}$ saved in the smartphone

(Step 2) Then, the smartphone of U_i calculates a masked for the password and the feature extraction as follows: $MPW'_i = h(MPW_i \bigoplus R_i)$ and $MFP'_i = h(MFP_i \bigoplus R_i)$. Also, it computes $b_i^{**} = h(a_i^{\text{Factor}_i} \bigoplus e_i \bigoplus MPW_i \bigoplus X_{g_n})$ and $c_i^{**} = h(MFP_i \bigoplus b_i^{\text{Factor}_i} \bigoplus \text{Factor}_i)$

(Step 3) Next, the original values of b_i and c_i extract as follows: $b_i^* = h(MPW_i \bigoplus X_{g_u})$ and $c_i^* = h(MFP_i \bigoplus X_{g_u})$

(Step 4) $\mathrm{U_i}$ computes the value of the following verification parameters $\mathrm{b_i^{**}}$ and $\mathrm{c_i^{**}}$ as $b_i^{**} = h(a_i^{\text{Factor}_i} \bigoplus e_i \bigoplus MPW_i \bigoplus X_{g_n})$ and $c_i^{**} = h(MFP_i \bigoplus b_i^{\text{Factor}_i} \bigoplus \text{Factor}_i)$

(Step 5) Then, the accurateness of b_i^* and c_i^* is verified with $\mathrm{b_i^{**}}$ and $\mathrm{c_i^{**}}$. If $b_i^* = \mathrm{b_i^{**}}$? and $c_i^* = \mathrm{c_i^{**}}$?, then the login proceeds to the next step. Otherwise, the user is not legal and has entered incorrect credentials, and the process will terminate

(Step 6) On successful the user validation, it calculates the security parameters: $UD_k = h(X_{g_u} \| TS_1 \| \text{Factor}_i R_i)$ and $UC_i = R_i \oplus a_i$

(Step 7) Also, calculates $\text{Factor}_i^* = \text{Factor}_i \oplus TS_1$ for use in a security check later

(Step 8) In the end, U_i sends the login parameters $M_5 = \{\text{Factor}_i^*, UD_k, UC_i, TS_3, e_i, f_i\}$ to the desired IoT node. Upon completing step 8, the login phase is complete. The user U_i can select any node in the IoT environment

4.4. Authentication and Key Agreement Phase. To access the services of the IoT sensor nodes, the user will attempt to login to the proper node, after which the node will redirect the user login request to GW, which will carry out the necessary process to check the user's authentication. When mutual validation is achieved between these three entities, a session key will be established between the user and the IoT sensor node. Figure 4 summarizes the login and the authentication phase. The following steps illustrate the processes of this phase.

(Step 1) On receiving the login request message from U_i, D_k performs the timestamp check on receive TS_3, i.e., $(|TS_3 - T| < \Delta T)$. Also, check the security parameter $(\text{Factor}_i^* ? = \text{Factor}_i \oplus TS_1)$?, to authenticate the U_i. If the condition is unsatisfied, then the login is terminated; otherwise, the process proceeds to the next step

(Step 2) D_k uses the stored values of e_j and a_j to calculate $b_j = e_j \oplus a_j$

(Step 3) Next, D_k calculates $A_j = h(X_{g_{D_k}} \| TS_1 \| TS_2) \oplus b_j$

(Step 4) D_k sends $M_6 = \{UC_i, UD_k, e_i, f_i, TS_3, TS_4, \text{Factor}_i^*\}$ to the GW. GW can recognize the legitimacy of the U_i and the node D_k on the basis of the parameter Factor_i^* and the transaction time. In this step, the node D_k authenticates the GW

(Step 5) GW verifies the received timestamp $(|TS_4 - T| < \Delta T)$ and $(\text{Factor}_i^* ? = \text{Factor}_i \oplus TS_1)$, authority of the U_i, and the device D_k simultaneously. If the condition is satisfied, then the GW proceeds to the next step; otherwise, the process is terminated

(Step 6) Then, GW calculates the security parameters: $a_j^* = h(ID_{D_k} \| X_g)$, $b_j^* = e_i \oplus a_j^*$, and $b_j = A_j \oplus h(X_{g_{D_k}} \| TS_3 \| TS_4)$. Afterwards, the GW checks the quality of b_j and b_j^*. If they are equal, then GW authenticates the node D_k and the user U_i

The IoT sensor node D_k must be successfully verified by the GW on the basis of the retrieved $(Factor_i)$ depending on MID_i. Therefore, GW performs the following:

(Step 1) GW calculates $R_i^* = UC_i \oplus h(MID_i \oplus X_g)$ and $UD_k^* = h(X_{g_{u_i}} \| TS_3 \| \text{Factor}_i \| R_i^*)$

(Step 2) GW compares the original UD_k and the calculated UD_k^* to authenticate the U_i. If the verification condition is unsuccessful, then the GW terminates the communication; otherwise, the GW continues to the next step

(Step 3) Next, GW computes the security parameters: $GP_{ij} = \text{Factor}_i^* \oplus R_i^* \oplus h(a_j^* \| X_{g_{D_k}})$ and $V_i = h(UD_k^* \| TS_3 \| TS_4 \| TS_5 \| X_{g_u})$

(Step 4) GW submits $M_7 = \{GP_{ij}, V_i, TS_5\}$ to D_k

Upon receiving the verification parameters M_7 from the GW, D_K computes the following processes:

(Step 1) D_k verifies the timestamp$|TS_5 - T| < \triangle T$. If the verification condition is unsatisfied, then the process is terminated; otherwise, it continues forward

(Step 2) Then, D_K checks the validity of GP_{ij} with $\text{Factor}_i^* \oplus R_i \oplus h(a_j^* \| X_{g_{D_k}})$. If the condition is unsatisfied, then the process is terminated; otherwise, it proceeds to the next step

(Step 3) Next, D_K calculates $cha = R_i \oplus \text{Factor}_i \oplus M_i$, and $V_i^* = h(V_i \| TS_4 \oplus M_i)$, where M is a random number generated once. Afterwards, D_K computes the session key as $SK = h(R_i \oplus M_i \oplus \text{Factor}_i^*)$

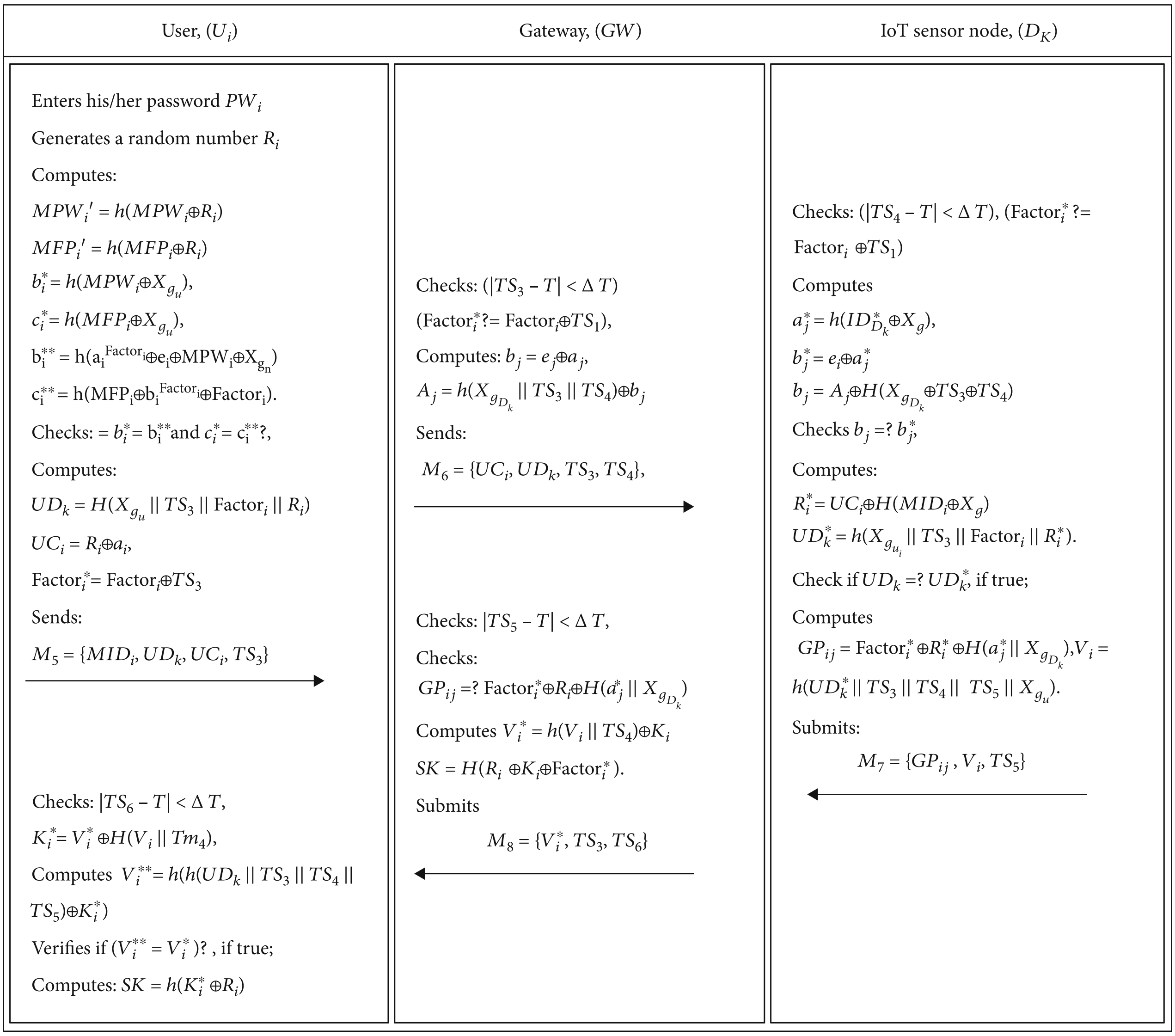
(Step 4) At last, D_K sends $M_8 = \{V_i^*, TS_3, TS_4, TS_5, TS_6, cha\}$ to the U_i. When U_i receives the verification parameter M_8 from D_K, U_i executes the following steps:

(Step 1) U_i performs timestamp checks, i.e., $|TS_6 - T| < \triangle T$? If not, then the process is terminated; otherwise, it continues to the next step

(Step 2) U_i retrieves $M_i^* = cha \oplus R_i \oplus \text{Factor}_i^*$

(Step 3) Then, U_i computes $V_i^{**} = h(h(UD_k \| TS_3 \| TS_4 \| TS_5) \oplus M_i^*)$. Then, U_i verifies if $(V_i^{**} = V_i^*)$. If not, then U_i is unsure of the authority of D_K and the GW; otherwise, the U_i computes the session key as $SK = h(M_i^* \oplus R_i)$ and the authentication and key agreement phase successfully

4.5. Password and Biometric Change Phase. This phase is necessary to regularly update the user password to preserve high security. The proposed protocol allows the remote user to change his/her password easy.



User, (U_i)

Enters his/her password PW_i

Generates a random number R_i

Computes:

$MPW_i' = h(MPW_i \oplus R_i)$

$MFP_i' = h(MFP_i \oplus R_i)$

$b_i^* = h(MPW_i \oplus X_{g_u})$,

$c_i^* = h(MFP_i \oplus X_{g_u})$,

$\mathrm{b_i^{**} = h(a_i^{Factor_i} \oplus e_i \oplus MPW_i \oplus X_{g_n})}$

$\mathrm{c_i^{**} = h(MFP_i \oplus b_i^{Factor_i} \oplus Factor_i)}$.

Checks: $= b_i^* = \mathrm{b_i^{**}}$ and $c_i^* = \mathrm{c_i^{**}}$?,

Computes:

$UD_k = H(X_{g_u} \,||\, TS_3 \,||\, \mathrm{Factor}_i \,||\, R_i)$

$UC_i = R_i \oplus a_i$,

$\mathrm{Factor}_i^* = \mathrm{Factor}_i \oplus TS_3$

Sends:

$M_5 = \{MID_i, UD_k, UC_i, TS_3\}$

Checks: $|TS_6 - T| < \Delta T$,

$K_i^* = V_i^* \oplus H(V_i \,||\, Tm_4)$,

Computes $V_i^{**} = h(h(UD_k \,||\, TS_3 \,||\, TS_4 \,||\, TS_5) \oplus K_i^*)$

Verifies if $(V_i^{**} = V_i^*)$? , if true;

Computes: $SK = h(K_i^* \oplus R_i)$

Gateway, (GW)

Checks: $(|TS_3 - T| < \Delta T)$

$(\mathrm{Factor}_i^* ?= \mathrm{Factor}_i \oplus TS_1)$,

Computes: $b_j = e_j \oplus a_j$,

$A_j = h(X_{g_{D_k}} \,||\, TS_3 \,||\, TS_4) \oplus b_j$

Sends:

$M_6 = \{UC_i, UD_k, TS_3, TS_4\}$,

Checks: $|TS_5 - T| < \Delta T$,

Checks:

$GP_{ij} =? \mathrm{Factor}_i^* \oplus R_i \oplus H(a_j^* \,||\, X_{g_{D_k}})$

Computes $V_i^* = h(V_i \,||\, TS_4) \oplus K_i$

$SK = H(R_i \oplus K_i \oplus \mathrm{Factor}_i^*)$.

Submits

$M_8 = \{V_i^*, TS_3, TS_6\}$

IoT sensor node, (D_K)

Checks: $(|TS_4 - T| < \Delta T)$, $(\mathrm{Factor}_i^* ?= \mathrm{Factor}_i \oplus TS_1)$

Computes

$a_j^* = h(ID_{D_k}^* \oplus X_g)$,

$b_j^* = e_i \oplus a_j^*$

$b_j = A_j \oplus H(X_{g_{D_k}} \oplus TS_3 \oplus TS_4)$

Checks $b_j =? b_j^*$,

Computes:

$R_i^* = UC_i \oplus H(MID_i \oplus X_g)$

$UD_k^* = h(X_{g_{u_i}} \,||\, TS_3 \,||\, \mathrm{Factor}_i \,||\, R_i^*)$.

Check if $UD_k =? UD_k^*$, if true;

Computes

$GP_{ij} = \mathrm{Factor}_i^* \oplus R_i^* \oplus H(a_j^* \,||\, X_{g_{D_k}})$, $V_i = h(UD_k^* \,||\, TS_3 \,||\, TS_4 \,||\, TS_5 \,||\, X_{g_u})$.

Submits:

$M_7 = \{GP_{ij}, V_i, TS_5\}$

Figure 4: Summarize of login and Authentication Phase.

(Step 1) U_i who must change his/her password opens the IoT application on a smart device and enters his/her old password MPW_i and feature extraction MFP; then, he/she calculates the masked for each of and feature extraction of user biometrics as $MPW_i = h(MPW_i \bigoplus R_i)$, $MFP_i = h(MFP_i \bigoplus R_i)$

(Step 2) Then, U_i calculates $b_i^{**} = h(a_i^{\mathrm{Factor}_i} \bigoplus e_i \bigoplus MPW_i \bigoplus X_{g_n})$ and $c_i^{**} = h(MFP_i \bigoplus b_i^{\mathrm{Factor}_i} \bigoplus Factor_i)$ and proceeds to the next step

(Step 3) Next, U_i checks the equality of b_i^{**} and c_i^{**} with the original one $b_i^* = h(MPW_i \bigoplus X_{g_u})$ and $c_i^* = h(MFP_i \bigoplus X_{g_u})$. If any conditions do not hold, the U_i unsuccessfully enters his correct data, and the system will be terminated; otherwise, U_i is a valid user, and then U_i is permitted to change his/her password

(Step 4) U_i enters the new password PW_i^* and new fingerprint FP_i^*. Then, he/she calculates mask the hash function for each of them as $MPW_i^* = h(PW_i^*{}_i \bigoplus_i R_i)$ and $MFP_i^* = h(FP_i^* \bigoplus R_i)$, correspondingly

(Step 5) Then, U_i updates the parameter b_i^* on the basis of the new password as $b_i' = h(MPW_i^* \oplus X_{g_u})$. Then, it calculates new f_i as: $f_i' = b_i^{\prime f_i} \bigoplus X_{g_u}$

(Step 6) At last, U_i changes the old f_i stored in the smart device memory with the new one f_i', and the phase terminates successfully

Table 2: BAN logic symbols and their respective abbreviations.

Symbols	Abbreviation
$P \mid \equiv X$	P believes X as a valid statement.
$P \triangleleft X$	Principal P sees the statement X.
$P \mid \sim X$	Principal P once said the statement X.
$\#(X)$	The formula X is fresh.
$P\overset{K}{\longleftrightarrow}Q$	P and Q use the shared session key K to communicate, and K will never be discovered by any principal except P and Q.
$P \Longrightarrow X$	P has jurisdiction over X.
$(X)_K$	X is hashed with the key K.
$\langle X \rangle_K$	X is combined with the key K.
$\{X\}_K$	X is encrypted with the key K.

5. Security Analysis

We evaluate the security strength of the proposed protocol using both formal and informal security analysis in this section. First, we prove that the proposed protocol provides mutual authentication between the remote user and the IoT sensor node using the BAN logic verification. First, we prove that the proposed protocol provides mutual authentication between the remote user and the IoT sensor node using the BAN logic verification. Then, we prove that the proposed protocol is resistant to other well-known attacks using informal security analysis. After that, we perform a formal security analysis using the popular widely accepted automated verification tool, AVISP.

5.1. Mutual Authentication Proof through BAN Logic. We use the widely recognized BAN logic [58] to prove that the mutual authentication is achieved between the registered legitimate remote user and an accessed IoT sensor node with the help of a trusted gateway node. Table 2 shows the symbols used of BAN logic and their respective abbreviations, where P and Q represent the principals, and X denotes a statement.

There are five rules used which govern the BAN logic are listed as follows:

Rule 1: message meaning rules: $P \mid \equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft (X)_K / P \mid \equiv Q \mid \sim X$ OR $P \mid \equiv P \overset{Y}{\rightleftharpoons} Q, P \triangleleft (X)_Y / P \mid \equiv Q \mid \sim X$

Rule 2: the nonce-verification rule: $P \mid \equiv \#(X), P \mid \equiv Q \mid \sim X / P \mid \equiv Q \mid \equiv X$

Rule 3: the jurisdiction rule: $P \mid \equiv Q \mid \Rightarrow X, ,P \mid \equiv Q \mid \equiv X / P \mid \equiv X$

Rule 4: the freshness rule: $P \mid \equiv \#(X) / P \mid \equiv \#(X, Y)$

Using the above rules, we the following prove Theorem.

Theorem 1. *The proposed protocol provides secure mutual authentication between U_i and D_k in the presence of the GW.*

Proof. We define the following four goals:

Goal 1: $U_i \mid \equiv N_k \mid \equiv (U_i \overset{SK}{\longleftrightarrow} D_{k.})$

Goal 2: $U_i \mid \equiv (U_i \overset{SK}{\longleftrightarrow} D_k)$

Goal 3: $D_k \mid \equiv U_i \mid \equiv (U_i \overset{SK}{\longleftrightarrow} D_k)$

Goal 4: $D_k \mid \equiv (U_i \overset{SK}{\longleftrightarrow} D_k)$

The idealization form of the transmitted messages during the login and authentication phase under the proposed protocol is presented as follows:

$$\text{(M1)}\ U_i \overset{\text{via } D_k}{\longleftrightarrow} \text{GW}: \{ID_i, Tm_1, (U_i \overset{ID_i}{\leftrightarrow} D_K)\}_{X_{g_u}}$$

$$\text{(M2)}\ U_i \overset{via\ N_k}{\longleftrightarrow} GW: \{\ UD_K, UC_i, e_i, f_i, SID_i(U_i \overset{ID_i}{\leftrightarrow} D_K), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K\right)\}_{X_{g_u}}$$

$$\text{(M3)}\ D_k \longrightarrow GW: \{SID_i, TS_2, \text{Factor}_i, D_k \overset{SID_i}{\leftrightarrow} GW\}_{X_{g_{N_k}}}$$

$$\text{(M4)}\ D_k \longrightarrow GW: \{UD_K, UC_i, e_i, f_i, Tm_1, Tm_2, D_k \overset{r_i}{\leftrightarrow} GW, D_k \overset{SID_i}{\leftrightarrow} GW\}_{X_{g_{N_k}}}$$

$$\text{(M5)}\ GW \longrightarrow D: \{TS_3, (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)\ \}_{X_{g_{D_k}}}$$

$$\text{(M6)}\ GW \longrightarrow D: \{TS_3, TS_4, TS_5, SP_{ij}, (D_k \overset{X_{g_{N_k}}}{\leftrightarrow} GW), \left(D_k \overset{r_i^*}{\leftrightarrow} GW\right)\}_{X_{g_{D_k}}}$$

$$\text{(M7)}\ U_i \overset{\text{via } GW}{\leftrightarrow} D_k: \{TS_3, r_i^*, (D_k \overset{SID_i}{\leftrightarrow} GW), (D_k \overset{r_i^*}{\leftrightarrow} GW)\ \}_{X_{g_{D_k}}}$$

$$\text{(M8)}\ GW \overset{\text{via } D_k}{\leftrightarrow} U_i: \{TS_3, r_i^*, (U_i \overset{ID_i}{\leftrightarrow} GW), (U_i \overset{r_i^*}{\leftrightarrow} GW)\ \}_{X_{g_{N_k}}}$$

$$\text{(M9)}\ D_k \longrightarrow U_i: \{TS_3, Ts_4, Ts_5, ,Ts_6, V_i^*, \left(D_k \overset{SID_i}{\leftrightarrow} GW\right), r_i^*, \left(U_i \overset{K_l}{\leftrightarrow} G\right)\}_{SK}$$

We consider the following initial assumptions according to the proposed protocol description:

(H1) $GW \mid \equiv (U_i \overset{X_g}{\leftrightarrow} GW)$

(H2) $GW \mid \equiv \#(Ts_1)$

(H3) $GW \mid \equiv U_i \mid \Longrightarrow (U_i \overset{ID_i}{\leftrightarrow} GW)$

(H4) $GW \mid \equiv (U_i \overset{SID_i = h(ID_i \bigoplus R_i \oplus r_i)}{\leftrightarrow} GW)$

(H5) $GW \mid \equiv \#(r_i)$

(H6) $GW \mid \equiv U_i \mid \Longrightarrow (U_i \overset{r_i}{\leftrightarrow} GW)$

(H7) $GW \mid \equiv (U_i \overset{X_{g_u}}{\leftrightarrow} GW)$

(H8) $GW \mid \equiv \#(Ts_2)$

(H9) $GW \mid \equiv D_k \mid \Longrightarrow (D_k \overset{SID_i}{\leftrightarrow} GW)$

(H10) $GW \mid \equiv (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)$

(H11) $GW \mid \equiv \#(r_i^*)$

(H12) $GW \mid \equiv N_k \mid \Longrightarrow (D_k \overset{r_i^*}{\leftrightarrow} GW)$

(H13) $D_k \mid \equiv (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)$

(H14) $D_k \mid \equiv \#(Ts_3)$

(H15) $GW \mid \equiv D \mid \Longrightarrow (D_k \overset{X_g}{\leftrightarrow} GW)$

(H16) $D_k \mid \equiv \#(r_i^*)$

(H17) $D_k \mid \equiv GW \mid \Longrightarrow (D_k \overset{r_i^*}{\leftrightarrow} GW)$

(H18) $D_k \mid \equiv U_i \mid \Longrightarrow (D_k \overset{r_i^*}{\leftrightarrow} GW)$

(H19) $U_i \mid \equiv (U_i \overset{SID_i = h(ID_i \bigoplus R_i \oplus r_i)}{\leftrightarrow} GW)$

(H20) $U_i \mid \equiv \#(K_i)$

(H21) $U_i \mid \equiv GW \mid \Longrightarrow (U_i \overset{K_i}{\leftrightarrow} GW)$

(H22) $U_i \equiv \#(Tm_4)$

(H23) $U_i \mid \equiv D_k \mid \Longrightarrow (U_i \overset{K_i}{\leftrightarrow} GW)$

By analyzing the messages M1-M9 and assumptions H1-H23 based on the BAN logic rules, the goals (goal 1-goal 4) are provided as follows:

From M1, we get S1: $GW \triangleleft \langle ID_i, Tm_1, (U_i \overset{ID_i}{\leftrightarrow} D_K) \rangle_{X_g}$

Based on S1, H1, and rule 1, we get S2: $GW \mid \equiv \sim \langle ID_i, Tm_1, (U_i \overset{ID_i}{\leftrightarrow} \mathrm{D}) \rangle_{X_g}$

Based on H2 and rule 1, we get S3: $GW \mid \equiv \# \langle ID_i, Tm_1, (U_i \overset{ID_i}{\leftrightarrow} D_k) \rangle_{X_g}$

Based on S2, S3, and rule 2, we have S4: $GW | \equiv U_i | \equiv \langle ID_i, Tm_1, (U_i \overset{ID_i}{\leftrightarrow} D_K) \rangle_{X_g})$

Based on S4 and rule 5, we get S5: $GW \mid \equiv U_i \mid \equiv (U_i \overset{ID_i}{\leftrightarrow} \mathrm{GW})$

Based on S5, H3, and rule 3, we can get S6: $GW \mid \equiv (U_i \overset{ID_i}{\leftrightarrow} GW)$

From M2, we get

S7: $GW \triangleleft$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{ID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_u}}$$

Based on S7, H4, and rule 1, we get

S8: $GW \mid \equiv U_i \mid \sim$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{ID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_u}}$$

Based on H2, H5, and rule 4, we could get

S9: $GW \mid \equiv \#$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{ID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_u}}$$

Based on H2, H5, and rule 4, we have

S10: $GW \mid \equiv \#$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{ID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_u}}$$

Based on S5, S6, S10, and rule 5, we could get S12: $GW \mid \equiv U_i \mid \equiv (U_i \overset{r_i}{\leftrightarrow} \mathrm{GW})$

Based on S13, H7, and rule 1, we get

S14: $GW | \equiv N_k | \sim$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{ID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_{D_k}}}$$

Based on H7 and rule 4, we have

S15: $GW \mid \equiv \#$

$$\left\langle UD_K, UC_i, \mathrm{Factor}_i^*, e_i, f_i, SID_i \left(U_i \overset{MID_i}{\leftrightarrow} D_K \right), \left(U_i \overset{X_{g_u}}{\leftrightarrow} D_K \right) \right\rangle_{X_{g_{D_k}}}$$

Based on S14, S15, and rule 2, we get

S16: $GW \mid \equiv D_k \mid \equiv \langle SID_i, TS_2, \mathrm{Factor}_i, (N_{ki} \overset{MID_i}{\leftrightarrow} \mathrm{GW}) \rangle$

Based on S16 and rule 5, we have S17: $GW \mid \equiv D_k \mid \equiv (D_{ki} \overset{MID_i}{\leftrightarrow} \mathrm{GW})$

Based on S17, H9, and rule 3, we could get S18: $GW \mid \equiv (D_{ki} \overset{MID_i}{\leftrightarrow} \mathrm{GW})$

From Mssg4, we get

S19: $GW \triangleleft$

$$\left\langle UD_K, UC_i, e_i, f_i, Tm_1, Tm_2\, \mathrm{Factor}_i^*, \left(D_k \overset{r_\mathrm{i}}{\leftrightarrow} \mathrm{GW} \right), \left(D_k \overset{SID_\mathrm{i}}{\leftrightarrow} \mathrm{GW} \right) \right\rangle_{X_{g_{D_k}}}$$

Based on S19, H10, and rule 1, we get

S20: $GW \mid \equiv D_k \mid \sim \langle UD_K, UC_i, e_i, f_i, Tm_1, Tm_2,$

$$\left(D_k \overset{r_\mathrm{i}}{\leftrightarrow} \mathrm{GW} \right), \left(D_k \overset{SID_\mathrm{i}}{\leftrightarrow} \mathrm{GW} \right) \rangle_{X_{g_{D_k}}}$$

Based on H8, H11, rule 4, we have

S21: $GW\mid\equiv\#$

$$\left\langle UD_K, UC_i, e_i, f_i, Tm_1, Tm_2, \Big(D_k \overset{r_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big)\right\rangle_{X_{g_{D_k}}}$$

Based on S20, S21, and rule 2, we have

S22: $GW\mid\equiv D_k\mid\equiv$

$$\left\langle UD_K, UC_i, e_i, f_i, Tm_1, Tm_{2,}, \Big(D_k \overset{r_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big)\right\rangle_{X_{g_{D_k}}}$$

Based on S17, S18, S22, and rule 5, we could get S23: $GW\mid\equiv D_k\mid\equiv(D_k \overset{r_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW})$

Based on S23, H12, and rule 3, we get S24: $GW\mid\equiv(D_k \overset{r_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW})$

From Mssg5, we could get S25: $D_k\triangleleft\langle TS_3, (D_k \overset{X_{D_{N_k}}}{\leftrightarrow} GW)\rangle_{X_{g_{D_k}}}$

Based on S25, H13, and rule 1, we have

S26: $D_k\mid\equiv GW\mid\sim\langle TS_3, (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)\rangle_{X_{g_{D_k}}}$

Based on H14 and rule 4, we have S27: $D_k\mid\equiv\#\langle TS_3, (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)\rangle_{X_{g_{D_k}}}$

Based on S26, S27, and rule 2, we get S28: $D_k\mid\equiv GW\mid\equiv\langle TS_3, (D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)\rangle_{X_{g_{D_k}}}$

Based on S28 and rule 5, we could get S29: $D_k\mid\equiv GW\mid\equiv(D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)$

Based on S29, H15, and rule 3, we have S30: $D_k\mid\equiv(D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW)$

Based on S30, S31, H13, and Rule 1, we get

S32: $N_k\mid\equiv GW\mid\sim$

$$\left\langle Ts_1, Tm_2, Ts_3, SP_{ij}, \left(D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW\right), \left(D_k \overset{r_i^*}{\leftrightarrow} GW\right) \right\rangle_{X_{g_{D_k}}}$$

Based on H14, H16, and rule 4, we obtain the following:

S33: $D_k\mid\equiv\#$

$$\left\langle Ts_1, Ts_2, Ts_3, SP_{ij}, \left(D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW\right), \left(D_k \overset{r_i^*}{\leftrightarrow} GW\right) \right\rangle_{X_{g_{D_k}}}$$

Based on S32, S33, and rule 2, we have the following:

S34: $D_k\mid\equiv GW\mid\equiv$

$$\left\langle Ts_1, Ts_2, TS_3, SP_{ij}, \left(D_k \overset{X_{g_{D_k}}}{\leftrightarrow} GW\right), \left(D_k \overset{r_i^*}{\leftrightarrow} GW\right) \right\rangle_{X_{g_{D_k}}}$$

Based on S17, S18, and S34, we get S35: $D_k\mid\equiv GW\mid\equiv(D_k \overset{r_i^*}{\leftrightarrow} GW)$

Based on S35, H17, and rule 3, we get S36: $D_k\mid\equiv(D_k \overset{r_i^*}{\leftrightarrow} GW)$

From Mssg7, we get S37: $D_k\triangleleft$

$$\left\langle Ts_3, r_i^*, D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(D_k \overset{r_i^*}{\leftrightarrow} GW\Big)\right\rangle_{X_{g_{D_k}}}$$

Based on S37, H13, and rule 1, we get:

S38: $D_k\mid\equiv U_i\mid\sim$

$$\left\langle Ts_3, r_i^*, \Big(D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(D_k \overset{r_i^*}{\leftrightarrow} GW\Big)\right\rangle_{X_{g_{D_k}}}$$

Based on H14, H16, and rule 4, we get

S39: $D_k\mid\equiv\#\langle Ts_3, r_i^*, (D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}), (D_k \overset{r_i^*}{\leftrightarrow} GW)\rangle_{X_{g_{D_k}}}$

From S38, S39, and rule 2, we get

S40: $D_k\mid\equiv U_i\mid\equiv$

$$\left\langle Ts_3, r_i^*, \Big(D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(D_k \overset{r_i^*}{\leftrightarrow} GW\Big)\right\rangle_{X_{g_{D_k}}}$$

Based on S17, S18, S35, and rule 5, we get goal 4: $D_k\mid\equiv U_i\mid\equiv(U_i \overset{\mathrm{SK}}{\leftrightarrow} D_k)$

Based on S36, H18, goal 4, and rule 3, it will lead to the following:

Goal 3: $D_k\mid\equiv(U_i \overset{\mathrm{SK}}{\leftrightarrow} D_k)$

From Mssg8, we get S41: $U_i\triangleleft$

$$\left\langle Ts_3, r_i^*, \Big(U_i \overset{ID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), (U_i \overset{r_i^*}{\leftrightarrow} GW\right\rangle_{X_{g_{D_k}}}$$

Based on S41, H19, and rule 1, we get

S42: $U_i\mid\equiv GW\mid\sim$

$$\left\langle Ts_3, r_i^*, \Big(U_i \overset{ID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(U_i \overset{r_i^*}{\leftrightarrow} GW\right\rangle_{X_{g_{D_k}}}$$

Based on H20, and rule 4, we get S43: $U_i\mid\equiv\#$

$$\left\langle Ts_3, r_i^*, \Big(U_i \overset{ID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\Big), \Big(U_i \overset{r_i^*}{\leftrightarrow} GW\right\rangle_{X_{g_{D_k}}}$$

Based on S42, S43, and rule 2, we get

S44: $U_i \mid \equiv GW \mid \equiv \left\langle Ts_3, r_i^*, \left(U_i \overset{ID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}\right), \left(U_i \overset{r_i^*}{\leftrightarrow} GW\right) \right\rangle_{X_{g_{D_k}}}$

Based on S5, S6, S44, and rule 5, we have S45: $U_i \mid \equiv GW \mid \equiv (U_i \overset{r_i^*}{\leftrightarrow} GW)$

Based on S45, H21, and rule 3, we get S46: $U_i \mid \equiv (U_i \overset{r_i^*}{\leftrightarrow} GW)$

From Mssg9, we have

S47: $U_i \triangleleft \langle Ts_1, Ts_2, Ts_3, ,Ts_4, V_i^*, (N_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}), r_i^*, (U_i \overset{K_l}{\leftrightarrow} GW) \rangle_{SK}$

Based on S47, H9, and rule 1, we get

S48: $U_i \mid \equiv \sim \langle Ts_1, Ts_2, Ts_3, ,Ts_4, V_i^*, (D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}), r_i^*, (U_i \overset{K_l}{\leftrightarrow} GW) \rangle_{SK}$

Based on H20, H22, and rule 4, we get

S49: $U_i \mid \equiv \# \langle Ts_1, Ts_2, Ts_3, ,Ts_4, V_i^*, (D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}), r_i^*, (U_i \overset{K_l}{\leftrightarrow} GW) \rangle_{SK}$

From S48, S49, and rule 2, we have

S50: $U_i \mid \equiv N_k \mid \equiv \langle Ts_1, Ts_2, Ts_3, ,Ts_4, V_i^*, (D_k \overset{SID_{\mathrm{i}}}{\leftrightarrow} \mathrm{GW}), r_i^*, (U_i \overset{K_l}{\leftrightarrow} GW) \rangle_{SK}$

Based on S45, S50, and rule 5, we have

Goal 2: $U_i \mid \equiv N_k \mid \equiv (U_i \overset{SK}{\leftrightarrow} D_k)$

Finally, using S46, H23, goal 2, and rule 3, we obtain

Goal 1: $U_i \mid \equiv (U_i \overset{SK}{\leftrightarrow} D_k)$.

Hence, the goals 1 and 2 assure mutual authentication among $U_i$and N_k in presence of GW

5.2. Informal Security Analysis. In this section, we present an informal security analysis to prove that the proposed protocol is withstanding against various well-known malicious attacks. Besides, it provides the most security functionality requirement.

Proposition 2. *Resistance to the IoT sensor node capture attack.*

Proof. Assume that a malicious attacker MA attempts to compose the legal authentication request message $M_6 = \{ UC_i, UD_k, TS_3, TS_4 e_i, f_i \mathrm{Factor}_i^* \}$ or $M_7 = \{ V_i^*, TS_4, TS_6, cha \}$ of the IoT sensing node N_k and sent them to $U_i$or GW on behalf of N_k.For this motivation, MA tries to modify the exchanges message M_6 and M_7 to $M_6^i = (UC_i', UD_K', Factor_i^{*\prime}, e_i', f_i', TS_3', TS_4')$ and $M_7^i = (V_i^{*\prime}, TS_{4,}', TS_{6,}')$ by extracting the stored information. MA cannot obtain the value of MID_i as it is protected by a one-way hash function and the shared secret key Xg_{Nk}, which is only known to the IoT sensor node N_k. Also, MA cannot calculate V_i^* as it protected by a one-way hash with the random number M_i. Therefore, our proposed protocol resists node compromise attacks.

Proposition 3. *Resistance to impersonation attacks.*

Proof. In our proposed protocol, the attacker cannot extract or impersonate the level 3 feature extraction of the fingerprint of U_i. Moreover, if a malicious attacker attempts to adjust the parameter $UD_k = h(X_{g_u} \| TS_1 \| \mathrm{Factor}_i \bigoplus R_i)$ to a new one as UD_k', then the attacker will fail in the GW side due to a mismatch with UD_k calculated by the GW in the authentication phase with UD_k'. Therefore, the proposed protocol resists impersonation attacks.

Proposition 4. *Resistance to replay attacks.*

Proof. Assuming that a malicious attack aims to retransmit a message gained by eavesdropping on an efficient communication channel between the U_i and the D_k through the login and authentication phase, the attacker will fail, because our proposed protocol uses timestamps (TS_3, TS_4, TS_5, TS_6), and the delay time of the timestamp is brief. Our proposed scheme also uses Factor_i^* which is stored on the basis of level 3 feature extraction. Therefore, the proposed protocol provides an efficient security against replay attacks.

Proposition 5. *Resistance to stolen smart device attacks.*

Proof. In the case where the user's smart device is stolen or lost, the attacker aims to access the sensitive information stored in the device's memory using a power examination attack. Our proposed protocol provides efficient security against this kind of attack. The attacker cannot determine the identity ID_i and the password PW_i of the U_i since these are masked by a hash function on the basis of a random number R_i that is generated only once. Moreover, the attacker cannot identify the feature extraction FP_i given the hash function. Accordingly, our proposed protocol provides an efficient security against stolen smart device attacks.

Proposition 6. *Resistance to password change attacks.*

Proof. To change the user password, a malicious attack must use the personal fingerprint of a genuine U_i. Thus, the attacker cannot change the password. Assuming that a user's smart device is stolen or lost or is used by an attacker through another method, the attacker still cannot change the password, since this process requires the old password. Therefore, our proposed protocol resists password changes attacks.

Proposition 7. *Resistance to denial-of-service attacks.*

Proof. In our proposed scheme, this kind of attack is infeasible because the U_i receives an authorization message from the node D_k for security verification. Furthermore, we use timestamps TS_3, TS_4, TS_5, and TS_6 to mitigate any crucial request.

Proposition 8. *Resistance to parallel session attacks.*

Proof. If a malicious attack aims to build a parallel session of the scheme, then the attacker will fail even if he/she interrupts the communication message ($M_5 = \{\mathrm{Factor}_i^*, UD_k, UC_i, TS_3, e_i, f_i\}$) due to our utilization of level 3 feature extraction and the timestamp used in the login and authentication phases.

Proposition 9. *Resistance to gateway node bypass attacks.*

Proof. In this kind of attack, the attacker aims to impersonate the GW with the aim of later connecting to any IoT node D_k. Our proposed scheme can resist this type of attack because, as illustrated in Figure 4, the U_i initially sends the authenticated message Factor_i^*, UD_k, UC_i, TS_3, e_i, and f_i to the desired node D_k to initiate the authenticated phase. Subsequently, the node D_k returns this message to the GW (Figure 3.7). Then, GW verifies D_k and U_i. Accordingly, U_i, as the first step, uses any IoT facility that is disconnected from the GW. Therefore, the propose protocol provides an efficient security against gateway node bypass attacks.

Proposition 10. *Resistance to MITM attacks.*

Proof. As previously explained in Section 4, this type of attack aims to intercept communication between two legitimate parties and to modify, delete or delay messages. We suppose that a malicious attack intercepts the login message ($M_5 = \{Factor_i^*, UD_k, UC_i, TS_3, e_i, f_i\}$) transmitted from U_i to the node D_k and the authentication message ($M_6 = \{UC_i, UD_k, e_i, f_i, TS_3, TS_4, Factor_i^*\}$) that transmitted from the node D_k to GW. In this scenario, the attacker aims to modify the login message or authentication message to (M_5', M_6'). However, the attacker cannot predict the shared secret key needed to modify these messages. Moreover, each message communicated in the login and authentication phases has a timestamp with a short delay, thereby preventing an attacker from changing the messages. Therefore, our proposed scheme resists MITM attacks.

Proposition 11. *Resistance to Off-line Guessing Attacks.*

Proof. In our proposed scheme, a malicious attacker cannot gain an advantage by using off-line password-guessing attacks because the attacker cannot obtain the real passwords of a genuine U_i using the communication messages $M_5 = \{Factor_i^*, UD_k, UC_i, TS_3, e_i, f_i\}$ and $M_6 = \{UC_i, UD_k, e_i, f_i, TS_3, TS_4, \mathrm{Factor}_i^*\}$ in the login and authentication phases, respectively. Even if the user's smart device is stolen, the attacker cannot predict the password due to the nature of the hash function. Furthermore, the attacker cannot deduce the user fingerprint because the fingerprint is stored on the basis of a random number R_i, level 3 feature extraction that is generated only once, and the use of a strong hash function. If the adversary guesses PW_i', then, to legalize PW_i' with $b_i^* = \mathrm{b}_\mathrm{i}^{**}$? and $c_i^* = \mathrm{c}_\mathrm{i}^{**}$?, he/she needs to know U_i's identity as well as U_i's biometric B_i. Moreover, to guess PW_i, the adversary will need to guess ID_i and B_i along with the password. However, revealing of user biometric information or stealing it or forging it is not achievable; hence, the proposed protocol withstands offline-password-guessing attacks.

Proposition 12. *Provides key agreement.*

Proof. This feature indicates that the U_i and the IoT node D_k must agree on a secure session key to protect their successive communications. In our protocol, once D_k receives the authentication request ($M_7 = \{GP_{ij}, V_i, TS_5\}$) from the GW , it computes the session key $\mathrm{SK} = \mathrm{H}(\mathrm{R_i} \bigoplus \mathrm{M_i} \bigoplus \mathrm{Factor}_\mathrm{i}^*)$ on the basis of mask nonce M_i, R_i and Factor_i^*. Afterwards, D_k sends the message ($M_8 = \{V_i^*, TS_3, TS_4, TS_5, TS_6, cha\}$) to the U_i. Subsequently, U_i receives the authenticated message and then calculates the session key $SK = h(M_i^* \bigoplus R_i)$, and both session keys are equal as shown in Figure 3.6. Therefore, our proposed protocol supports a secure session key.

Proposition 13. *Provides user anonymity.*

Proof. Anonymity means protecting the information of a U_i from being tracked by an attacker. The user information, identity ID_i, password PW_i, and fingerprint FP_i are masked by a hash function. The fingerprint FP_i is calculated on the basis of the hash function of level 3 feature extraction. Accordingly, if a particular attacker attempts to interrupt the message exchange between the entities, then the attacker will fail to trace the user information.

Proposition 14. *Provides forward secrecy.*

Proof. In our protocol, we created the session key $SK = h(R_i \bigoplus M_i \bigoplus Factor_i^*)$ on the basis of the nonce number M_i which is generated once for each U_i who desires to log in to the (IoT) nodes. We also created the random number R_i and the $Factor_i$ which is not saved as a plaintext. Therefore, a malicious attack cannot obtain the session key by any way.

Proposition 15. *Provides mutual authentication.*

Proof. An authentication mechanism requires each entity in the IoT environment,, i.e. GW, the U_i and the IoT node D_k to validate each other. In our proposed protocol, after executing the necessary steps, $\mathrm{U_i}$ sends the authentication message ($M_5 = \{Factor_i^*, UD_k, UC_i, TS_3, e_i, f_i\}$) to D_k in the login phase (see Figure 3.7). Then, D_k send the authentication message ($M_6 = \{UC_i, UD_k, TS_3, TS_4, e_i, f_i, Factor_i^*\}$) to GW. Accordingly, the GW uses the authenticated message to validate the U_i and the node D_k. Therefore, the proposed protocol achieves mutual authentication.

Proposition 16. *Provides Key Freshness*

Proof. In our work, we generate a session key $SK = h(R_i \bigoplus M_i \bigoplus \mathrm{Factor}_i^*)$ that consists of fresh timestamps that are different in each session. Accordingly, our proposed protocol achieves key freshness. A security analysis of possible attacks against this model is presented below, and it is shown that our proposed protocol can resist several well-known attacks.

5.3. Formal Security Analysis Using the AVISPA Tool. AVISPA is a powerful automated validation tool which provides a wide applications range for constructing cryptographic protocols analysis models, verification, and validation. To validate the protocol using the AVISPA tool, firstly, the protocol is coded by using HLPSL language. Then, translate the HLPSL code in intermediate format (IF) by the HLPSL2IF translator. Finally, the IF specification as input is given to the back ends. After the IF execution, the back-end displays the result of the simulation of the protocol by analyzing to output format (OF), with an explanation of whether the protocol is safe or unsafe against man-in-the-middle and replay attacks. Also, back ends confirm the security features of the protocol such as the flexibility against most of the known attacks, authentication, and the secrecy of keys. Note that AVISPA performs the Dolev-Yao threat model [59, 60]. More details of the AVISPA tool and HLPSL can be found in [61].

To implement and simulate the proposed protocol on AVISPA, we have concentrated on the major tool SPAN Version 1.6 based on a computer system which is consist of Windows 10 Enterprise operating system (64 bit) that is supported by Ubuntu 10.10 light on Virtual machine, Intel (R) Core (TM) i7-7500U CPU @ 2.70 GHz 2.90 GHz processor, and 8 GB RAM. In AVISPA, there is a role for each entity, and these roles are independent of each other. AVISPA has an implementation in the form of four back ends, namely, TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols), OFMC (On-the-fly Model-Checker), CL-AtSe (Constraint Logic-based Attack Searcher), and SATMAC (SAT-based Model checker) [62]. We have evaluated the proposed protocol against man-in-the-middle and replay attacks under the OFMC and CL-AtSe back ends using SPAN.

The user registration, login, and authentication phases for the proposed protocol are implemented in HLPSL utilizing three basic roles for a remote user, the IoT sensor node, and the gateway node. The compulsory roles for the environment, session, and goal are also defined. Figure 5 provides the simulation results that obviously indicate that the proposed protocol is protected against man-in-the-middle and replay attacks.

6. Comparative Study

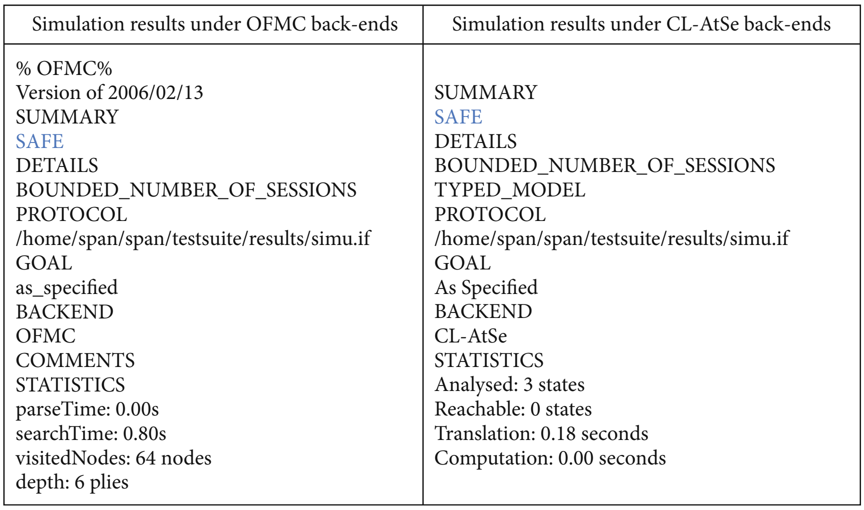
The proposed protocol is compared with the recent user authentication protocols proposed in the IoT environment such as the protocols of Banerjee et al. [1], Yang et al. [8], Dhillon and Kalra [33], Dammak et al. [45], Li et al. [50], and Farkoon et al. [60].

6.1. Security Functionality Comparisons. Table 3 summarizes the comparison of the functionality features of the recent user authentication protocols [1, 8, 33, 45, 50, 60]. It can be observed that the proposed protocol offers improved security and functionality features, in comparison to the other recent protocols.

6.2. Computation Overhead Comparison. In this section, we compare our proposed protocol in terms of computation overhead with those of recent related protocols [1, 8, 33, 45, 50, 60]. The protocol comprises four phases: user and sensor node registration phase, login phase, key agreement and authentication phase, and password and biometrics change phase. In the IoT WSN environment, the performance of the user authentication protocol mainly is affected by the login and authentication phase [2]. These two phases are the major part of the user authentication protocol and is what chiefly characterize it from the different user authentication protocols in IoT WSNs. Consequently, we focused our discussion of computation overheads during the login and authentication phase. The computational costs are the time consumed by the user and service provider in the process [9]. For computation overheads analysis, we utilized the notations T_h and T_m to indicate the time complexity of the hash function and elliptic curve cryptography (ECC) algorithm, respectively. The computational costs of the OXR operation are usually neglected because it requires a minimal number of computations.

In the login and authentication phase of our protocol, the remote user requires only $8T_h$ to calculate the parameters of a login and authentication request message. The IoT sensor node expends only $3T_h$ bits to verify the login request and to calculate the parameters of the key agreement message. As for the gateway node, it requires the gateway node which requires only $7T_h$ bits to verify whether the verification equations hold. Our proposed protocol uses only the XOR and one-way hash function operations to design simple user authentication and key agreement protocol. However, Li et al.'s protocol [50] provides authentication and key agreement protocol that is designed using an asymmetric encryption ECC algorithm. The time complexity of the asymmetric ECC encryption operation is greater than that of a one-way hash function. According to the practical example of the computational costs in an environment with a CPU of 3.2 GHz and with 3.0 GB of RAM, the time complexity of one-way hash operations requires 0.02 ms when using SHA-1 and for the ECC encryption operation which requires 0.45 ms when using ECC-160 [63]. Therefore, the total computational overheads of our protocol are 0.36 ms. Table 4 summarizes the computational overheads of our proposed protocol and the existing protocols in [1, 8, 33, 45, 50, 60] with approximate time (in milliseconds). It is clear that the proposed protocol requires less overall computation costs. The energy consumption of the IoT sensor node in our work is 0.06 ms which is 50%, 81.25%, 25%, 87.75%, 62.5%, and 95.8% lower than the computation times in the protocols of [1, 8, 33, 45, 50, 60].

Consequently, the total energy consumed of the IoT sensor node by our protocol is 0.36 ms. Therefore, our proposed protocol is more efficient and suitable for constrained sensor devices in the IoT WSNs environment. Table 4 presents the energy consumption of the IoT sensor node of our proposed protocol with those of [1, 8, 33, 45, 50, 60] along with total



Simulation results under OFMC back-ends

```
% OFMC%
Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/simu.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.80s
visitedNodes: 64 nodes
depth: 6 plies
```

Simulation results under CL-AtSe back-ends

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/simu.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed: 3 states
Reachable: 0 states
Translation: 0.18 seconds
Computation: 0.00 seconds
```

Figure 5: The simulation results under OFMC and CL-AtSe back ends.

Table 3: Functionality comparison of our protocol with other recent related protocols.

Properties	[1]	[8]	[33]	[45]	[50]	[60]	Our
User anonymity	✓	✗	✓	✗	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓	✓	✓
Key agreement	✗	—	✓	✓	✓	✗	✓
Resistance to impersonation attack	✓	✓	✗	✗	✗	✗	✓
Resistance to MITM attack	✓	✗	✓	✓	✗	✓	✓
Replay attack	✓	✓	✗	✓	✗	✓	✓
Resistance to password guessing attack	✓	✓	✓	✓	✓	✗	✓
Resistance to GW bypassing attack	✗	✓	✓	✗	✗	✗	✓
Resistance to parallel session attack	✗	✓	✓	✗	✗	✗	✓
Resistance to smart device stolen attack	✓	✗	✗	✗	✓	✓	✓
Resistance to DOS attack	✓	✓	✓	✓	✓	✗	✓
Resistance to insider attack	✓	✗	✓	✓	✗	✓	✓
Password change phase	✓	✓	✓	✓	✓	✓	✓
Forward secrecy	✓	✗	✗	✗	✗	✗	✓
Key freshness	✗	✓	✗	✓	✓	✗	✓
BAN logic security analysis	✓	✗	✗	✓	✓	✓	✓

Table 4: Computation overhead comparison.

Protocols	User	Sensor nodes	*GW* nodes	Total cost	Total estimation
[1]	$4T_h$	$24T_h$	$5T_h$	$33T_h$	0.66 ms
[8]	$16T_h$	$16T_h$	$20T_h$	$52T_h$	1.04 ms
[33]	$9T_h$	$6T_h$	$7T_h$	$22T_h$	0.44 ms
[45]	$20T_h$	$8T_h$	$20T_h$	$48T_h$	0.96 ms
[50]	$13T_h + 3T_m$	$4T_h + 2T_m$	$8T_h + T_m$	$24T_h + 6T_m$	3.18 ms
[60]	$13T_h$	$4T_h$	$13T_h$	$30T_h$	0.6 ms
Ours	$8T_h$	$3T_h$	$7T_h$	$18T_h$	0.36 ms

improvements of computational costs of the present protocols. From Table 5, it can be observed that the computational costs for the resource-limited IoT sensing device in our protocol is less in comparison to that of the recent existing protocols. The proposed protocol achieves superior performance because it consumes less energy compared to recent related protocols and is highly efficient. As the sensors nodes deployed in IoT networks have low battery life, low storage, and limited processing capability, the energy consumption of these IoT sensor nodes must be optimized. The IoT sensor nodes energy depends on two factors: the number of cryptographic operations to be performed and the amount of data being transmitted. Our proposed protocol minimized the number of cryptographic computations, therefore, more data can be transmitted via IoT sensor nodes. For the evaluation of the proposed protocol, the workload is not taken into consideration. In the future, the proposed protocol will be executed for different workloads in Cloud computing and IoT environments.

Table 5: Energy consumption of the IoT sensor node and improvement.

Protocols	Energy consumption of the IoT sensor node	Energy consumption improvement %	Protocol improvement %
[1]	0.48 ms	87.75	45.4
[8]	0.32 ms	81.25	65.3
[33]	0,12 ms	50	18.1
[45]	.016 ms	62.5	62.5
[50]	0.43 ms	95.8	88.67
[60]	0.08 ms	25	40
Ours	0.06 ms	—	—

6.3. Communication Overhead Comparison. For communication overhead computation, we assumed that the timestamp, hash digest (assuming SHA-1 hashing algorithm is applied), identity, a random nonce, and the secret key are 128 bits, while the ECC operations are 160 bits. There are four exchanges messages between U_i, N_k, and GW in proposed protocol that are $M_5 = \{MID_i, UD_k, UC_i, TS_3\}$, $M_6 = \{UC_i, UD_k, TS_4\}$, $M_7 = \{GP_{ij}, V_i, TS_5\}$, and $M_8 = \{V_i^*, TS_4, TS_6\}$, where MID_i, UD_k, UC_i, GP_{IJ}, and V_i are the hash function output. TS_3, TS_4, TS_5, and TS_6 are timestamps. According to our above assumption, each parameter is 128 bits. Therefore, the communication overhead of the proposed protocol is $128 \times 13 = 1664$ bits. Table 6 summarizes the communication overheads and the number of exchanged messages for all protocols in addition to the proposed protocol. We observe that the proposed protocol obtains less communication overhead as compared to the protocols in [1, 8, 33, 45, 50, 60] and incurs greater overhead than the protocol in [60]. Although the protocol [60] bears the less overhead but did not achieve the desired functionality and security features such as resistance to impersonation attacks, password guessing attacks, DOS attacks, preserved user anonymity, and forward secrecy in contrast to our protocol which achieved all functionality and security features (see Table 3).

Table 6: Communication overhead comparison.

Protocols	Communication in bits
[1]	2176
[8]	3840
[33]	3200
[45]	2560
[50]	1792
[60]	1408
Ours	1664

7. Conclusion

In this paper, we presented a secure and lightweight three-factor remote user authentication protocol designed for future IoT WSN application. The proposed protocol grants the legitimate remote user that mutually authenticates with the IoT sensor node through a trusted gateway node. The symmetric session key SK is established by the end of successful mutual authentication between the user and the IoT sensor node for future secure communications. The security of the proposed protocol is formally using the popular widely accepted BAN logic. Furthermore, informal security verification demonstrates that the proposed protocol resists the most well-known attacks. The formal security using the AVISPA simulation is evaluated, and the results showed that our protocol is safe. Finally, the performance analysis comparison in terms of computation and communication overheads demonstrated that our protocol showed high efficiency and performance compared to those of recent related protocols and is more suitable for practical IoT WSN environments.

Data Availability

All data are available within the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Banerjee, V. Odelu, A. K. Das et al., "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.

[2] A. Alkhayyat and M. S. Mahmoud, "Novel cooperative mac aware network coding under log-normal shadowing channel model in wireless body area network," *International Journal on Communications Antenna and Propagation (IRECAP)*, vol. 9, no. 3, pp. 198–206, 2019.

[3] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.

[4] 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," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[5] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, no. 1, 2020.

[6] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, 2020.

[7] S. Challa, M. Wazid, A. K. Das et al., "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, no. 1, pp. 3028–3043, 2017.

[8] Z. Yang, J. Lai, Y. Sun, and J. Zhou, "A novel authenticated key agreement protocol with dynamic credential for wsns," *ACM Transactions on Sensor Networks*, vol. 15, no. 2, pp. 1–27, 2019.

[9] C. T. Chen, C. C. Lee, and I. C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *PLOS ONE*, vol. 15, no. 4, article e0232277, 2020.

[10] D. Abdulmohsin Hammood, H. A. Rahim, A. Alkhayyat, and R. B. Ahmad, "Body-to-body cooperation in Internet of Medical Things: toward energy efficiency improvement," *Future Internet*, vol. 11, no. 11, 2019.

[11] M. Teymourzadeh, R. Vahed, S. Alibeygi, and N. Dastanpour, "Security in wireless sensor networks: issues and challenges," 2020, https://arxiv.org/abs/2007.05111.

[12] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474–3484, 2020.

[13] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996–8004, 2018.

[14] A. Alkhayyat, A. A. Thabit, F. A. Al-Mayali, and Q. H. Abbasi, "WBSN in IoT health-based application: toward delay and energy consumption minimization," *Journal of Sensors*, vol. 2019, 2019.

[15] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for internet of things," *Future Generation Computer Systems*, vol. 89, pp. 110–125, 2018.

[16] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for internet of things environments," *Journal of Information Security and Applications*, vol. 52, article 102494, 2020.

[17] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Computer Networks*, vol. 148, pp. 196–213, 2019.

[18] D. Minoli, S. Kazem, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 269–283, 2017.

[19] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 47–53, 2016.

[20] M. Kamruzzaman, N. I. Sarkar, J. Gutierrez, and S. K. Ray, "A study of IoT-based post-disaster management," in *2017 International Conference on Information Networking (ICOIN)*, pp. 406–410, Da Nang, Vietnam, 2017.

[21] A. A. Thabit, M. S. Mahmoud, A. Alkhayyat, and Q. H. Abbasi, "Energy harvesting Internet of Things health-based paradigm: towards outage probability reduction through inter–wireless body area network cooperation," *International Journal of Distributed Sensor Networks*, vol. 15, no. 10, 2019.

[22] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks*, vol. 9, Article ID 730831, 2013.

[23] P. Kumar, S. Lee, and H. Lee, "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, pp. 1625–1647, 2012.

[24] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Security and Communication Networks*, vol. 9, 2655 pages, 2015.

[25] P. Gope and T. Hwang, "BSN-care: a secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[26] L. Wang, "Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography," *Journal of Applied Mathematics*, vol. 2014, Article ID 247836, 11 pages, 2014.

[27] V. Odelu, A. K. Das, and A. Goswami, "An efficient ECC-based privacypreserving client authentication protocol with key agreement using smart card," *Journal of Information Security and Applications*, vol. 2, no. 1, pp. 1–19, 2015.

[28] M. Turkanovic, 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 Networks*, vol. 20, pp. 96–112, 2014.

[29] M. S. Farash, M. Turkanovic, S. Kumaric, 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 Networks*, vol. 36, pp. 152–176, 2016.

[30] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, "An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 13, p. 2092, 2016.

[31] S. Arasteh, S. F. Aghili, and H. Mala, "A new lightweight authentication and key agreement protocol for internet of things," in *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pp. 52–59, Tehran, Iran, September 2016.

[32] R. Amin, S. 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," *Computer Networks*, vol. 101, pp. 42–62, 2016.

[33] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," *International Journal of Communication Systems*, vol. 30, no. 16, article e3323, 2017.

[34] J. Li, Y. Ding, Z. Xiong, and S. Liu, "An improved two-factor mutual authentication scheme with key agreement in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 11, 2017.

[35] W. Zhang, D. Lin, H. Zhang, C. Chen, and X. Zhou, “A lightweight anonymous mutual authentication with key agreement protocol on ECC,” in *2017 IEEE Trustcom/BigDataSE/ICESS*, p. 170176, August 2017.

[36] 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,” vol. 14, no. 1, 2018.

[37] Y. F. Lu, C. F. Kuo, H. M. Chen, G. B. Wang, and S. C. Chou, “A mutual authentication scheme with user anonymity for cyber-physical and internet of things,” in *Proceedings of the 2018 Conference on Research in Adaptive and Convergent Systems - RACS '18*, pp. 88–93, October 2018.

[38] G. Xu, S. Qiu, H. Ahmad et al., “A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography,” *Sensors*, vol. 18, no. 7, article 2394, 2018.

[39] J. Ryu, H. Lee, H. Kim, and D. Won, “Secure and efficient three-factor protocol for wireless sensor networks,” *Sensors*, vol. 18, no. 12, article 4481, 2018.

[40] 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 of Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[41] Y. Chen, Y. Ge, W. Wang, and F. Yang, “A biometric-based user authentication and key agreement scheme for heterogeneous wireless sensor networks,” *KSII Transactions on Internet and Information Systems*, vol. 12, no. 4, 2018.

[42] C. C. Chang and H. D. Le, “A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.

[43] J. Srinivas, S. Mukhopadhyay, and D. Mishra, “A self-verifiable password based authentication scheme for multi-server architecture using smart card,” *Wireless Personal Communications*, vol. 96, no. 4, pp. 6273–6297, 2017.

[44] F. Wu, L. Xu, S. Kumari, and X. Li, “An improved and provably secure three-factor user authentication scheme for wireless sensor networks,” *Peer-to-Peer Networking and Applications*, vol. 11, pp. 1–20, 2018.

[45] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, “Token-based lightweight authentication to secure IoT networks,” in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–4, Las Vegas, NV, USA, 2019.

[46] A. Gupta, M. Tripathi, T. J. Shaikh, and A. J. C. N. Sharma, “A lightweight anonymous user authentication and key establishment scheme for wearable devices,” *Computer Networks*, vol. 149, pp. 29–42, 2019.

[47] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. J. I. A. Liu, “Remotely access “My” smart home in private: an anti-tracking authentication and key agreement scheme,” *IEEE Access*, vol. 7, pp. 41835–41851, 2019.

[48] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, “An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks,” *IEEE Internet of Things Journal*, 2019.

[49] K. Renuka, S. Kumari, D. Zhao, and L. J. I. A. 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.

[50] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, “A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems,” *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2019.

[51] A. A. Yassin, H. Jin, A. Ibrahim, and D. Zou, “Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing,” in *2012 Second International Conference on Cloud and Green Computing*, pp. 282–289, Xiangtan, China, 2012.

[52] P. K. Dhillon and S. Kalra, “Multi-factor user authentication scheme for IoT-based healthcare services,” *Journal of Reliable Intelligent Environments*, vol. 4, no. 3, pp. 141–160, 2018.

[53] X. Niu and Y. Jiao, “An overview of perceptual hashing,” *Acta Electronica Sinica*, vol. 36, no. 7, pp. 1405–1411, 2008.

[54] B. H. Taher, S. Jiang, A. A. Yassin, and H. Lu, “Low-overhead remote user authentication protocol for IoT based on a fuzzy extractor and feature extraction,” *IEEE Access*, vol. 7, pp. 148950–148966, 2019.

[55] Z. Jie, “A novel block-DCT and PCA based image perceptual hashing algorithm,” 2013, https://arxiv.org/abs/1306.4079.

[56] L. Kotoulas and I. Andreadis, “Colour histogram content-based image retrieval and hardware implementation,” *IEE Proceedings - Circuits, Devices and Systems*, vol. 150, no. 5, pp. 387–393, 2003.

[57] M. Wazid, A. K. Das, S. Shetty, J. P. C. Rodrigues, and Y. Park, “LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment,” *Sensors*, vol. 19, no. 24, p. 5539, 2019.

[58] M. Burrows, M. Abadi, and R. M. Needham, “A logic of authentication,” *Proceedings of the Royal Society of London A*, vol. 426, no. 1871, pp. 233–271, 1989.

[59] D. Dolev and A. C. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[60] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, “Secure remote anonymous user authentication scheme for smart home environment,” *Internet of Things*, vol. 9, article 100158, 2020.

[61] AVISPA, “Automated validation of internet security protocols and applications,” March 2018, http://www.avispa-project.org/.

[62] W. Bae and J. Kwak, “Smart card-based secure authentication protocol in multi-server IoT environment,” *Multimedia Tools and Applications*, vol. 79, no. 23-24, pp. 15793–15811, 2020.

[63] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 36, pp. 316–323, 2013.