1. Alumuru Mahesh Reddy[1], 2.Dr.M.Kameswara Rao[2]

Koneru Lakshmaiah Education Foundation (1,2)

doi:10.15199/48.2023.10.30

An Efficient Key Management and Authentication Protocol for IoT Networks

Abstract. *The increasing integration of IoT technology into our daily lives through applications, it is critical to assure these systems security and privacy problems. Furthermore, time-critical IoT applications in healthcare necessary access to real-time private information from third parties (users) via wireless communication devices As a consequence; user identity concerns have to be handled in IoT wireless sensor system networks. (WSNs). In this paper, a secure and compact three-factor identification technique for future IoT WSN applications that relies on user biometric feature extraction. The method that was proposed depends on hash and XOR functions, and it includes (i) three-factor authentication; (ii) a shared session key; (iii) mutual authentication; and (iv) key freshness. The simulation tool here using is AVISPA for Rapid Verification of Internet Security Protocols and an informal security research that confirms its other qualities. Furthermore, our calculations show suggested method outperforms existing similar authentication methods with respect to of safety and usefulness, as well as communications and computing costs. Furthermore, the proposed protocol is suitable for usage in the vast majority of IoT and WSN applications*

Streszczenie. *Rosnąca integracja technologii IoT z naszym codziennym życiem za pośrednictwem aplikacji sprawia, że zapewnienie bezpieczeństwa tych systemów i problemów związanych z prywatnością ma kluczowe znaczenie. Ponadto krytyczne czasowo aplikacje IoT w opiece zdrowotnej wymagają dostępu do prywatnych informacji w czasie rzeczywistym od stron trzecich (użytkowników) za pośrednictwem bezprzewodowych urządzeń komunikacyjnych. kwestie związane z tożsamością użytkownika muszą być rozwiązywane w sieciach bezprzewodowych systemów czujników IoT. (WSN). W tym artykule omówiono bezpieczną i kompaktową technikę trójczynnikowej identyfikacji dla przyszłych aplikacji IoT WSN, która opiera się na ekstrakcji cech biometrycznych użytkownika. Zaproponowana metoda opiera się na funkcjach haszujących i XOR oraz obejmuje (i) uwierzytelnianie trójskładnikowe; (ii) wspólny klucz sesyjny; (iii) wzajemne uwierzytelnianie; oraz (iv) kluczowa świeżość. Narzędziem symulacyjnym, którego tutaj używamy, jest AVISPA do szybkiej weryfikacji protokołów bezpieczeństwa internetowego oraz nieformalne badanie bezpieczeństwa, które potwierdza jego inne cechy. Co więcej, nasze obliczenia pokazują, że sugerowana metoda przewyższa istniejące podobne metody uwierzytelniania pod względem bezpieczeństwa i użyteczności, a także kosztów komunikacji i obliczeń. Ponadto proponowany protokół nadaje się do wykorzystania w zdecydowanej większości aplikacji IoT i WSN. (**Wydajny protokół zarządzania kluczami i uwierzytelniania dla sieci IoT**)*

Keywords: Internet of Things (IoT), AVISPA, RFID, Wireless Sensor Networks (WSN), Mutual Authentication.
Słowa kluczowe: ToT, besprzewodowa sieć czujników

Introduction

The Internet of Things has been popular recently and is probably going to keep doing so [1]. Prior to being delivered to other intermediate device, IoT device, or the cloud via the Internet IoT monitoring devices such as embedded devices, RFID, wearable's, and low wattage IEEE 802.15.4 devices perceive or gather information. Many gadgets in IoT can communicate with one another over the Internet. Many IoT applications, such as healthcare systems, industries, transportation, and households, have already been deployed [2]. WSNs are quite crucial in various IoT applications. Because they are inexpensive, simplicity of deployment, and flexibility, WSNs have seen a significant surge in their use in delivering services to activities and monitoring settings [3]. Because of this, security and privacy are significant obstacles in the application of consumer technologies [4]. Take the IoT healthcare application. Giving a doctor rapid access to data gathered by In this case, healthcare sensor nodes implanted in his patient's physique can improve the excellent medical care. Current vital indicators like BP, cholesterol, C-reactive protein, and Glucose level may be included in this data. As a consequence of this confidential and personal latest data, a choice on the patient's health state can be made to give essential corrective steps. Sensor nodes/devices in WSN present a serious security concern in IoT. Typically, the sensor nodes are placed in areas where people may easily touch them crack [5]. Furthermore, given that the harmful attacker may have obtained the incident compromised all important verification data, fresh remote user authentication may be exposed to this attack. As a result, security issues are increasingly present in IoT WSN applications. The presented a safe and In an IoT WSN utilization context, a lightweight distant user authorization and key management method is used to achieve this aim.

1.1. Motivation

The Internet of Things WSN has created several opportunities in various fields, which have eased procedures for consumers and companies. This broad and quick expansion has resulted in significant issues that necessitate the creation of more security methods with the goal to support applications for the IoT protect users' privacy data. Security is perhaps the most pressing issue confronting the IoT WSN ecosystem. Information from IoT sensor nodes can be accessed remotely via the Internet by remote users in an IoT WSN. Researchers have created viable ways for integrating wireless networks into IoT contexts [6]. Sensor nodes are intrinsically resource-constrained devices because to their small size and limited energy [7]. They have limited processing capabilities, restricted communication bandwidth, and very low storage capacity. As a result, developing a safe and it is challenging to develop an effective remote user authentication mechanism for IoT WSN situations.

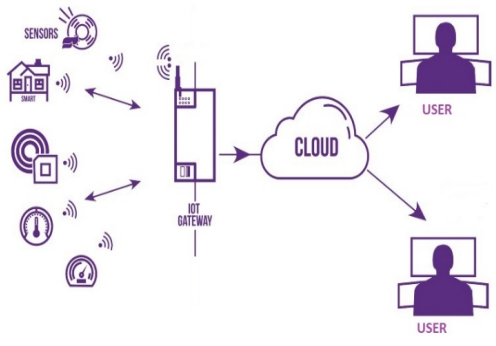

Fig 1: IoT Secure gateway Authentication

The security effectiveness of remote user authentication is a critical problem in IoT systems for securely delivering information [8]. User or device authentication is a crucial problem that needs to be dealt with in terms of security for the IoT. The majority conventional authentication mechanisms rely on either a secret key or a smart chip, or both. Because intruders have exploited these protocols, they are presently worthless changed their attack approach on IoT devices.

1.2. The Attack Model

To use majorly established and more realistic Dolev-Yao threat (DY) protocol in our suggested approach [9]. Communication between two entities is achieved under this architecture via a public channel. In addition, an opponent MA will possess total command of the communication path. As a result, MA has the ability to modify, listen in on, inject, and delete false communications exchanged during contact.

1.3. Involvement and proposal's primary contributions arise:

(1) To provide a compact and secure procedure for distant identification for users, IoT WSN applications through unique biometric extraction of features and a hash function with a single way that is suited for usage in wireless healthcare applications. To achieve our aim, the suggested protocol has three components: user password, smartphone, and biometrics. The employed biometrics to strengthen the protocol's security since fingerprints is difficult to steal, or forget.
(2) In existing authentication techniques, distortion in fingerprint images is dealt with using the third level of extracted features.
(3) To demonstrate a protocol with security utilizing the random oracle approach, assessment of security is both informal and formal.
(4) To use simulation to test the suggested procedure AVISPA, a well-liked and well acknowledged resource and demonstrate it's entirely secure from both direct and indirect assaults.
(5) A comparison of this model to comparable communicating through protocols and computing overheads was carried out.

2. Relevant Work

In addition, developed approach should incorporate a password/biometric update phase and decrease computation and transmission costs. Assume a A healthcare professional is investigating medical IoT ecosystem. In an assumption, must protect specific data about this user, for maintaining anonymity to protect from other users disclosing the patient's vital private knowledge as he or she participates in system sessions. To clarify, user anonymity is one of the major elements of the user authentication protocol [10]. Also, in IoT WSN applications, un-traceability is vital to preventing an individual's tracking by an intruder throughout a session [11]. After modernization, WSNs have expanded a significant and required infrastructure for networks, and they may be employed in several current domains [12]. Many user authentication methods have been put forth to meet the safety needs of IoT WSN context. A novel user-authentication mechanism for WSNs based on ECC [13]. Unfortunately, due to the relatively large storage and processing cost, it is inapplicable for healthcare application systems [14]. As explained in, real-time users typically employ very easy-to-remember settings for their ease of use, such private identification and keys; hence, user anonymity is not offered. Lightweight remote user authentication approaches were provided in research [15] to improve the security of IoT WSNs. Nonetheless, these contributions require enhancements in order to withstand assaults while maintaining optimal communication and computing speed. Suggested an verification strategy for an IoT network that attempted to address the shortcomings [16] suggested a lightweight 3FA system in 2017 that used a user password, biometrics, and a smart device. It emphasized that technique is resistant to familiar assaults such as DOS, impersonation, offline password guessing, and stolen smart device attacks. Although, system is till now vulnerable to aforementioned attacks and lacks a session key agreement. In the same year [17] introduced key agreement authentication techniques.
They demonstrated that their system was light and suitable for restricted IoT situations. Several research on remote user authentication for the IoT context were released in 2018. The author of [18] provided an verification strategy for ad-hoc WSN utilizing ECC cryptograph to improve the security flaw of the scheme. Provided a mutual authentication suggested technique with user anonymity in Cyber-Physical Systems and IoT. [19] Demonstrated that Srinivas et.al's authentication techniques are sensitive to a variety of attacks and do not provide user anonymity. Furthermore [20] approach and concluded that Wu et al. scheme's had two security flaws against outsider attackers. A novel user authentication strategy for an IoT network depends on hierarchy. These researchers discovered that their system had less processing, and discussion expenses. Furthermore, [21] introduced a fuzzy extractor-based authentication technique. Nonetheless, Chen's method has a high overhead, has published works on this topic in 2019. However, both approaches have flaws, notably considering the costs of calculating and communicating, which are significantly higher than our suggested scheme. Generally speaking, remote authentication for users methods either fall short of the security needs of the IoT WSN environment or lacks safety features such as variable anonymity and un-traceability, as well as biometric and password change processes

3. Fundamental Preliminaries

It will go through the characteristics of the perceptual hashing, level 3 feature, and one-way hash function extractions in this section.
(i) Fingerprint level 3 feature extractions: The arrangement of on the outdoors of the fingertip, with mountains and slopes is known as a fingerprint that is unique to each individual. The first level of fingerprint identification contains specifics like the type of design and ridge-line flow; the second level comprises minor spots for immediate spurs, terminations, and bifurcations. The third stage possesses all of the dimension characteristics of a ridge, including immediate sweat pores, edge, and crispiness.
As a result, our suggested the method employs this third step since it is distinct and immutable and eternal [22] has further information.
(ii) The one-way hashing function is a mathematics function that is commonly utilized in a wide range of apps, including assessing data integrity during transmission, establishing message authentication codes, and conducting digital forensic investigations. Cryptographic 1HF is particularly delicate enough to modest input changes. Because the 1HF is impossible to reverse, obtaining the actual text from a hash value is challenging. It generates hash values of at least 128 bits. 1FH is frequently used in the generation of digital signatures that are used to determine identity of the person who sent those [23].
(iii) Traditional encrypting and hashing methods the biometric template can't be encrypted using this method.

when using biometrics for user authentication. Biometric data, like fingerprints and voice, change with time in various contexts. As a result, hashing or encryption techniques are unable to be applied to encryption the biometric template while developing a biometric user authentication system. Researchers proposed perceptual hashing (p-hash) to overcome this problem [24].

The advantage of utilizing p-hash is that it can embrace small changes in source excellence and arrangement. The hash number produced via perceptual hashing ranges in size from 64 to 128 bits. The employed the perceptual hashing function published in a previous work by Jie [25] in this article.

The authors of [26] create a perceptual feature by blending image blocks with a low-frequency DCT coefficients and the color histogram, which is then reduced as an intertexture using PCA and cutoff to create an effective hash.

4. The Protocol Proposal

Using the network model scenario depicted in Figure 1, For IoT Secure gateway Authentication, we offer an effective and reliable authentication for user's mechanism. in this section. The further emphasized that the suggested protocol is intended to be general enough to be applicable to the majority of IoT WSN applications that require user authentication.

Table 1 show representations utilized symbols used in this analysis. To use current timestamps in our work to ensure the adaptability to replay assaults. To use current timestamps in our work to ensure the adaptability to replay assaults.

As a result, the clocks of many method objects are anticipated and synchronized, which is a widely held assumption in the literature [27]. Our verification method, which is based on three factors: a password, a user's biometric, and a mobile device, emphasizes In addition to lower expenses to IoT nodes, the user. A smart device, like a mobile phone, may be used to easy to access IoT nodes and the benefits that they provide. The proposed protocol has three participants: a distant user (U) whose goal is to optimize the environment's services, collection sensor nodes for the Internet of Things (SN), and a reliable residential gateway (GW). Registration, pre-computation, credentials modification, key acceptance, and verification are the four stages of our job. The registration phase was completed, whereas pre-computation, verification, and password modification phases are conducted anytime a remote user logs in or changes his or her password. The suggested method makes it simple for remote users to modify their passwords and/or biometric data using their smartphone without contacting GW.

Table 1: The representations utilized.

Symbols	Explanation
S_{key}	Session key
$\oplus$	XOR Function
U	User
ID_u	ID of user
SK_g	Secret key of Gateway
SK_{gu}	Secret Key of user
TS_1, TS_2, TS_3, TS_4, T	Time stamps
SN	IoT Sensor nodes
X_k	Secret key by SN node
$r1,r2$	Random numbers generated by user
P_i	Users Password
F_p	User's fingerprint Biometric
H (.)	Hash function
F_x	Features of Biometric data

Phase 4.1: Remote User Registration On the user's end: This time, every U wishing to use IoT assets need to be registered using GW. U performs below actions to complete the registration:

(Step i) The user (U) chooses its identification (ID_u) and password (P_i). U enters his or her fingerprint (F_p)

(Step ii) U calculates biometric stage three extracting of features as below: $FF_x = FXT(F_p)$

(Step iii) U chooses an unplanned number. $r_1,r_2 \in Z_n^+$ and generates a unique identity conceal for the person using it, password, as well as the following fingerprint: mask of identity: $UID_U = H(ID_u \oplus r_1)$, password mask: $UP_i = H(P_i \oplus r_1)$, as well as a fingerprint barrier: $UF_i = H(F_X)$

(Step iv) The U forwards UID_u, UP_i, UF_i, and FF_x to the GW as a communication request to the GW node with a secure connection

When the GW receives a request message from the U, it follows the steps below.

(Step i) Confidential keys are generated by GW such as SK_g, SK_{gu}.GW then calculates the protection settings $p_i = h(UID_u \oplus SK_g)$, $q_i = h(UP_I \oplus SK_{gu})$, and $r_i = H(FF_X \oplus SK_{gu})$, prior to use

(Step ii) GW calculates Nonce = $\Sigma^{L}_{i=1}ASCII(F_xF_{pi})$,$ue_i = p^{fi}_i \oplus SK_{gu}$, and $uf_i = q^{fi}_i \oplus SK_{gu}$

(Step iii) The GW node makes a submission $msg1 = UID_u$, ue_i, f_i, SK_{gu}, and UF_i to U. On receiving msg1, U stores it in the device's memory. Figure 3 summarizes the several processing procedures that took place at this phase

4.2. The enrollment process of IoT Sensor Nodes: At this level, each IoT sensor node serves as a register. More nodes can be connected globally at this point, which includes the below steps, IoT node side:

(Step i) SN produces an unique numbers. $R_k \in Z_n^+$. SN the common secret is well known SK_{gSN} It has an own identification inside the GW, ID_{SN}*

(Step ii) SN calculates the parameters $UP_J = h(SK_{gSN} \| Rk \| ID_{SN}^*)$ & $MSN = RSN \oplus SK_{gSN} \oplus Nonce_i$ for future evaluation purposes

(Step iii) SN forwards UP_J, MSN, ID_{SN}*, & TS_1 to the GW using a safe route

The GW node performs the next steps after receiving an enrolment demand from the IoT sensor nodes SN.

(Step i) Evaluates the timelines condition $|TS1 - T| < \triangle T$. If the requirement is not met, the registration phase is ended; alternatively, the GW moves on to the next stage.

(Step ii) Evaluates $r_k' = MSN \oplus SK_{gSN} \oplus Nonce_i$, and UP_J' based on the prior communication received from U as $UP_J' = h(SK_{gSN} \| r_k' \| ID_{SN}^*)$

(Step iii) Verifies whether $UP_J = UP_J'$ or not. As a result, if the parameters aren't dissimilar, the node is no, the session is terminated since it is illegitimate, according to the GW. Otherwise, GW proceeds to the next stage.

(Step iv) Calculates the necessary attributes for future usage, $a_j = h(ID_{SN}^* \| X_g)$, $b_j = h(UP_J \| SK_{gDSN} \| Nonce_i)$, and the $r_j = p_j \oplus q_j$

(Step v) Then, GW sends p_j, q_j, and TS_2 to SN. Upon receiving the registration messages (a_j, c_j, and TS_2) from the GW, SN checks the timelines condition $|TS2 - T| < \triangle T$ To check for any outside influences. The time period was terminated if the condition is not satisfied. Otherwise, SN records the parameters p_j, q_j, and TS_2 into the gadget's storage. Finally, the step of user registration is completed. The processes of the IoT sensor node registration phase are depicted in Figure 3.

4.3. Login and Pre-computation Phase After successfully completing the registration step, during the authentication step, An authenticated user interface can get accessibility to every sensor node in the IoT network. To initiate the authentication stage, U must verify login to chosen IoT

service application by utilizing login methods created during this phase.

(Step i) First and foremost, the user U opens applications on their own mobile and inputs PW_i extraction of passwords and third-level features F_x F_{Pi} kept on the mobile device.

(Step ii) The U mobile devices then computes a disguised pin and extracts features in the following manner: $UP_I' = h(UPW_I \oplus r_i)$ and $UF_i' = h(UF_i \oplus r_i)$. Also, it computes $b_i^{**} = h(p_i^{Noncei} \oplus ue_i \oplus UPW_I \oplus SK_{gn})$ and $r_i^{**} = h(UF_i \oplus q_i^{Nonce\ i} \oplus Nonce_i)$

(Step iii) Following that, the first q_i and r_i gather results are listed below: $q_i^* = h(UP_I \oplus SK_{gu})$ and $r_i^* = h(UF_i \oplus SK_{gu})$

(Step iv) U calculates the values of the validation specifications listed below q_i^{**} and r_i^{**}, $q_i^{**} = h(pi^{Nonce\ i} \oplus ue_i \oplus UP_I \oplus SK_{gn})$ and $r_i^{**} = (uf_i \oplus q_i^{Nonce\ i} \oplus Nonce_i)$

(Step v) Then, the precision of q_i^* and r_i^* is validated by b_i^{**} and c_i^{**}. If $q_i^* = q_i^{**}$? & $r_i^* = r_i^{**}$? The process of logging in then advances to further stage. Alternatively, the action will be cancelled since the user has not been authorized and has given inaccurate information.

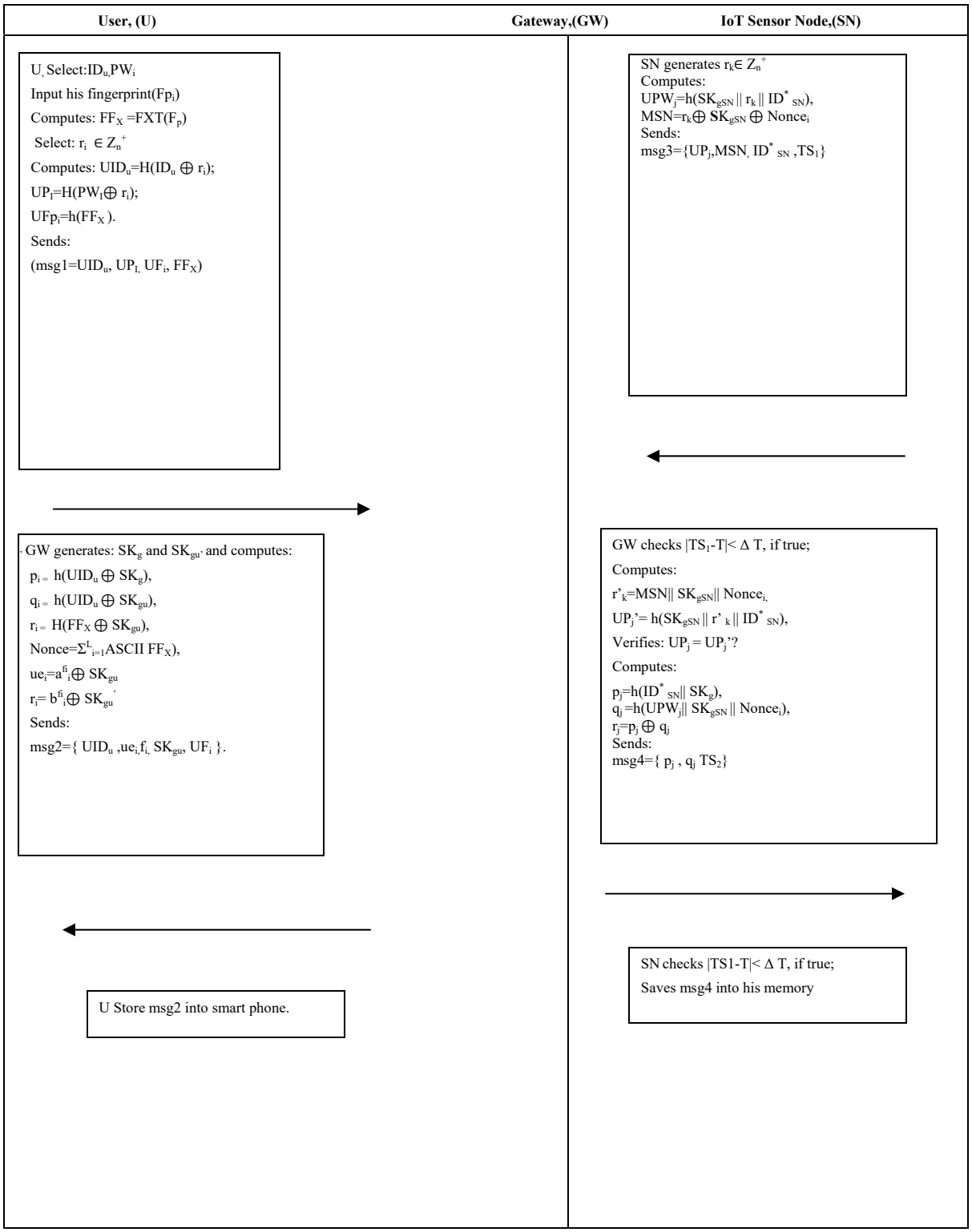

Fig 2: The user registration process.

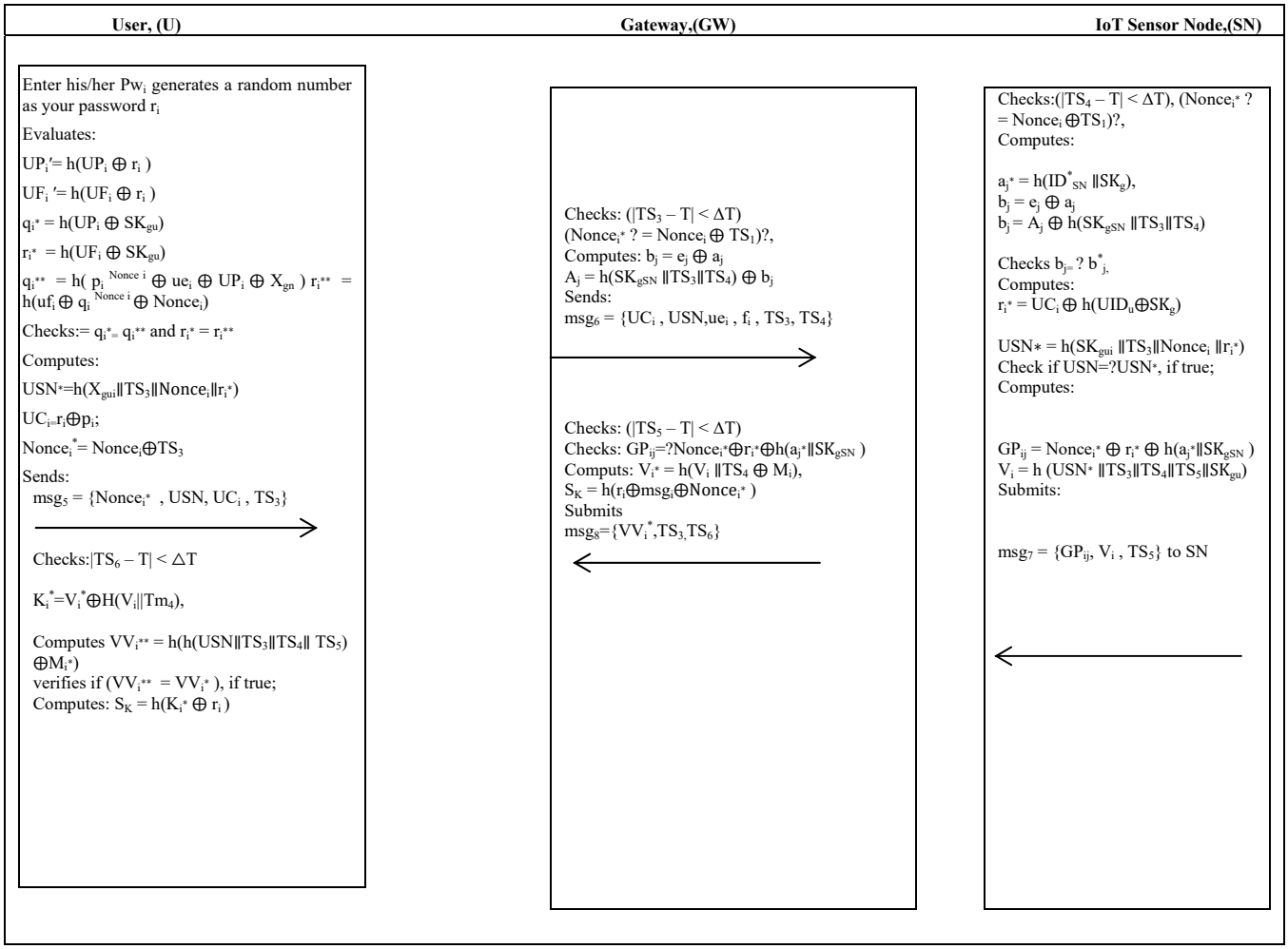

Fig 3: login and authentication phases

(Step vi) When the user authentication succeeds, the following privacy settings are calculated: USN = h(SK_{gu} ‖TS_1‖ $Nonce_i$ r_i) and UC_i = r_i ⊕ pi

(Step vii) Also, calculates $Nonce_i^*$ = $Nonce_i$ ⊕ TS_1 for subsequent usage in a safety evaluation.

(Step viii) Finally, the U delivers the sign-in credentials. Msg_5 = {$Nonce_i^*$, USN, UC_i, TS_3, ue_i, f_i to the specified IoT node. The sign in process is complete after step 8 is completed. The user interface allows the user to pick any node in the IoT ecosystem.

4.4. Validation and Keys Acceptance Stage to make use of the IoT sensor node's activities. Upon connecting to the right node, it will submit the login credentials of the user demand to GW, it will carry out the required verification tests. When all three of these things confirm each other, a session ID is created among the device of the user and IoT sensor node. The registration and validation phases are depicted in Figure 4. The processes of this phase are shown in the stages that follow.

(Step i) When getting the notification from requesting a login, U, SN checks the timestamp when receiving TS_3, i.e., (|TS_3 – T| < ΔT). Check the security parameter as well. ($Nonce_i^*$? = $Nonce_i$ ⊕ TS_1)?, in order to verify the U .

The operation moves on to the next stage if the requirement fails to be fulfilled, in which case the login process has been suspended..

(Step ii) SN utilizes the values of ue_j and p_j to evaluate q_j = ue_j ⊕ p_j

(Step iii) Next, SN calculates A_j = h(SX_{gSN} ‖TS_1‖TS_2) ⊕ q_j

(Step iv) SN sends msg6 = {UC_i , USN, ue_i , ufi , TS_3, TS_4, $Nonce^*_i$} in relation with GW. By the assumption of the parameter $Nonce^*_i$ and the transaction time, it may determine the authenticity of U and the node SN. The node SN validates the GW in this stage.

(Step v) GW confirms the received timestamp (|TS4 – T| < ΔT) and ($Nonce^*_i$? = $Nonce_i$ ⊕ TS_1), competence over both the U and the gadget's SN. The GW advances to the following phase if the prerequisite is satisfied; else, the procedure is terminated.

(Step vi) The safety characteristics are then calculated by GW.: a_j^* = h(ID^*_{SN} ‖SK_g), q_j^* = ue_i ⊕ p_j^*, and q_j = A_j ⊕ h(SK_{gSN} ‖TS_3‖TS_4). Following that, GW evaluates the standard of q_j and q_j^*. GW confirms the corresponding nodes SN & the user U if they're each identical.

GW must correctly validate the IoT sensor node SN based on the obtained data. (Noncei) depending on UIDu . As a result, GW does below listed steps:

(Step i) GW computes r_i^* = UC_i ⊕ h(UID_u ⊕ SK_g) and USN^* = h(SK_{gui} ‖TS_3‖$Nonce_i$ ‖r_i^*)

(Step ii) GW contrasts with the initial USN and the evaluated USN^* to validate the U If the confirmation requirement is not met, GW stops If the communication fails, the GW moves on to its subsequent phase.

(Step iii) Next, GW computes the security parameters: GP_{ij} = $Nonce_i^*$ ⊕ r_i^* ⊕ h(a_j^*‖SK_{gSN}) and VV_i = h(UD_{SN^*} ‖TS_3‖TS_4‖TS_5‖SK_{gu})

(Step iv) GW submits msg_7 = {GP_{ij}, VV_i ,TS_5} to SN.

After receipt of the validation requirements msg7 from the GW, SN evaluates the below processes

(Step i) SN checks the timestamp $|TS_5 - T| < \triangle T$. If the confirmation condition is not met, procedure is aborted; alternatively, it will proceed.
(Step ii) Then, SN verifies the validity of GP_{ij} with $Nonce_{i^*} \oplus r_i \oplus h(a_{j^*} \| SK_{gSN})$. If the condition is not met, procedure is ended; alternatively, it continues to the further stage.
(Step iii) Next, SN evaluates $cha = R_i \oplus Nonce_i \oplus msg_i$, and $VV_{i^*} = h(V_i \| TS_4 \oplus msg_i)$, where msg is a single-time-generated random number. Afterwards, SN computes the session key as $S_{Key} = h(r_i \oplus msg_i \oplus Nonce_{i^*})$
(Step iv) At last, SN sends $msg_8 = \{VV_{i^*}, TS_3, TS_4, TS_5, TS_6, cha\}$ to the U. When U collects the verification parameter msg8 from SN, U carries out upcoming actions:
(Step i) U conducts timelines verification, $|TS_6 - T| < \triangle T$? If such is the case, this process is terminated; alternatively, the following phase is conducted.
(Step ii) U fetch $msg_{i^*} = cha \oplus r_i \oplus Nonce_{i^*}$
(Step iii) U validates $VV_{i^{**}} = h(h(USN \| TS_3 \| TS_4 \| TS_5) \oplus msg_{i^*})$. Then, U verifies if $(VV_{i^{**}} = VV_{i^*})$. If otherwise, the U is dubious about the SN and GW's authorization; alternatively, the U calculates the session key as $S_K = h(msg_{i^*} \oplus r_i)$ successfully completed the authentication and key agreement step.
4.5. Phase of Password and Biometric Change to maintain strong security, the user password must be updated on a frequent basis during this period. The suggested protocol makes it simple to allow the user to modify their password.
(Step i) User Interface (U) who has to update their password launches the IoT application on a smart device and inputs their previous password UP_i and feature extraction UF; they then compute the masked for every user's biometric extraction of features as $UP_i = h(UP_i \oplus r_i)$, $uf_i = h(uf_i \oplus r_i)$
(Step ii) Then, U calculates $q_{i^{**}} = h(p_i^{Nonce\ i} \oplus ue_i \oplus UP_i \oplus X_{gn})$ and $r_{i^{**}} = h(uf_i \oplus q_i^{Nonce\ i} \oplus Nonce_i)$ and moves on to the subsequent action
(Step iii) U then verifies the equality of $q_{i^{**}}$ and $r_{i^{**}}$ with the original one $q_{i^*} = h(UP_i \oplus SK_{gu})$ and $r_{i^*} = h(uf_i \oplus SK_{gu})$. If any of the prerequisites are not met, the system will be terminated and the user will be unable to reset their password even though they entered their information correctly.
(Step iv) U inserts the new password PW_{i^*} and fresh fingerprint F_{Pi^*} . He or she then determines the mask hash function for every one of them as $UP_{i^*} = h(PW_{i^*\ i} \oplus_i r_i)$ and $UF_{i^*} = h(F_{Pi^*} \oplus r_i)$, correspondingly
(Step v) Later, U In accordance with the fresh password, changes the parameter q_i^* as $q_i' = h(UP_{i^*} \oplus SK_{gu})$. Then, it calculates new uf_i as: $uf_i' = q_i'^{\ uf\ i} \oplus SK_{gu}$
(Step vi) The phase successfully ends when the U replaces the old f_i that was saved in the memory of the smart gadget with the new uf_i'.

5. Formal Security Examination

Making use of the AVISPA Tool is a robust and a versatile automatic verification tool of applications for the development of cryptographic protocol evaluations models, verification, and validation. This protocol is initially coded in HLPSL and then validated with the AVISPA tool. Using the HLPSL2IF interpreter, the HLPSL program is subsequently transformed to intermediate format (IF). Finally, the back ends are provided the IF specification as input. Following the execution of the IF, the back-end presents the outcome of the protocol simulation by evaluating the output format (OF), accompanied with a description of whether the protocol is secure or hazardous against MIM and replay attacks. Back ends also confirm the protocol's security properties, such as its adaptability against most known attacks, authentication, and key secrecy. It should be noted that AVISPA employs the Dolev-Yao threat model [28] has more information on the AVISPA tool and HLPSL.

To put the suggested protocol into action and simulate it on the proposed protocol's user registration, login, and authentication stages are accomplished in HLPSL by using three fundamental distant user roles, IoT sensor node duties, and gateway node responsibilities. The environment, session, and objective mandatory roles are also stated. Figure 5 shows the simulated results, which clearly show the protocol that has been suggested is resistant to MIM and replay attacks.

Results and Discussion

Also mentioned are the mandatory roles for the environment, session, and aim. The simulation results shown in Figure 5 show the suggested protocol is resistant to MIM and replay attacks.

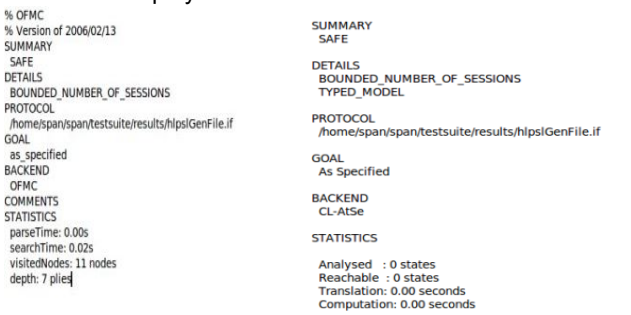

Fig: 5 The simulated outcomes for the OFMC and CL-AtSe back ends

Conclusion

The provided a safe and lightweight three-factor distant authentication for user's solution suitable for future IoT WSN applications in this paper. The suggested protocol enables a trustworthy gateway node to authenticate an authorized distant user with an IoT sensor node. Following mutual authentication between the user and the IoT sensor node, a symmetric session key SK is generated for future safe interactions. The protocol presented is security is formalized utilizing the popular technique. An unofficial security assessment also proves that the recommended technique is effective is robust to the most common attacks. AVISPA simulation is used to investigate the formal security, and the results indicate that our protocol is trustworthy.

***Authors**: 1.Research Scholar Mr.Alumuru Mahesh Reddy, Department of ECM,KLEF(Koneru Lakshmaiah Education Foundation). Green Fields, Vaddeswaram, Andhra Pradesh 522302,E-mail: alumuru.mahesh@gmail.com.*
2. Associate Professor, Dr M.Kameswarao Department of ECM,KLEF(Koneru Lakshmaiah Education Foundation). Green Fields, Vaddeswaram, Andhra Pradesh 522302,E-mail: kamesh.manchiraju@kluniversity.in

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

[5] 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.
[6] C. T. Chen, C. C. Lee, and I. C. Lin, “Efficient and secure threeparty mutual authentication key agreement protocol for WSNs in IoT environments,” PLOS ONE, vol. 15, no. 4, article e0232277, 2020.
[7] M. Teymourzadeh, R. Vahed, S. Alibeygi, and N. Dastanpour, “Security in wireless sensor networks: issues and challenges,” 2020, https://arxiv.org/abs/2007.05111.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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. Journal of Sensors 17
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] X. Niu and Y. Jiao, “An overview of perceptual hashing,” Acta Electronica Sinica, vol. 36, no. 7, pp. 1405–1411, 2008.
[25] Z. Jie, “A novel block-DCT and PCA based image perceptual hashing algorithm,” 2013, https://arxiv.org/abs/1306.4079.
[26] L. Kotoulas and I. Andreadis, “Colour histogram contentbased image retrieval and hardware implementation,”IEE Proceedings - Circuits, Devices and Systems, vol. 150, no. 5, pp. 387–393, 2003.
[27] 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.
[28] 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.