Biometric Based User Authentication Protocol in Smart Homes

Hossein Gharaee*
ICT Security Faculty
ICT Research Institute (ITRC)
Tehran, IRAN
gharaee@itrc.ac.ir

Fateme Shabani
Tarbiat Modares University
Tehran, IRAN
fateme.shabani@modares.ac.ir

Naser Mohammadzadeh
Department of Computer Engineering, Shahed University
Tehran, IRAN
mohammadzadeh@shahed.ac.ir

Shayan Mehranpoor
Department of Computer Engineering, Shahed University
Tehran, IRAN
Shayanmehranpoor@yahoo.com

Received: 2020/07/18 Revised: 2020/09/22 Accepted: 2020/09/30

***Abstract*— The smart home is an important Internet of Things applications. Due to the smartphones development, expansion of their network, and growing the data transfer rate, security in personal life has become a dramatic challenge. Therefore, it is essential to secure such a system to create a sense of relaxation in the lives of users and homeowners to deal with possible occurrences. The integration of technologies for the automation of home affairs with the Internet of things means that all physical objects can be accessed on cyberspace; therefore, the concerns raised by users about the lack of privacy and security are serious arguments that science and technology should answer. Therefore, addressing security issues is a crucial necessity for the development of the smart homes. Although authentication protocols have been proposed based on smart cards for multi-server architectures, their schemes cannot protect the system against stolen smart cards and dictionary attacks in the login phase and do not satisfy perfect forward secrecy. To overcome these limitations, this paper proposes an anonymous, secure protocol in connected smart home environments, using solely lightweight operations. The proposed protocol in this paper provides efficient authentication, key agreement, and enables the anonymity of devices and unlinkability. It is demonstrated that the computation complexity of the protocol is low as compared to the existing schemes, while security has been significantly improved. This protocol ensures that even if the stakeholder's device or the IoT device is attacked, they are robust against them.**

Keywords*— *Internet of Things, Smart Home, Security, Anonymity, Authentication Protocol.

1. INTRODUCTION

The Internet of things (IoT) refers to devices communicating with one another along with their identification and discovery under an integrated network with a specific identifier [1]. Smart home, smart wear, intelligent power distribution network, smart city, all using IoT technology that can help people to improve their health and safety and reduce energy consumption. The new environment and features of the devices, especially smart home-based systems, have made the security of this technology particularly attractive and have provided many architectures and platforms for it. In addition, there is a large volume of communication between devices on a machine-to-machine basis, which means that we will not have much control over this connection [2].

In addition, due to the ownership of the things and the privacy of individuals, attention to security issues related to identification, discovery, accessibility, access control, privacy, and trust are also more important in the subject of smart objects [3]. Abuse of IoT technology in smart homes will endanger the lives of people; therefore, security is a key issue in the implementation of this technology, which requires extensive research [4]. Ensuring the safety of human life, preventing undesirable events, the availability of objects, cryptography and protection technologies, confidentiality and integrity of information, irrevocability, information security and their security levels in different systems, authentication of objects and individuals using multiple factors such as cipher Pass, location and biometrics, different models for trust and non-centralized authentication, are some of these needs [5]. There are many solutions to provide security and privacy. One of the methods for providing security and privacy is authentication protocols by which the user and servers confirm the validity of the other party before sending data [6].

Five general characteristics, including automation, multi-purpose, adaptation, interaction, and productivity should be provided in a smart home. Various technologies have been developed to provide these features. Home automation is implemented in the form of manageable, programmable and intelligent houses; with the advancement of technology and the introduction of the IoT in this area, the issue of intelligence and especially remote control has been special [7]

Recently, authentication schemes [8] [9] [10] has been proposed based on smart cards for multi-server architectures, but their schemes cannot protect the system against stolen smart card and dictionary attack in login phase and do not satisfy perfect forward secrecy. On the other hand, three-factor authentication, by including biometrics into the authentication schemes, has been proposed in literature [11] [12].

In smart homes, we can use many communication technologies but each of them has security problems that require consideration. The security issue in a smart home is one of the key issues that is posed before choosing the appropriate

platform for its implementation. Essentially providing an unsafe platform can give us a good platform for attacks such as tricks, eavesdropping, and man in the middle, and replay attacks [5].

Therefore, the main challenge in using this technology is the adoption of an architecture that has a proper solution in this area, not only covering the issues of communication and performance of systems in the area but also able to provide security for users. In this way, providing a framework for enhancing security, privacy, and trust are of great importance [13].

In this research, we propose a framework of IoT for improving the security of smart home through the Internet. We can protect and prevent system against well-known attacks such as smart card stolen and dictionary attack by using biometrics in the authentication phase,. Also, we can provide perfect forward secrecy in the system. In our system, we use smartphone instead of smart card, so we should access to the smartphone biometric output, but the only output that we can access is user biometric acceptation by the smartphone, which in smart cards is not like that. Therefore, for solving this problem we use hash of biometric output and concatenation of UDID.

The proposed protocol is completely symmetric key based and contains the additional important properties of anonymity and unlinkability of the user and the end-node to any outsider. Thanks to this property, user profiling can be avoided based on the behaviour of the accessed nodes. Leakage of the user's information is not possible even in instances where the end-node is compromised because the end-nodes cannot derive the real identity of the user.

We considered a Two-factor authentication in our system, based on the password of the user and the biometrics of the user's device. Even if the user's device is stolen, the intruder cannot abuse the stored secret information due to its particular construction. All of the other solutions proposed in the literature exploit expensive public key solutions including elliptic curve cryptographic (ECC) operations to obtain authentication and anonymity in the access control system [5].

Improvement of authentication and key agreement protocol in IoT environment, protocol analysis, comparing security requirements, and computational cost between proposed scheme and other schemes are main contributions of this paper. The main contributions of this paper are summarized as follows. We propose two-factor anonymous authentication protocol using biometrics in smart homes and this protocol is completely symmetric key based. All of the other solutions proposed in the literature exploit expensive public key solutions including elliptic curve cryptographic (ECC) operations to obtain authentication and anonymity in the access control system. The proposed protocol contains the additional important properties of anonymity and unlinkability of the user and the end-node to any outsider and leakage of the user's information is not possible even in instances where the end-node is compromised because the end-nodes cannot derive the real identity of the user. In the proposed protocol even if the user's device is stolen, the intruder cannot abuse the stored secret information due to its particular construction.

The rest of this paper consists of the following sections. Section 2 presents the related works. In Section 3, we discuss smart home security and its security requirements. Section 4 describes our protocol. In Section 5, we analyze the security of the protocol. In Section 6, we analyze the performance of the protocol. Finally, we conclude the paper in Section 7.

2. Related Works

Cyberspace includes storage, review and information exchange through network systems and physical infrastructure, especially the Internet. Entering a smart home into the Internet of Things means storing, processing, and analyzing data into cyberspace. Connecting smart home to the Internet and entering it into cyberspace has created new security challenges. Equipment in these homes is important and private information for users should have a high degree of security. These homes are highly vulnerable to online attacks and if the attacker hacks the system, he will access personal information, home-based information, and privacy of their families [14]. The importance of security in smart home is more than the importance of security in other systems [15]. The introduction of IoT technology into smart home has led to a balance between control, security, and privacy [16].

For authentications in WSNs with symmetric key-based system, we have two approaches. In the first approach, we can use secret-sharing as explained in Benenson et al [17] and Banerjee and Mukhopadhyay [18] that let sensors to collaborate in order to make a decision. The second approach contains the domain of smart-card approaches where recently many papers have been published in this approach. However, most of them were vulnerable to Offline Guessing Attack, MITM attack, and Stolen card attack. In our scheme, we guaranty anonymity and untraceability of the user, which make our framework stronger.

WSNs access control is divided into two major architectural categories: distributed or centralized. In the distributed mechanism, the end-device makes the final decision but in the centralized one, final decision is made in gateway level. Centralized access control systems have several severe disadvantages. First, they are not able to make decisions based on contextual information related to the end-device itself since the end-nodes can be seen as smart devices. Second, the central gateway, which stores and manages all information of every device, becomes a single point of failure.

In our scheme, we use anonymous authentication for IoT devices based on symmetric key cryptography. Following its purpose and functionality, our system is called efficient distributed anonymous authentication and access control for smart home sensors using symmetric key cryptography [8].

In our proposed system, we consider 4 entities: (Table 1)

$$\begin{cases} 1-Owner \equiv \mathrm{Re}gistration\ Server \\ 2-User\ Device \rightarrow \quad Mobile\ with\ Biometric \quad \rightarrow \begin{cases} Fingerpr\mathrm{int} \\ Face\ Detection \end{cases} \\ 3-User \\ 4-end-node \quad \rightarrow \quad N_j \end{cases}$$

In this scheme, the homeowner acts as a registration server and it is responsible for the authentication management of

TABLE 1. ENTITIES IN THIS ARTICLE

	Description
U	User
U_d	User Device
EN_s	IoT devices or End-Nodes in Smart Home
O	Home Owner

nodes. All nodes should be pre-installed by the homeowner. In addition, for using IoT devices, the user should login with biometric parameter in smartphone. After user logs into the system, he or she can send an anonymous request with struggling of the homeowner. In designing this system, the main purpose is to maintain anonymity in such a way that no external entity can obtain information from the user or the node.

In our scheme, owner should pre-install all the nodes of network with some secure information. In addition, user needs to register with the owner for key material related for communicating with a particular node or set of end-devices. The secret key material is defined by the owner and kept on the user's smartphone.

In this scheme, the ENs can check the validity of the authentication of the user. If it is positive, a message containing the essential information is sent to the user. Our scheme contains the following security features:

- Anonymity: No one can get the identity of the ENs or the user. In addition, we satisfy unlinkability of the users and end-nodes with respect to outsiders.
- Access Control: The owner accesses to each node uniquely which no one can access to them.
- Data authentication: It is ensured that the information has not been altered by unauthorized or unknown means.

Our system is lightweight, which we limit the operations used in the protocol to hashes, concatenations and symmetric key encryptions/decryptions. In addition, our system is a distributed system that the access control and authentication are made at the sensor layer.

3. SMART HOME

Privacy, trust, security, and communications are some of the of the major challenges to smart home, according to the definition and presentation of the smart power company and complementary research by Komninos and his colleagues on smart home security in 2017 [19].

3-1. Smart Home Security Challenges

According to a study conducted in 2015-2017, as shown in Table 2, the challenges in the smart home domain can be the reliability of sensors and monitoring systems and the proper settings for proper operation, reliable and secure communications in the smart home and maintaining integrity of information, proper scenario against system disruption or denial of service, security for integration systems, including decision-making tools and software, reliability and security

TABLE 2. IOT CHALLENGES IN SMART HOME [2] [5] [19]

Title	Description
Privacy	Privacy, and affiliate issues such as information security and disclosure of information and data
Connections	Strength, security stability, high communication protocols and heterogeneity of these communications
Safety	Physical safety of objects, physical access and self-sustainability
Network & Security	The network is also a concern due to communication and the breadth and variety of communications
Security	Preserving security independently of the challenges of the Internet of things
Trust	Trust mechanism
Confidentiality	Maintaining confidentiality and related solutions such as encryption and object constraints have created challenges.
Information Security	Increasing the amount of information, the number of objects and heterogeneity, protecting information security against the Internet of things
Identity Management	Authentication, identification and objects, and standardization in this area are Internet of things concerns.
Energy consumption	The development of the Internet of objects will increase energy consumption, which is also a solution to energy consumption control challenges of the Internet of things.
Big data & Cloud	An increase in the amount of generated data and its transmission methods and the creation of large data has created concerns in controlling the processing of this data.
Ability to work devices and objects together	In order to establish communication and maximize the productivity of the Internet, due to the expansion of the number and heterogeneity of objects, have affected the ability to work with various objects.
Storage	An increase in storage volume takes storage concerns into the volume of generated data
Heterogeneity of objects	Increasing the number of heterogeneities and the need to establish communications and different types of data created and managed and processed

related to architecture and technical design, privacy protection for smart home residents, social protection, privacy and encryption, number of disparate objects and smart devices and big data, cloud and data storage problems are named.

3-2. Vulnerabilities

Smart home is a smart living environment that is designed to meet human needs to provide its comfort and security [20]. The advancement of smartphone technology and increased use of smart devices in homes have led to the learning of this technology and on the other hand, have increased the level of security vulnerabilities of users in this area [21]. The security risks are due to the lack of attention of manufacturers to the vulnerabilities of the services provided. Yoon and colleagues conducted a study on the causes of vulnerabilities in 2015, which we will continue to provide the results of this study [22].

- Access to networked systems: Internet-based systems are objects that are connected to the Internet; attacks can be done remotely or with direct access to controllers, networks, or by downloading malware on equipment.
- Physical access to systems: Smart home network, whether wireless or with cable connections, can be physically attacked.
- Systems Limited Resources: Smart device controllers use thin chips and limited memory. This leads to the inability to equip itself with the use of sophisticated security algorithms and lower security levels.
- Lack of uniformity of equipment: The variety of equipment and the lack of sufficient documentation of the operating system, the software used and the security mechanisms used in them will cause vulnerabilities.
- Use Fixed Firmware: Failure to design and providing mechanisms to update the security of the middleware will cause serious vulnerabilities.
- No use of daytime security standards: In designing and operating, the equipment is another vulnerability.
- Lack of expertise in users: The lack of awareness of security issues in home users for managing equipment is one of the most important vulnerabilities in this area.
- Lack of security in accessing cloud services: Failure to use secure and proper protocols for this service will increase the chances of data theft in a single cloud.
- Use of inappropriate and poorly encoded algorithms: Failure in cryptographic algorithms can lead to theft of information.
- Data disclosure: It is vulnerable due to the weakness of the storage space on the cloud or on its own.

3-3. Smart home security threats

Connecting smart home appliances will create a link between real life and cyberspace. This connection will bring the threats of cyberspace into human life; therefore, security in intelligent home systems to protect life and health, property, personal information and control home and its equipment is imperative. Daniel Schwartz, a consultant on the security of the Intelligent Home Systems Security Institute in 2016, presented a study.

This research is done according to the current architecture of the smart home, divides the range of activities in this area into the internal and external boundaries (Fig.1) [23].

The internal range includes indoor equipment and systems that ultimately use a central system to communicate with the outside environment. The outside range is the Internet and Outdoors area, which includes the Internet, the Web, and cloud computing and existing services for controlling home systems. In numerous research and papers, threats to the Internet of things and smart home have been introduced. These studies are based on the type of media, either in terms of manipulation or in terms of change, or the internal and external scope mentioned above.

- Traffic manipulation: In this attack, the attacker with physical or network access, by tampering with traffic, misleads the sender or receiver of the information [20].
- Identity impersonation: An intruder can deceive, steal, and violate privacy by impersonating one of the smart home components [22].
- Remote Control: Attackers provide users with programs that empower users to steal user information remotely.
- Eavesdropping Attack: The attacker may listen to the stream of information. This attack violates the privacy and disclosure of information.
- Reflection: The striker will store the valid data and send it back to the equipment in the future. This data is valid for the system and can therefore cause system confusion.
- Duplicate: In this attack, the attacker uses a duplicate identity on the network.
- Counterfeiting: Object identity is forged and used in multiplication attack.
- Malicious codecs: Media playback codes used to steal and disclose information that violates privacy, trust, and information security.
- Malware: These malwares use corrupt encryption code to corrupt and encrypt data and often extort users to unlock files.

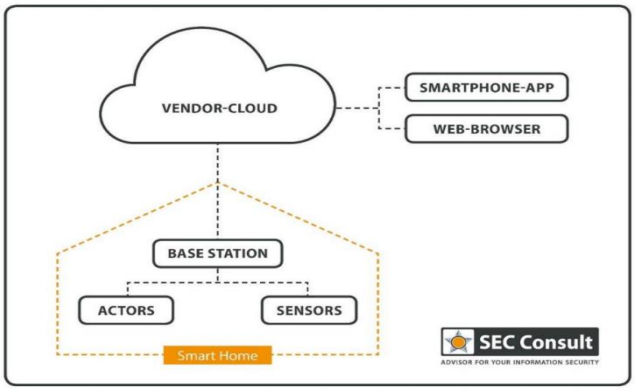

Fig. 1 Internal range and external range and smart home constituent parts [23]

3-4. Security Requirements

Exploring the threats and attacks mentioned in the previous section will be a good guide to understanding the security requirements of the smart home domain. In the field of smart home security needs, Kang and his colleagues conducted a study in 2017 [24]. We summarized the general requirements according to the results of this study:

- Confidentiality: Ensures that messages exchanged are only understandable by the contact person.
- Integrity: This ensures that messages exchanged by a third party are not altered.
- Validation: This mechanism ensures that the people who participate in each process are those who claim to be.
- Availability: Ensures sustainability and service delivery. Attack target this requirement because these attacks cause disruptions to the service.
- Access Policies: This mechanism is intended to ensure that users are properly licensed to perform operations.
- Freshness: This ensures that the received information is not duplicate. Replay attacks target this requirement in which an old message is sent to restore its status to its old state.
- Non-Repudiation: This mechanism ensures that an entity cannot deny it after doing business.
- Forward secrecy: This mechanism ensures that when an object gets out of the network, it will no longer be able to understand the routed information on the network.
- Backward secrecy: This ensures that any new object that connects to the network will not be able to understand network communications before joining it.

4. PROPOSED PROTOCOL

In this scheme, different phases can be distinguished: (a) the installation phase of the ENs, (b) registration phase, (c) installation phase of the user, (d) user login phase, (e) request phase, (f) answer phase, (g) information retrieval, (h) update of user's password. Fig.2 shows an overview of the protocol among each entity under the different phases. In addition, Table 3 gives a summary of notations and abbreviations.

In first phase, we use (1), pre-shared keys between owner and user (*Kuo*) and end-node and owner (*Keo*).

$$K_{uo} = H(H(ID_u^r) \| K_m) \qquad (1)$$

$$\begin{cases} ID_u^r \rightarrow real\ identity\ of\ the\ user\ like\ name \cdot national\ ID... \\ K_m \rightarrow master\ key\ of\ the\ owner \end{cases}$$

This key $E_k(K_{uo})$ keep in the smartphone is encrypted and even if the user's smartphone is stolen, the attacker cannot access the stored information. Now user enters IDru, PWu, BIOu, this information helps the device calculate below information (2):

TABLE 3. SUMMARY OF NOTATIONS AND ABBREVIATIONS

	Description
U, Ud	User and User's device
EN_s	End-Nodes or IoT devices
O	Home Owner
K_m, x, y	Master key and two other secrets of O
ID_i^r, PW_i	Real username and password of U
BIO_u	H(Device biometric output (true or false) ‖ Device UDID)
$ID_i = H(ID_i^r)$	Derived identity of U
N_j	Identity of end-node j
$K_{uo} = H(H(ID_i^r) \| K_m)$	Secret shared key between O and U_d
$K_{eo} = H(N_j \| K_m)$	Secret shared key between O and EN

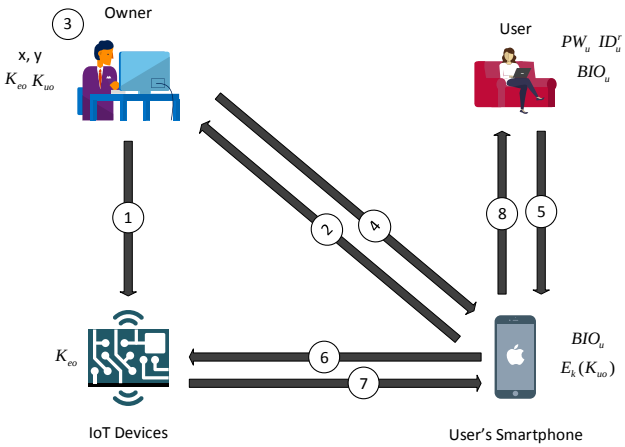

Fig. 2 Overview of the proposed protocol

$$\begin{cases} RPW_u = H(PW_u \oplus BIO_u) \\ ID_u = H(ID_u^r) \end{cases} \rightarrow K = H(ID_u \| RPW_u) \qquad (2)$$

Thus, we derive K_{uo} like (3):

$$D_k(E_k(K_{uo})) \\ K_{eo} = H(N_j \| K_m), \quad N_j: \ identity\ of\ the\ node \qquad (3)$$

A. Installation phase of the ENs

Let x, y be two secrets chosen by the owner. N_j denotes the identity of the end-node j. The owner shares below parameters with each node in the network using the pre-installed or pre-shared secret key K_{eo} between end-node and owner. Note that (4), *y* is still a secret parameter for the user.

$$y, N_j, H(x \| y), H(N_j \| H(x)) \qquad (4)$$

B. Registration phase

As we mentioned before, only BIO_u, together with the encrypted shared secret key with the owner $E_k(K_{uo})$ are stored on its device. Now if user entered ID^r_u and PW_u, the U_d is able to calculate below parameters (5):

$$\begin{cases} RPW_u = H(PW_u \oplus BIO_u) \\ ID_u = H(ID_u^r) \end{cases} \quad (5)$$

Now with this information, $K = H(ID_u \parallel RPW_u)$ has been calculated. Then registration request consists of the message registration with the owner to the specific device N_j. We use a time stamp in reqAcc to avoid replay attacks (6):

$$ID_u \parallel E_{k_{uo}}(ID_u^r \parallel RPW_u \parallel reqAcc) \quad (6)$$

C. Installation phase of the users

First, the secret shared key $K_{uo} = H(ID_u \parallel K_m)$ is computed and after decryption of received message, the owner checks the identity ID_u^r by verifying if $ID_u = H(ID_u^r)$ and also with computation of $RPW_u = H(RPW_u^r)$ uses to compute secret key material with parameters x, y.

Each of these parameters, A_i, B_i, C_i, D_i, E_i has a specific role. After these computations, owner sends the message $E_{k_{uo}} = (B_i, C_i, D_i, E_i, H(B_i, C_i, D_i, E_i))$ to the user's smartphone, so the parameters B_i, C_i, D_i, E_i will be stored on the user's smartphone. In Fig.3, we can see a graphical overview of the registration and installation phase.

D. User login phase

First, the user enters identity ID_u^r and its password PW_u with BIO_u, then device can compute in (7).

$$\begin{cases} ID_u = H(ID_u^r) \\ RPW_u = H(RPW_u^r) \end{cases} \xrightarrow{then} E_i \overset{?}{=} H(ID_u \parallel RPW_u) \oplus RPW_u \quad (7)$$

Now, if computed E_i equals with stored E_i, login is successful.

E. Request phase

After successful user login, first, the user selects N_j, then the following (8) and (9) computations are performed by the device.

$$H(x) = D_i \oplus H(ID_u \parallel RPW_u) \quad (8)$$

$$H(A_i) = C_i \oplus H(RPW_u \parallel ID_u) \quad (9)$$

First, from H(x), user can construct $H(Vj \parallel H(x))$ which is also stored at the end-node. Since $H(x \parallel y)$ is stored in end-node, the end-node constructs B_i and from B_i it can find A_i. Consequently, the following operations are performed to construct a secret shared key and corresponding cipher text.

We consider a random nonce N_i and a Req which contains time stamp to prevent replay attacks.(Equations (10)-(15))

$$C_1 = H(N_j \parallel H(x)) \oplus H(ID_u \parallel N_i) \quad (10)$$

$$C_2 = H(A_i) \oplus N_i \quad (11)$$

$$V_1 = H(N_i \oplus B_i) \quad (12)$$

$$CID_i = B_i \oplus H(C_1) \quad (13)$$

$$K = H(N_i \parallel N_j \parallel H(A_i)) \quad (14)$$

$$E_K(ID_u \parallel C_2 \parallel \mathrm{Req}) \quad (15)$$

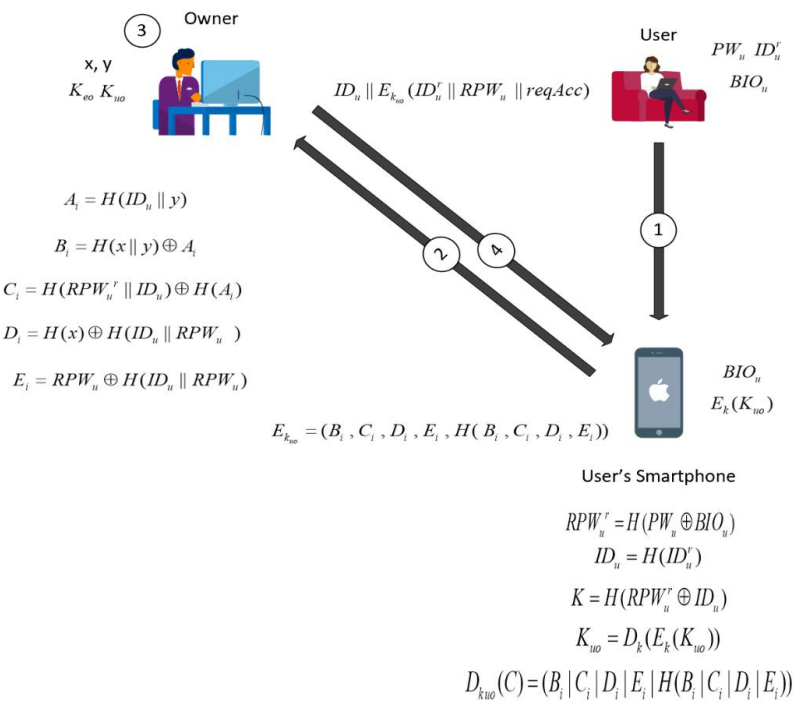

Fig. 3 overview of the registration and installation phase

The following message is sent to the gateway, which forwards the message further to the corresponding node N_j.

$$CID_i \| C_1 \| C_2 \| V_1 \| E_K(ID_u \| C_2 \| \mathrm{Re}\,q_1) \quad (16)$$

F. Answer phase

In this phase, N_j executes following computations with its stored parameters.(Equations (17)-(21))

$$H(ID_u \| N_i) = H(N_j \| H(x)) \oplus C_1 \quad (17)$$

$$B_i = CID_i \oplus H(H(N_j \| H(x)) \| H(ID_u \| N_i)) \quad (18)$$

$$A_i = B_i \oplus H(x \| y) \quad (19)$$

$$N_i = H(A_i) \oplus C_2 \quad (20)$$

$$V_1^* = H(N_i \oplus B_i) \quad (21)$$

If V_1^* is equal toV_1 value, the user will be authenticated. Then the key $K = H(N_i \| N_j \| H(A_i))$ is derived that the decryption $D_k = (ID_u \| C_2 \| \mathrm{Re}\,q)$ can be executed. In this case, the following computations (Equations (22)-(24)) are performed with random value R_j:

$$C_3 = R_j \oplus H(ID_u \| N_i) \quad (22)$$

$$V_2 = N_i \oplus H(N_j \| B_i \| R_j) \quad (23)$$

$$SK_{ij} = H(N_i \| R_j) \quad (24)$$

Finally, $C_3 \| V_2 \| E_{SK_{ij}}(M)$ which M is the requested information or is a confirmation that is sent to the user. Fig.4 gives a graphical overview of the steps in the user's login, request, and answer phases.

G. Information retrieval

The user first derives $R_j = C_3 \oplus H(ID_u \| N_i)$. Then $N_u \oplus H(N_j \| B_i \| R_j)$ is computed and compared with the transmitted value V_2. If it is positive, mutual authentication is obtained and the shared symmetric key can be derived in order to decrypt the last part of the message.

H. Update of user's password

This can be easily done by the user, without involvement of the owner or changes to the other end-nodes in this scheme.

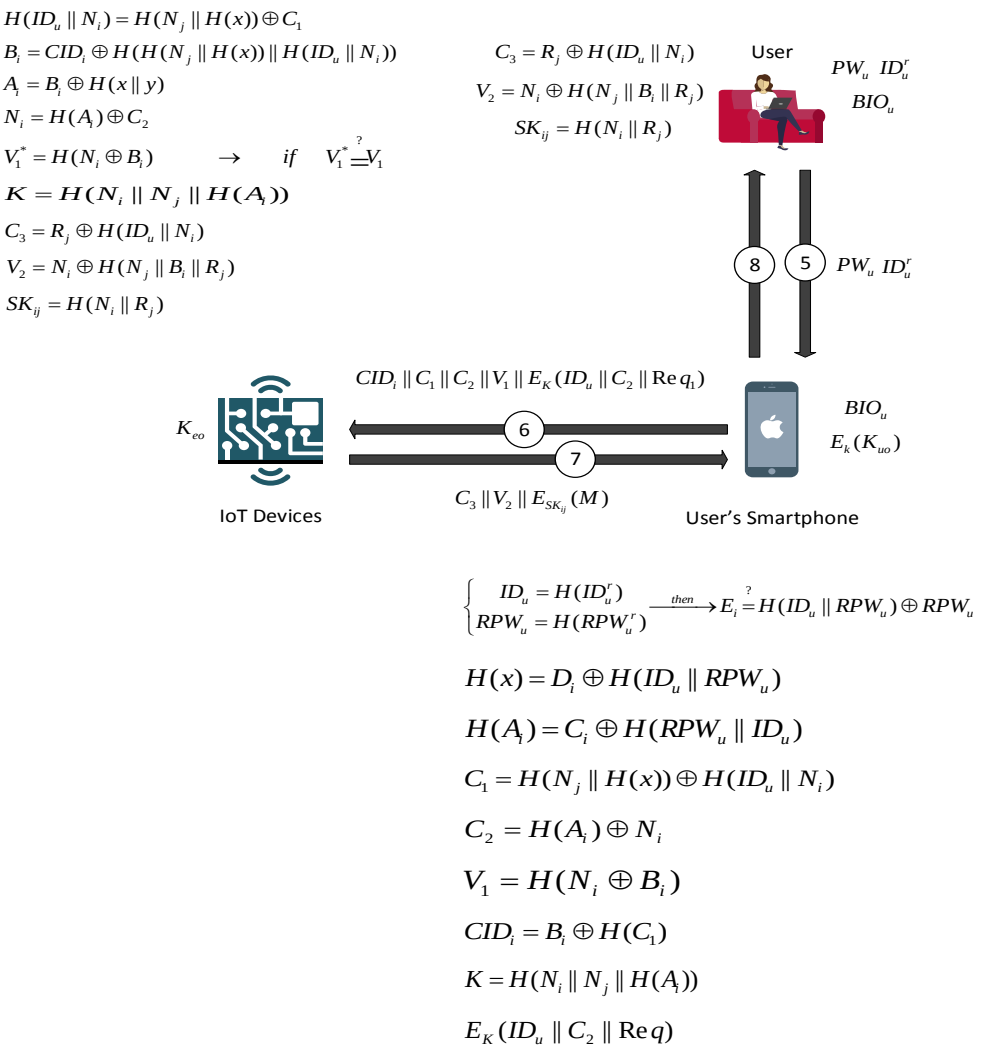

Fig. 4 overview of the steps in user login phase, request phase, and answer phase.

The user needs to enter a new value of the password, and then the value of RPW_u will be updated. With this update, new values of C_i and E_i are computed, which are then stored on the user's device. Also note that the encryption key K of k_{uo} needs to be updated, leading to an update of $E_k(k_{uo})$.

5. SECURITY ANALYSIS

Our protocol protects the system entities from a range of attacks. In this section, we have used AVISPA tool and BAN logic model and informal analysis to show that proposed protocol can withstand all known attacks.

5-1. Informal Security Analysis

In this subsection, we also informally prove that the proposed protocol is secure against the all known attacks.

1) Replay attacks

Since inclusion of a time tamp in the reqAcc parameter, replay attacks in the registration phase are avoided. Since an attacker is unable to decrypt the registration request or the corresponding answer, it cannot change any value. In addition, a replay attack on the user's request to the IoT end-node is impossible due to the presence of a time stamp in the request message.

2) Illegitimate data access or control

A user cannot derive a token itself, since the token is included in the computation of the parameter A_i. From A_i, parameter B_i is derived. As a user does not know the secrets x, y, he is unable to find valid constructions for both A_i, B_i. An adversary cannot get access to a node, even if he is in the possession of the user's device. This follows from the two-factor authentication, where identity and password on the corresponding device are required to further proceed the process.

3) Insider attacks

We distinguish the insider attacks by the impact of four different situations, which are dependent on the combination of compromised objects and users:

- Endanger the user's device: here, the enemy is not aware of the user's identity and password. Consequently, the process cannot be continued. Even if an enemy can restore the information stored on the device such as $B_i, C_i, D_i, E_i, H(B_i, C_i, D_i, E_i)$, it is still impossible to do so, because a valid request requires an identity and a password.
- At risk of getting the final node: Here, it is possible to send false information. The attacker cannot publish important information related to the user's identity, since the information received is only indirectly related to the user's identity. A damaged node does not have enough information to create users that can handle valid requests to other nodes because the hidden secret is no longer known x.
- End Device and Endpoint: Since the identity of the owner is unknown, it may be possible to obtain H(x) from Di. As a result, no credible requests to other nodes can be performed, nor can it be retrieved useful information from other requests.
- End-node user and device at risk: The system is completely broken when the user, device and one of the nodes are compromised. We can expect such a combination of incidents that are very rare.

4) HW/SW attacks

This system is based on a security protocol for smart cards. Similar ideas are applied to the user's side. Even with the recognition of the B_i, C_i, D_i, E_i parameters, the attacker has no other advantage, since the user's identity and password are required, which is related to the confirmation feature of two factors. Note that the attacker can, according to the Ei parameter, launch a dictionary attack into the user's identity and password. But we use user biometric parameter that help us to avoid this attack.

5) Mutual authentication

Mutual authentication between the user and the end-node is obtained since the constructed secret shared key SKij is built using nonces generated by the user and the end-node. As explained before, only the user and the end-node have the required credentials to generate correct requests and answers for the construction of this key.

6) Anonymity and unlinkability

Note that the user request contains the parameter CIDi, which is a dynamic reference that is related to the hidden user's Bi identity. As a result, no one else can connect different requests to a specific user or the same user. It also maintains the privacy of the user's location for any external attacker. From the request, the final node can obtain the indirect link Bi, which is related to the user's identity. Only the owner can retrieve the actual identity.

The attacker can guess the user's password offline by extracting B_i, C_i, D_i, E_i information from a lost or stolen mobile phone. However, the enemy will not be able to confirm the encryption using the extracted information obtained. Confirming the guessed password requires that you calculate the RPWu enemy, which is not possible, because the enemy does not have any information about the user's biometric BIOi.

7) Resist against Man-in-the-Middle attack

In this attack, the attacker tries to hear all the messages between the user and the owner or between the user and the end-user and manually modifies them in the proposed model, even if the user both actively or inaccurately hears all the messages, he cannot get valuable information because he cannot get any information from $H(ID_u \| N_i), H(N_j \| H(x))$

8) Perfect forward secrecy

There are two hidden values: h(x) and h(x || y). The first one can be extracted by the user's smartphone; the latter stored on the server. Since an attacker, cannot access the server, then it cannot get the value of h (x || y) so it is unable to get A_i too. Given this amount is required to obtain the key, then Perfect Forward Secrecy is fully adhered to.

5-2. Simulation For Formal Security Verification Using Avispa

The proposed protocol was formally verified by AVISPA that is a commonly used tool for security protocol assessments. The entities and message exchanges were described by the HLPSL[1] language. The description and information in details can be found in [25].

This subsection discusses several roles for system entities, the session, the goal and the environment of proposed protocol. In Fig. 5-8, we have presented HLPSL code for our proposed protocol. These figures show the HLPSL language code that describes the establishment of the sessions, the environment and security objectives to be guaranteed by our proposed protocol according to the definition of elements declared as secrets in the functions of the entity and the values that authenticate the entities.

Finally, The results shown in Fig. 8 clearly show that the proposed protocol is secure against the replay and man-in-the-middle attacks.

5-3. Authentication proof based on BAN logic

In this sub-section, we present the formal analysis (e.g., authentication, session-key establishment and freshness) of the proposed protocol using the well-known BAN-logic [26]. For details, the reader may refer to [26] BAN logic notations and rules: We use directly BAN-logic symbols and notations from [26] to verify the proposed protocol. The intuitive assumptions for proof are as follows:

- $A1: O| \equiv O \overset{Kuo}{\longleftrightarrow} U$
- $A2: O| \equiv O \overset{Keo}{\longleftrightarrow} EN$
- $A4: U| \equiv \#(C2)$
- $A6: O| \equiv \#(C3)$
- $A7: U| \equiv \#(Nj)$
- $A8: U| \equiv \#(Ni)$
- $A9: O| \equiv U| \Longrightarrow Ni$
- $A10: O| \equiv U| \Longrightarrow Rj$

```
role role_A ( A, B, C:agent,   Ka:symmetric_key, H:function,
SND,RCV:channel(dy))
played_by A
def= local
State:nat,    IDa, IDb, Ta, Tb, Kac, Na, Nb:text
const   sub1, sub2, sub3, sub4, sub5, sub6, aut_ac, aut_ca :
protocol_id
init State := 0
transition
1. State=0 /\ RCV({H(IDa'.Ta').Ta'.H(IDb'.Tb').Kac'}_Ka) =|>
State':=1 /\  Na':=new() /\
%          secret({Ka},sub5,{C,A}) /\
secret({Kac',IDa'},sub1,{C,A}) /\
secret({Na'},sub3,{C,A,B}) /\
SND(H(IDa'.Ta').H(IDb'.Tb').Ta'.xor(Na',Kac').H(H(IDa'.Ta').Na'.Ta'
)) /\
witness(A,C,aut_ac,Kac')
2. State=1 /\
RCV(xor(xor(Na,Nb'),H(Kac.H(IDb.Tb))).H(H(IDb.Tb).
xor(xor(Na,Nb'),H(Kac.H(IDb.Tb))).Na.Ta)) =|> State':=2 /\
secret({Nb'},sub4,{C,A,B}) /\
request(C,A,aut_ca,Na)
end role
```

Fig. 5 Role of A in HLPSL code

```
role role_B( B, A, C:agent,  Kb:symmetric_key, H:function,
SND,RCV:channel(dy))
played_by B
def= local
State:nat,
IDb, IDa, Tb, Ta, Kbc ,Nb ,Na:text
const   sub0, sub1, sub2, sub3, sub4, sub5, sub6, aut_bc, aut_cb :
protocol_id
init State := 0
transition
1. State=0 /\ RCV({H(IDb'.Tb').Tb'.H(IDa'.Ta').Kbc'}_Kb) =|>
State':=1 /\ secret({Kbc',IDb'},sub2,{C,B})
2. State=1 /\ RCV(H(IDa.Ta)) =|> State':=2 /\ Nb':=new() /\
%          secret({Kb},sub6,{C,B}) /\
secret({Nb'},sub4,{C,A,B}) /\
witness(B,C,aut_bc,Nb') /\
SND(H(IDb.Tb).Tb.xor(Nb',Kbc).H(H(IDb.Tb).Nb'.Tb))
3. State=2 /\
RCV(xor(xor(Na',Nb),H(Kbc.H(IDa.Ta))).H(H(IDa.Ta).xor(xor(Na',
Nb),H(Kbc.H(IDa.Ta))).Nb.Tb)) =|> State':=3 /\
secret({Na'},sub3,{C,A,B}) /\
request(C,B,aut_cb,Nb)
end role
```

Fig. 6 Role of B in HLPSL code

[1] High Level Protocol Specification Language

```
role role_C ( C, A, B:agent,  Kac, Kbc, Ta, Tb:text,
Ka, Kb:symmetric_key,  H:function,
SND,RCV:channel(dy))
played_by C
def =  local
State:nat,
IDb, IDa, Na ,Nb ,Kac, Kbc, Ta, Tb:text
const sub1, sub2, sub3, sub4, sub5, sub6, aut_ac, aut_bc, aut_ca,
aut_cb: protocol_id
init  State := 0
transition
1. State=0 /\ RCV(start) =|> State':=1 /\ IDb':=new() /\
IDa':=new() /\ Ta':=new() /\ Tb':=new() /\ Kac':=new() /\
Kbc':=new() /\
%          secret({Ka},sub5,{C,A}) /\
%          secret({Kb},sub6,{C,B}) /\
secret({Kac',IDa'},sub1,{C,A}) /\
secret({Kbc',IDb'},sub2,{C,B}) /\
SND({H(IDa'.Ta').Ta'.H(IDb'.Tb').Kac'}_Ka) /\
SND({H(IDb'.Tb').Tb'.H(IDa'.Ta').Kbc'}_Kb)
2. State=1 /\
RCV(H(IDa.Ta).H(IDb.Tb).Ta.xor(Na',Kac).H(H(IDa.Ta).Na'.Ta))
=|> State':=2 /\
secret({Na'},sub3,{C,A,B}) /\
request(A,C,aut_ac,Kac) /\
SND(H(IDa.Ta))
3. State=2 /\
RCV(H(IDb.Tb).Tb.xor(Nb',Kbc).H(H(IDb.Tb).Nb'.Tb)) =|>
State':=3 /\
secret({Nb'},sub4,{C,A,B}) /\
request(B,C,aut_bc,Nb') /\
SND(xor(xor(Na,Nb'),H(Kac.H(IDb.Tb))).H(H(IDb.Tb).
xor(xor(Na,Nb'),H(Kac.H(IDb.Tb))).Na.Ta)) /\
SND(xor(xor(Na,Nb'),H(Kbc.H(IDa.Ta))).H(H(IDa.Ta).
xor(xor(Na,Nb'),H(Kbc.H(IDa.Ta))).Nb'.Tb)) /\
witness(C,A,aut_ca,Na) /\
witness(C,B,aut_cb,Nb')
end role
```

Fig. 7 Role of C in HLPSL code

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/LATAP6.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.06s
  visitedNodes: 14 nodes
  depth: 8 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/LATAP6.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 6 states
  Reachable  : 3 states
  Translation: 0.05 seconds
  Computation: 0.00 seconds
```

Fig. 8 Analysis of results using OFMC and CL-AtSe tools

Now we have to set goals. Given that the purpose of the protocol is to establish authenticity between entities, we therefore define the objectives as follows:

- $G1: O \mid\equiv V1$
- $G2: U \mid\equiv V2$

Now we proof first goal:

- $R1 = \frac{O\mid\equiv U \overset{Kou}{\longleftrightarrow} O, O\lhd CIDi, C1, C2, V1, Ek(IDu, C2, Req1)}{O\mid\equiv U\mid\sim V1}$
- $R2: \frac{O\mid\equiv\#(C2)}{O\mid\equiv\#(C2, V1)}$
- R3: $O\mid\equiv\#(V1)$
- $R4: \frac{O\mid\equiv\#(V1), O\mid\equiv U\mid\sim V1}{O\mid\equiv U\mid\equiv V1}$
- $R5: \frac{O\mid\equiv U\mid\Rightarrow V1, O\mid\equiv U\mid\equiv V1}{O\mid\equiv V1}$

For proofing the second goal:

- $R1 = \frac{U\mid\equiv O \overset{Kuo}{\longleftrightarrow} U, U\lhd \mathrm{C3,V2,Esk(M)}}{O\mid\equiv U\mid\sim \mathrm{V2}}$
- $R2: \frac{U\mid\equiv\#(C3)}{U\mid\equiv\#(C3, V2)}$
- R3: $U\mid\equiv\#(V2)$
- $R4: \frac{U\mid\equiv\#(V2), U\mid\equiv O\mid\sim V2}{U\mid\equiv O\mid\equiv V2}$
- $R5: \frac{U\mid\equiv O\mid\Rightarrow V2, U\mid\equiv \mathrm{O}\mid\equiv V2}{U\mid\equiv V2}$

5-4. Comparison security features

The security features of our proposed scheme with the other prior related schemes will be compared in this section. The results of the comparison are listed in Table 4.

From Table 4, it can be concluded that the proposed scheme is the only one who can resist against various kinds

of known attacks and fulfil the desirable security features. Therefore, our scheme has better security than the previously related schemes.

6. PERFORMANCE ANALYSIS

Most Smart device controllers have limited resources. Therefore, performance analysis considers as a substantial issue in the real-world. Generally, the performance has been evaluated by using two following main criteria [31]:

6-1. Computational Cost (CC)

This criteria has been evaluated according to the time costs of operations symmetric encryption/ decryption and hash functions. For efficiency analysis, we compare the computation costs of our protocol with the other prior related protocols. To facilitate the analysis, we use the following notations to measure computation costs:

- T_h: the time complexity of the general hash function.
- $T_{E/D}$: the time complexity of general symmetric-key encryption/decryption algorithm.

As pointed out in [16] [17], the running time of a one-way hash function operation, and symmetric-key encryption/decryption operation are 0.00032s and 0.0056s respectively. Thus, we have $T_h \approx 0.00032$s, $T_{E/D} \approx 0.0056$s. The results of the computation complexity comparisons of our scheme and other related schemes are summarized in Table 5. It shows that our scheme is as efficient as the most efficient one of these prior related schemes at sensor nodes. Although the computation cost for the user and the GWN of our proposed scheme is higher than that of Jung et al.'s scheme, it should be tolerable because our proposed scheme provides higher security, and resists most well-known attacks.

TABLE 4 . COMPARISON SECURITY FEATURES

Protocol	[30]	[29]	[28]	[27]	Proposed
User Anonymity	✓	✓	✓	✓	✓
Sensor Node Anonymity	✓	✓	✓	✓	✓
User Unlinkability	×	×	×	×	✓
Mutual Authentication	✓	✓	✓	✓	✓
Resist Stolen Smart Card Attack	✓	×	×	✓	✓
Resist Man-in-the-Middle Attack	✓	✓	✓	✓	✓
Resist Insider Attack	✓	✓	×	✓	✓
Perfect Forward Secrecy	×	×	×	×	✓
Resist Offline Guessing Attack	×	✓	×	✓	✓
Provide Password Change	✓	✓	✓	✓	✓

6-2. Communication Overhead (CO)

This criteria has been evaluated by considering the number of transmitted messages in the communication channel between the entities through the phases of authentication. To facilitate the analysis, we use the following notations and values to measure CO [28]:

- random nonce , hash digest (assuming SHA-1 hashing algorithm is applied) and identity: 128 bits
- ciphertext block (if AES-128 symmetric encryption is applied) : 128 bits.

In our proposed protocol, three exchanged messages in (25):

$$\begin{aligned} &M1=\{ID_u^r, PW_u, BIO_u\}, \\ &M2=\{CID_i \parallel C_1 \parallel C_2 \parallel V_1 \parallel E_K(ID_u \parallel C_2 \parallel \mathrm{Re}\,q_1)\}, \\ &M3=\{C_3 \parallel V_2 \parallel E_{SK_{ij}}(M)\} \end{aligned} \tag{25}$$

These require 1408 bits in the time of the login and authentication phase.

Table 6 summarizes the communication costs and the number of messages exchanged for other prior related protocols. We present the length of the message (bits) that an entity transmits or receives. For example, (768/640) indicates that the user transmits 768 bits and receives 640 bits in each session.

7. CONCLUSION

Presented protocol in this article, is a highly efficient and distributed authentication protocol to access end-nodes in an

TABLE 5. COMPUTATIONAL COST COMPARISON

Protocol	User	End-Node	Owner/RC	Total
[30]	$7T_h \approx$ 0.00224	$5T_h$ ≈0.0016s	$8T_h$ ≈0.00256s	$20T_h \approx$ 0.0064s
[32]	$11T_h \approx$ 0.00352s	$7T_h \approx$ 0.00224s	$14T_h \approx$ 0.00448s	$32T_h \approx$ 0.01024s
[29]	$7T_h + 2T_{E/D} \approx$ 0.01344s	$4T_h + 2T_{E/D} \approx$ 0.01248s	$8T_h + 4T_{E/D}$ ≈ 0.02496s	$19T_h + 8T_{E/D}$ ≈ 0.05088s
[28]	$5T_h + 2T_{E/D} \approx$ 0.01344s	$4T_h + 2T_{E/D} \approx$ 0.01248s	$5T_h + 2T_{E/D}$ ≈ 0.01344s	$13T_h + 4T_{E/D}$ ≈ 0.02688s
[27]	$8T_h \approx$ 0.00256s	$5T_h \approx$ 0.0016s	$8T_h \approx$ 0.00256s	$21T_h \approx$ 0.00672
Proposed	$5T_h + 2T_{E/D} \approx$ 0.01344s	$4T_h + 2T_{E/D} \approx$ 0.01344s	$5T_h + 1T_{E/D}$ ≈ 0.01344s	$13T_h + 5T_{E/D}$ ≈ 0.03248s

TABLE 6. COMMUNICATION OVERHEAD COMPARISON

Protocol	entity	No. of messages
[30]	*user*	*512/384*
	sensor	*1152/512*
	gateway	*512/768*
[32]	*user*	*512/640*
	sensor	*1664/1152*
	gateway	*640/1024*
[29]	*user*	*256/256*
	sensor	*256/256*
	gateway	*512/512*
[28]	*user*	*384/256*
	sensor	*256/512*
	gateway	*768/640*
Amin [27]	*user*	*768/640*
	sensor	*384/640*
	gateway	*280/1152*
Proposed	*user*	*384/384*
	sensor	*1024/768*
	gateway	*384/640*

IoT setting for smart homes, authorized by the homeowner. The efficiency is acceptable to the fact that only symmetric key–based operations are required. Due to the particular construction of the keying materials, the additional features are also obtained such as anonymity and unlinkability of the user and end-node for any outsider. In addition to that, the authentication mechanism can be easily combined with other access control modes. Also, this protocol prevents smart card stolen attack and password guessing attack, due to using customer biometrics parameter in our scheme.

REFERENCES

[1] M. Domb, "Smart home systems based on internet of things," in Internet of Things (IoT) for Automated and Smart Applications, IntechOpen, 2019.

[2] Gaikwad, Pranay P and Gabhane, Jyotsna P and Golait, Snehal S, "A survey based on Smart Homes system using Internet-of-Things," in 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), IEEE, 2015, pp. 0330--0335.

[3] Patil, Akash Suresh and Hamza, Rafik and Hassan, Alzubair and Jiang, Nan and Yan, Hongyang and Li, Jin, "Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts," Computers \& Security, vol. 97, no. Elsevier, p. 101958, 2020.

[4] Zheng, Serena and Apthorpe, Noah and Chetty, Marshini and Feamster, Nick, "User perceptions of smart home IoT privacy," Proceedings of the ACM on Human-Computer Interaction, vol. 2, no. ACM New York, NY, USA, pp. 1--20, 2018.

[5] Yoo, Sang Guun and others, "Security over smart home automation systems: A survey," in International Conference of Research Applied to Defense and Security, Springer, 2018, pp. 87--96.

[6] Shabani, Fateme and Gharaee, Hossein and Ghaffari, Fariba, "An intelligent RFID-enabled authentication protocol in VANET," in 2018 9th International Symposium on Telecommunications (IST), IEEE, 2018, pp. 587--591.

[7] Fakroon, Moneer and Alshahrani, Mohammed and Gebali, Fayez and Traore, Issa, "Secure remote anonymous user authentication scheme for smart home environment," Internet of Things, vol. 9, no. Elsevier, p. 100158, 2020.

[8] A. Braeken, "Efficient anonym smart card based authentication scheme for multi-server architecture," International Journal of Smart Home, vol. 9, pp. 177--184, 2015.

[9] Braeken, An and Porambage, Pawani and Stojmenovic, Milos and Lambrinos, Lambros, "eDAAAS: Efficient distributed anonymous authentication and access in smart homes," International Journal of Distributed Sensor Networks, vol. 12, no. SAGE Publications Sage UK: London, England, p. 1550147716682037, 2016.

[10] Kumar, Pankaj and Chouhan, Lokesh, "A secure authentication scheme for IoT application in smart home," Peer-to-Peer Networking and Applications, no. Springer, pp. 1--19, 2020.

[11] Baruah, Khanjan Ch and Banerjee, Subhasish and Dutta, Manash P and Bhunia, Chandan T, "An improved biometric-based multi-server authentication scheme using smart card," international journal of security and its applications, vol. 9, pp. 397--408, 2015.

[12] Wen, Fengtong and Susilo, Willy and Yang, Guomin, "Analysis and improvement on a biometric-based remote user authentication scheme using smart cards," Wireless Personal Communications, vol. 80, no. Springer, pp. 1747--1760, 2015.

[13] Shayan, Mehranpoor and Naser, Mohammadzadeh and Hossein, Gharaee, "IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes," in 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), IEEE, 2019, pp. 114--121.

[14] He, Debiao and Kumar, Neeraj and Lee, Jong-Hyouk and Sherratt, R Simon, "Enhanced three-factor security protocol for consumer USB mass storage devices," IEEE Transactions on Consumer Electronics, vol. 60, no. IEEE, pp. 30--37, 2014.

[15] Shouran, Zaied and Ashari, Ahmad and Priyambodo, Tri, "Internet of things (IoT) of smart home: privacy and security," International Journal of Computer Applications, vol. 182, pp. 3--8, 2019.

[16] Hern{\'a}ndez-Ramos, Jos{\'e} L and Bernabe, Jorge Bernal and Moreno, M and Skarmeta, Antonio F, "Preserving smart objects privacy through anonymous and accountable access control for a m2m-enabled internet of things," Sensors, vol. 15, no. Multidisciplinary Digital Publishing Institute, pp. 15611--15639, 2015.

[17] Benenson, Zinaida and Gedicke, Nils and Raivio, Ossi, "Realizing robust user authentication in sensor networks," Real-World Wireless Sensor Networks (REALWSN), vol. 14, p. 52, 2005.

[18] Banerjee, Satyajit and Mukhopadhyay, Debapriyay, "Symmetric key based authenticated querying in wireless sensor networks," in Proceedings of the first international conference on Integrated internet ad hoc and sensor networks, 2006, pp. 22--es.

[19] Komninos, Nikos and Philippou, Eleni and Pitsillides, Andreas, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," IEEE Communications Surveys \& Tutorials, vol. 16, no. IEEE, pp. 1933--1954, 2014.

[20] B. Fan, "Analysis on the security architecture of zigbee based on ieee 802.15. 4," in 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), IEEE, 2017, pp. 241--246.

[21] Koyuncu, Murat and Pusatli, Tolga, "Security awareness level of smartphone users: An exploratory case study," Mobile Information Systems, no. Hindawi, 2019.

[22] Yoon, Seokung and Park, Haeryong and Yoo, Hyeong Seon, "Security issues on smarthome in IoT environment," in Computer science and its applications, Springer, 2015, pp. 691--696.

[23] D. Schwarz, "The Current State of Security in Smart Homes Systems," SEC Consult Vulnerability Lab, Vienna, 2016.

[24] Kang, Won Min and Moon, Seo Yeon and Park, Jong Hyuk, "An enhanced security framework for home appliances in smart home," Human-centric Computing and Information Sciences, vol. 7, no. Springer, pp. 1--6, 2017.

[25] Armando, Alessandro and Basin, David and Boichut, Yohan and Chevalier, Yannick and Compagna, Luca and Cu{\'e}llar, Jorge and Drielsma, P Hankes and H{\'e}am, Pierre-Cyrille and Kouchnarenko, Olga and Mantovani, Jacopo and others, "The AVISPA tool for the automated validation of internet security protocols and applications," in International conference on computer aided verification, Springer, 2005, pp. 281--285.

[26] Burrows, Michael and Abadi, Martin and Needham, Roger Michael, "A logic of authentication," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 426, no. The Royal Society London, pp. 233--271, 1989.

[27] Amin, Ruhul and Islam, SK Hafizul and Kumar, Neeraj and Choo, Kim-Kwang Raymond, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," Journal of network and computer applications, vol. 104, no. Elsevier, pp. 133--144, 2018.

[28] Jung, Jaewook and Kim, Jiye and Choi, Younsung and Won, Dongho, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," Sensors, vol. 16, no. Multidisciplinary Digital Publishing Institute, p. 1299, 2016.

[29] "An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks," Sensors, vol. 16, no. Multidisciplinary Digital Publishing Institute, p. 837, 2016.

[30] Chang, Chin-Chen and Le, Hai-Duong, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," IEEE Transactions on wireless communications, no. IEEE, pp. 357--366, 2015.

[31] He, Debiao and Zeadally, Sherali, "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," IEEE internet of things journal, vol. 2, no. IEEE, pp. 72--83, 2014.

[32] Farash, Mohammad Sabzinejad and Turkanovi{\'c}, Muhamed and Kumari, Saru and H{\"o}lbl, Marko, "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, no. Elsevier, pp. 152--176, 2016.

Hossein Gharaee received B.Sc. degree in electrical engineering from K.N. Toosi University of Technologhy in 1998, M.Sc., and Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2000 and 2009 respectively. Since 2009, he has been with the Department of Network Technology in ICT Research Institute (ITRC). His research interests include VLSI with emphasis on basic logic circuits for low-voltage low-power applications, DSP, crypto chip and Intrusion detection and prevention systems.

Fateme Shabani received the M.Sc. degree in information security from Tarbiat Modares University in 2016, where she worked on anonymous authentication protocols for Internet of Things. Her area of research interest is security protocols, particularly in the field of authentication protocols.

Naser Mohammadzadeh received the B.S. and M.S. degrees in computer engineering from Sharif University of Technology, Iran. He received the Ph.D. degree in computer engineering from Amirkabir University of Technology, Iran. He is currently an associate professor of computer engineering at Shahed University. His research interests include smart homes, optimization and quantum design automation.

Shayan Mehranpoor was born in 1994 in Tehran, Iran. He received her B.Sc. in Computer Engineering - Hardware from Shahed University, in 2016 and M.Sc. in Information Technology Engineering (Secure Computing) from Shahed University (Tehran Province, Iran), in 2019. Her master's thesis is in the field of IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Home. Her interests include Internet of Things, Smart home, Security Based on Biometric, Blockchain, machine learning.