

Edge internet of things based smart home passwordless authentication

Maha Helal¹, Abdullah Aldawsari¹, Mousa Al-Akhras², Bayan Abu Shawar³, Hani Omar⁴

¹College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

²King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

³College of Engineering, Al Ain University, Abu Dhabi, United Arab Emirates

⁴Faculty of Information Technology, Zarqa University, Zarqa, Jordan

Article Info

Article history:

Received Feb 18, 2024

Revised Aug 6, 2024

Accepted Aug 14, 2024

Keywords:

Authentication

Automated validation of internet security protocols and applications

Internet of things

Multifactor authentication

One-time passwords

Smart home

ABSTRACT

The internet of things (IoT) has transformed the way appliances and devices are connected and especially in the case of smart homes, in which smart devices can communicate through networks to improve everyday activities. However, it might be difficult to provide a high level of security for the data produced by these devices. Current security mechanisms might not always function adequately in all circumstances, especially when the number of devices increases. This research proposes an edge IoT-based smart home authentication scheme that adopts IPv6. For devices that use a smartphone application, it also offers a passwordless user authentication approach through the use of the smartphone ID and biometrics. The proposed authentication scheme was simulated to verify its ease of use and security. Security and cost analysis was also performed by reviewing and comparing the proposed scheme with previous research on IoT authentication systems. This research finds that the proposed authentication scheme is efficient at shielding home IoT networks from possible attacks, as well as maintaining a high level of usability.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Maha Helal

College of Computing and Informatics, Saudi Electronic University

Riyadh 11673, Saudi Arabia

Email: mhelal@seu.edu.sa

1. INTRODUCTION

The internet of things (IoT) has been identified as the next reasonable evolutionary expansion stage of the Internet into the physical world. IoT is the widespread connection of devices capable of interacting with one another and sharing data to a more extensive network, from which the shared data may be used to extract value. Each device must have a unique identifier and relies on embedded technology to detect and collect data about itself and its surroundings and transmit them to other devices or hosts. However, the expansion of IoT renders the local network behavior alien to traditional network administrators [1]. Subsequently, these devices, and their data, must be connected and examined to make better informed judgments. While the technological hurdles are intriguing in and of themselves, from an industrial and business standpoint, IoT represents tremendous potential to harness untapped data and knowledge to revolutionize and construct new industrial processes and business models.

Previous research has identified that various definitions of IoT exist in different contexts. For instance, i) Gartner [2] defines IoT as a “network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment”; ii) IBM [3] refers to IoT as “a network of physical devices, vehicles, appliances, and other physical objects that are embedded

with sensors, software, and network connectivity, allowing them to collect and share data”; and iii) the International Data Corporation (IDC) [4] refers to IoT as “a network of uniquely identifiable endpoints (or things) that communicate without human interaction using IP connectivity” [5].

Research in 2021 forecast that the number of connected IoT devices would reach 35.82 billion worldwide that year and 75.44 billion by 2025 [6]. The impact of IoT is predicted to be astonishing in the near future and the increasing connectedness will radically alter how users interact with everyday items. More decisions may be made based on evidence, rather than intuition or habit, and data-driven decision making will prove to be more efficient and lucrative in everyday operations. Industry processes and systems will be better controlled and monitored, increasing overall safety. Quality of life will also rise as a result of the time, money, and energy savings associated with these improvements. New services may also be developed in the resulting data-rich environment, enhancing human well-being [5].

A business that adopts IoT can expect improved security, efficiency, and convenience. Hazardous settings and workplaces can be more precisely quantified, and risks can be controlled more easily. Increased knowledge about working circumstances enables choices to enhance comfort and, as a result, productivity. For example, a more localized thermostat may indicate temperature variances between the different areas in certain workplaces. Adjusting the temperature or lighting in places that are being used could also lower energy expenditure and increase efficiency. Monotonous activities could be automated, resulting in less downtime and increased productivity, accuracy, and outcomes. Leveraging these advantages enables employers to increase employee satisfaction and retention, which could result in increased revenues and a reduction in the investment involved in staff turnover [5]. Another possible use of IoT technology is in the home, for the purposes of improving the quality of life, greater spending efficiency, and increased control of resources. Edge-based IoT computing connects smart devices, products, and appliances to the Internet to improve the consumer experience.

Without a doubt, each change brings with it both rewards and obstacles that must be faced. For instance, security poses a challenge in the realm of IoT. It is essential to establish and maintain principles and functionalities that ensure a network’s functionality. This includes implementing measures such as authentication, confidentiality, end-to-end security, and integrity [7]. With the growth of technology and its widespread use, there is an increasing need for secure methods of communication and password storage [8]. Despite the advancements in internet-connected devices, online account passwords are still vulnerable to theft, cracking, and hacking. It is even possible for fraudsters to purchase user credentials from online media platforms. Numerous data breaches have occurred globally, affecting many international organizations. Therefore, passwordless authentication facilitates a more secure online account login [9], [10].

With regard to the advancements in smart home (SH) technologies, IoT data must be protected to ensure a high level of security and reasonable reliability. Due to the increasing number of IoT devices, however, current addressing systems and security protocols may not always work effectively, which leads to security vulnerabilities. Throughout the development and operation of devices and hubs, prioritizing security measures is paramount, including availability, authentication, and key management. Enhancing authentication methods can provide a safe, user-friendly, and convenient environment for all types of users who wish to use SH IoT systems.

This research contributes to the body of knowledge by proposing a multifactor passwordless secure authentication scheme. The proposed scheme adopts internet protocol version six (IPv6) and provides a one-time password (OTP), biometric authentication, user and device identification, and an encryption key. By doing so, the scheme aims to address a balance between security versus usability, which means increasing security while reducing complexity. In addition, the proposed scheme ensures a one-time setup mechanism, as well as enabling biometric verification in mobile phones and eliminating the use of passwords through a passwordless authentication method.

The rest of the paper is organized as follows. Section 2 discusses related work. This is followed by the details of the methodology in section 3. Section 4 presents the experimental results and related discussion. Section 5 concludes this work and offers directions for future work.

2. RELATED WORK

IoT is an emerging concept that is increasingly being adopted in the contemporary wireless telecommunications landscape. The underlying principle of this concept is the ubiquitous existence of diverse entities or artifacts, including radio-frequency identification (RFID) tags, sensors, actuators, and mobile phones. These entities possess the ability to engage in interactions and collaborate with neighboring entities to achieve shared objectives through distinct addressing mechanisms [11].

The fundamental advantage of IoT idea lies in its substantial impact on various aspects of everyday life and the behavior of potential consumers. IoT is expected to have significant implications for both professional and domestic domains, as perceived by individual users. In the given context, potential

application scenarios in the near future, such as home automation, assisted living, e-health, and enhanced learning, represent a limited selection of examples wherein the new paradigm is expected to have a substantial impact. From the standpoint of a business user, the value of this phenomenon is particularly evident in various fields, including automation and industrial production, logistics, business/process management, and the intelligent transportation of people and things [11]. Furthermore, IoT can be used to develop smart cities, smart grids, and intelligent logistics [12].

The Internet has made progress over the years by connecting billions of nodes worldwide. These nodes come in various sizes and with different capabilities and computing capacities, enabling them to support a wide range of possible applications. As a result, the traditional Internet evolved into IoT, which can now connect objects and incorporate intelligence into the system to analyze specific data from objects intelligently and make autonomous decisions that are beneficial. Therefore, IoT has the potential to create applications and services that users could not previously have imagined [13].

As stated earlier, IoT does not have a unified agreed-upon definition. Rather, different groups, such as academics, researchers, practitioners, innovators, developers, and business executives, have offered their own interpretations of the concept. However, the notion of IoT is commonly attributed to Kevin Ashton, a specialist in innovation. Although these groups have different definitions, they all agree that the initial iteration of the Internet primarily revolved around data produced by humans; the next version revolves around data generated by objects [14]. A comprehensive description of IoT is that it is a network of devices that can organize themselves autonomously. These devices are capable of exchanging information and resources among themselves, whereby they can respond and adapt to events and changes in their environment [14]. Interestingly, the concept of IoT went through a series of important key events, as summarized in previous research [15].

The concept of IoT has become increasingly popular and widely discussed in the information technology industry. Over the past decade, for example, IoT has gained attention for its vision of a network in which physical objects can be connected and communicate with each other at any time and from anywhere [16]. By assigning an identifier to each object, IoT creates a network that facilitates communication between humans, between humans and objects, and between the objects themselves, essentially connecting everything in the world [17]. Use of IoT envisions a future in which almost everything can be interconnected and communicate intelligently. Whereas users usually associated a “connection” with devices such as servers, laptops, tablets, and phones, IoT takes it further by connecting sensors and actuators embedded in objects such as roads or pacemakers through wired or wireless networks, and sometimes using the internet protocol (IP) to connect to the Internet. The data collected by these networks are then sent to computers for analysis. When objects can perceive their surroundings and communicate within them, they become tools for understanding complexity and responding quickly.

This technological advancement has improved many aspects, as it involves the implementation of information systems that can function independently. In practice, IoT refers to the process of coding and connecting everyday objects so that they can be easily identified and tracked using the internet [17]. A major part of the existing content related to IoT has been developed using RFID tags and IP addresses, which are connected to a network [18].

The idea of the smart home began in the late 1960s, when computer enthusiasts, such as Jim Sutherland, began installing computers in their homes for various reasons [19]. When personal computers became widely available in the late 1970s, the on-site control and automation of household appliances attracted enthusiasts. At a time when a domestic Internet service was not yet widely accessible, remote control was accomplished via decoding dual-tone multi-frequency signals sent over telephone lines [19]. Although research into smart homes has advanced, actual use remains very limited. Greichen [20], the development of the SH market came after a decade of study and deployment. Although it is anticipated that other needs may emerge as the concept of the smart home matures, the key requirements determined in previous research include heterogeneity, self-configurability, extensibility, context awareness, usability, security and privacy protection, as well as intelligence [19].

Stallings *et al.* [21] noted that insufficient confidentiality, integrity, and security of data in IoT can potentially jeopardize the technology’s broad adoption. As discussed before, securing IoT devices is further exacerbated by their resource-constrained nature, which suggests that solutions for attack mitigation and privacy protection that operate on conventional networks cannot easily be implemented on IoT networks. Once an IoT device is hacked, the attacker can also control how the device routes and forwards information. In addition, by targeting network devices, attackers can gain access to data collected and transmitted by IoT devices.

Digital user authentication establishes trust in user identities supplied to an information system electronically. The authenticated identity may be used to assess if the authenticated person is permitted to execute certain duties. There are four distinct methods for verifying a user’s identity, which may be used

alone or in combination: i) something the person knows, ii) something the person possesses, iii) a physical characteristic of the person (*i.e.*, static biometrics), and iv) a characteristic of something the person does (*i.e.*, dynamic biometrics). Where more than one method is used, this is referred to as multifactor authentication. The effectiveness of authentication systems depends on the number of elements they incorporate. Implementation with two factors is considered stronger than that with one factor, and implementations with three factors are believed to be even stronger [21]. Numerous studies have been conducted on authentication systems. Each study explored authentication from a variety of perspectives. For instance, one comprehensive overview of existing researcher schemes considered criteria and commonalities [22].

In assessing what a person knows, one study [12] compared various authentication schemes and discussed in detail the authentication scheme presented in another paper [23], which presented the idea of having a control server for multiple cloud servers. The control server would ensure authentication when the cloud servers were spread out. To assess the authentication, password, and identity management capability, the researchers implemented six procedures: cloud server registration, user registration, registering for an account, authentication, resetting and updating the password, and altering one's identity.

Another authentication scheme proposed a resource-efficient secure remote user authentication (SRUA-IoT) strategy for the internet engineering task force's IPv6-over-LoWPAN (6LoWPAN)-based IoT networks [24]. The proposed approach authenticates users before obtaining real-time data from sensors deployed in 6LoWPAN-based IoT networks. The technique accomplishes the authentication and key establishment procedure by using a lightweight, secure hash algorithm (SHA-160) and an advanced encryption standard (AES-192).

A novel remote user authentication (RUA) technique for using smart cards to authenticate users in wireless sensor networks has also been discussed [25]. The researchers found that smart cards could authenticate and operate IoT devices by calculating a session key from the authentication key. In the same context, other research proposed an authentication scheme based on RUA for cloud-IoT applications [26], [27]. The system's security defenses have six stages: pre-computation, registration, login, authentication, password change, and smart card revocation.

Kumar and Chouhan [28] propose a smart card-based secure addressing and authentication (SCSAA) method that uses smart cards to give SH appliances and devices individual addresses. The main contribution of their work is divided into two parts: secure addressing and secure authentication. Their method uses a good balance between an addressing scheme and an authentication scheme that adopts the mobile IPv6 and a secure scheme utilizing multifactor authentication via a smart card, password, and biometrics. Their method focuses on SH IoT applications and how to allow remote users to control IoT devices securely. A distinctive identifier is the modified unique 64-bit interface ID (IID). For authentication purposes, the identification is saved on the user's smart card, the edge server, and the home server. The edge server receives requests from users for access to SH devices and appliances by encapsulating the IID bits in each packet, which contains the packet's final 64 bits of the IPv6 format.

Subsequently, when a user requests a packet, the edge server retrieves the IID bits from that packet and checks them against the unique identification pre-stored in the edge server database. The home server stores this 64-bit object during the registration process and sends it to the user end via a smart card. Kumar and Chouhan [28] login authentication phase is triggered when the user receives the smart card and session key. The login and authentication procedure are based on multifactor authentication, which includes three characteristics: first, something you know (the password); second, something you are (biometrics); and third, something you have (the smart card).

The authentication scheme proposed in the current paper is an enhancement of Kumar and Chouhan [28] scheme, which was proposed to enable edge IoT-based SH devices to manage authentication by presenting the SCSAA method. In this research, the smart card model is enhanced through a mobile phone by adding an extra layer of protection, an OTP, while maintaining better user usability by utilizing the encryption method through a user authentication server (UAS) to provide a much more convenient passwordless authentication methodology. Therefore, this research proposes a multifactor passwordless secure authentication scheme that uses IPv6 and will provide an OTP, biometric authentication, user and device identification, and encryption key for passwordless authentication.

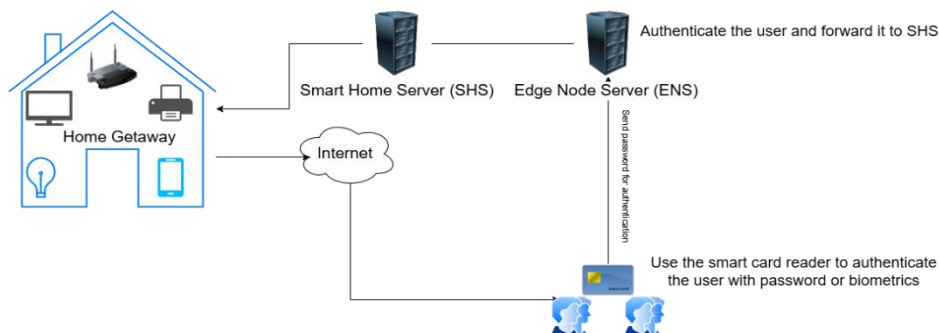
3. METHOD

As stated earlier, this research builds on Kumar and Chouhan [28] scheme. However, instead of using a smart card, the proposed authentication depends on the mobile phone subscriber identity module (SIM) card for user registration. It also relies on a mobile authenticator application to provide login authentication using OTP or biometrics, which can be limited by the smartphone capability of either fingerprint or face recognition. As shown in Figure 1, the main difference between Kumar and Chouhan [28] scheme and the scheme proposed in this research is mobile phone enablement, which will increase the

usability and security of using and controlling SH devices and entities. The proposed authentication scheme has five main components:

- Home gateway: Enables the device to connect to the Internet in a home network.
- UAS: Stores user information such as mobile device ID, user ID, IP address, and a public key for authentication purposes.
- Edge node server (ENS): Acts as a centralized server for controlling and monitoring aspects of the SH system.
- Smart home server (SHS): Assigns addresses and identifies all SH devices/appliances. It also handles the encryption and decryption of data packets. New users can only register once they are successfully validated by the SHS.
- Smart home mobile application: Serves as the platform upon which users interact and communicate with the SHS and their connected devices.

Kumar and Chouhan's original authentication [28]



Proposed Authentication

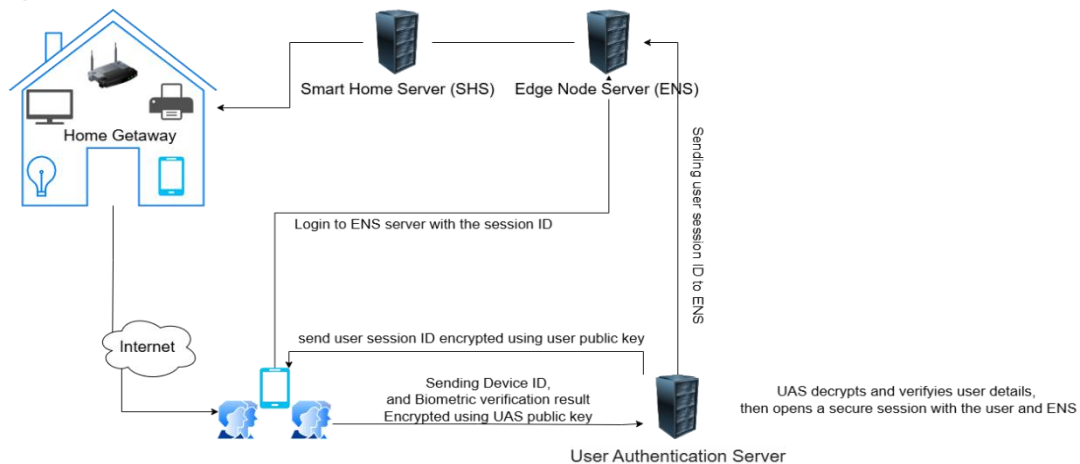


Figure 1. Comparison of Kumar and Chouhan [28] authentication approach and the proposed scheme

As suggested in Figure 1, Kumar and Chouhan [28] authentication scheme consists of six phases: initial phase, addressing phase, registration phase, login authentication phase, session agreement phase, and password update phase. The proposed authentication scheme uses both the initial phase and the addressing phase without any modifications. However, as the proposed solution is a passwordless authentication scheme, the last phase was removed. In addition, the registration, login, and session agreement phases were enhanced as follows.

3.1. Summary of the enhancement of the registration phase

In the proposed authentication scheme, the user makes a request to the SH mobile application via the user's SIM card, whereby the UAS receives the registration request and sends an OTP asking for user verification. The OTP will expire after 60 seconds if the user is not verified. The SH mobile application will send the device ID and the user's public key for future passwordless authentication.

3.2. Summary of the enhancement of the login authentication phase

As explained in the registration phase, the user will use a registered mobile phone for any further user login attempts to the SH network. In the login phase, the user will perform the following steps:

- a. The user will log in through the SH mobile application and send the registered public key to the UAS along with the biometric verification result from the mobile phone. The UAS will verify the information received. If it is not correct, the UAS will send an error message to the user. If it is correct, the UAS will generate a new session with an expiry time limit of 60 seconds, then encrypt it using the user public key, and send the session information to the user.
- b. The user will decrypt the message using a private key, then take the session ID and initiate a connection with the ENS that has the user device ID before the session expires.
- c. The ENS will validate the session from the UAS and add the user device ID to the 56-bits in the addressing scheme to allow the user access to the SH devices/appliances and save the session in detail in the SHS.

The biometric verification cannot be misused due to the Google Android or Apple iOS mobile phone operating system [29]. The application must include a safeguard or encryption to protect biometric data from fraudster attacks, robust registration procedures, and policies to protect data during transmission to and storage on computer servers and to strengthen biometric authentication. The algorithm also examines whether the screen has remained static over a certain period of time. When the user logs out or the time limit expires, the system re-authenticates the user using that individual's fingerprint, and the user can set the session timeout according to preference [30].

3.3. Summary of the enhancement of the session agreement phase

This phase shows how to safeguard network connections and construct a session key agreement using shared session keys. After registration, addressing, and login authentication, the session key agreement stage protects IoT network privacy and security via pseudo-identities [28]. The user retrieves the prior session key from a message and verifies the identity with the SH mobile app. Valid sessions continue and invalid sessions are discarded.

4. RESULTS AND DISCUSSION

This section discusses how the proposed authentication scheme behaved when various types of attacks were detected. The section then analyzes the performance of the proposed authentication scheme and provides a comparative analysis between the existing authentication scheme and the proposed one.

4.1. Simulation configuration and setup

Automated validation of internet security protocols and applications (AVISPA) is a tool that aims to evaluate internet security protocols and applications. It utilizes the high-level protocol specification language (HLPSL) for encoding. HLPSL is a modeling language specifically designed for security protocols and communication. It defines the characteristics of each participant in a scenario with each role being distinct from the others. Roles receive data from parameters and communicate with other roles through channels. The HLPSL2IF converter is used to convert an HLPSL protocol into a standard intermediate format (IF). This IF standard serves as input to one of four backends: i) On-the-fly model-checker (OFMC), ii) Tree automata based on automatic approximations for the analysis of security protocols (TA4SP), iii) Constraint-logic-based attack searcher (CL-AtSe), or iv) SAT-based model checker (SATMC). These backends generate an output format (OF) based on their analysis.

The proposed scheme also adopts the well-known Dolev-Yao (DY) threat model [28], which originated in 1983 and is still commonly used in protocol evaluation. In this model, the network is shown as a star, with the attacker as the center node. Accordingly, all communication is mediated by the attacker, who can alter messages, prevent them from reaching their intended destination, or deliver them intact [30]. Under the DY model, opponents can execute a wide variety of different assaults. The opponent employs an aggressive or passive assault that severely compromises the system and could also counterfeit, alter, or delete the communication received.

In the proposed scheme, roles are considered in the system, including the User, ENS, SHS, and UAS. Utilizing the DY threat model, several phases are evaluated on HLPSL using the sharing of a session key (SK) in the proposed scheme. To ensure security, the proposed scheme's roles are assessed using the AVISPA tool with CL-AtSe backends. This allows trusted users to validate security in the presence of attackers and prevents replay attacks. The protocol script is designed in such a way that these attacks cannot compromise security. By utilizing the CL-AtSe model checker, all defined roles meet the requirements. Figures 2(a) and 2(b) present a screenshot from the simulation illustrating how each session and environment

role is implemented in HLSPL inside the AVISPA tool. CAS+ language is also used to make the formulation and verification of security protocols simple and straightforward.

```

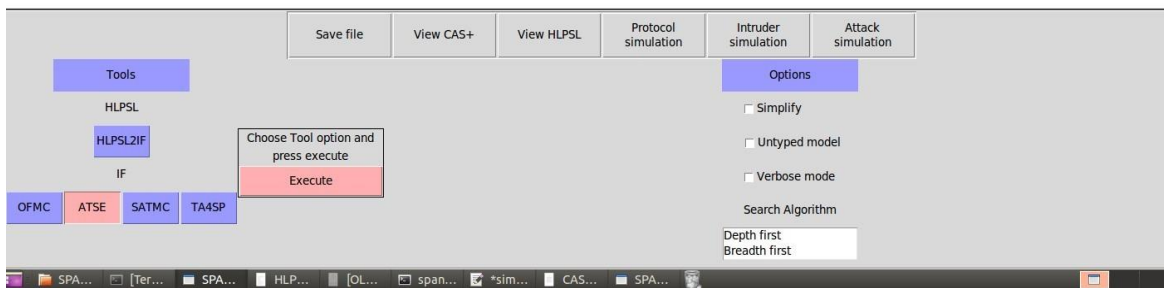
protocol simple;
identifiers
U, ENS, SHS, UAS : user;      %%% Declare all values, agent and keys occurring in the "messages" section
Uid, Sid         : number;    %%% Variable names should start by a capital letter.
H                : function;

messages
1. U -> UAS : U,Uid
2. UAS -> ENS : H(Uid)
3. UAS -> U : Sid
4. U -> ENS : Sid
5. ENS -> SHS : H(Sid)

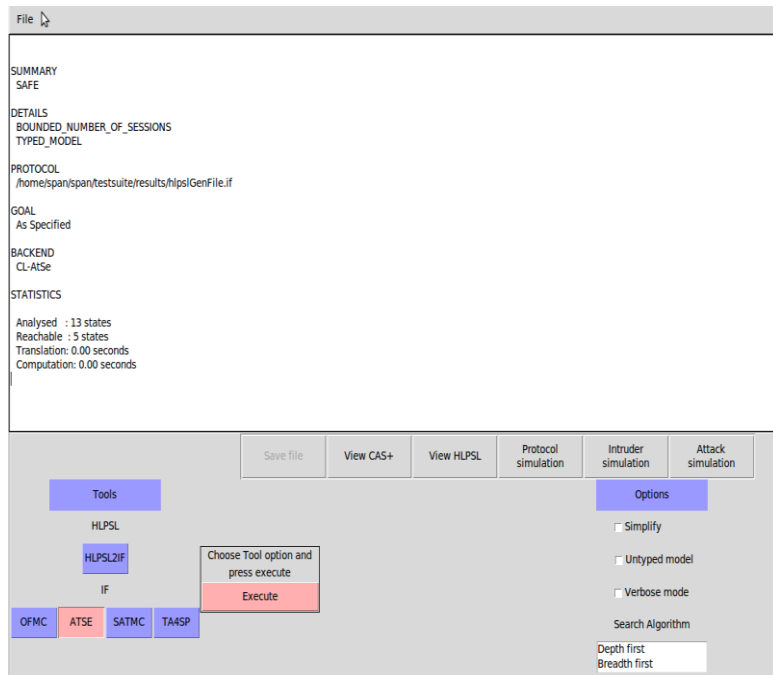
knowledge
U      : U, UAS, ENS, Sid, Uid;
UAS    : U, ENS, Uid, Sid;
ENS    : U, SHS, UAS, Sid;
SHS    : SHS, ENS;

session_instances
[U:users, UAS:authenticationserver, ENS:edgenode, SHS:homeserver, Uid:uid, Sid:sid]

[U:i, UAS:authenticationserver, ENS:edgenode, SHS:homeserver, Uid:uid, Sid:sid]
;
intruder_knowledge
users,authenticationserver,edgenode,homeserver,isd; %%% the intruder knows alice,bob,
    
```



(a)



(b)

Figure 2. Simulation illustrating how each session and environment role is implemented in HLSPL inside the AVISPA tool (a) CAS+ implementation of the proposed protocol and (b) AVISPA test result in AtSe

4.1.1. User role

The user role describes how the user interacts with the SH environment and how the user authenticates and connects the home devices, such as lights, security cameras, and sensors, securely. The user

starts the connection by sending an authentication request to the UAS, providing user details: username, user identity, and device identity. The UAS reacts to the request initiated by the user to verify his/her fingerprint using smartphone biometrics. The user sends the biometrics verification to get a session ID from the UAS to utilize with the ENS.

4.1.2. UAS role

The UAS is responsible for creating the user session ID, which is vital to the user being able to control the SH devices. The UAS is also responsible for managing authentication and authorization. The goal of having the authentication server on separate components is to separate this critical function from other roles, which will grant a better security layer. In Kumar and Chouhan [28] authentication scheme, the authentication is combined with the ENS, so the ENS is responsible for both controlling and monitoring the SHS and authenticating the users. Segregating the two roles into different components or servers will grant better security. In the case that the ENS is compromised, the user information will remain safe in the UAS and in the case of an intruder compromising the UAS, the ENS can still monitor and control the SHS without being affected by an intruder in the UAS.

4.1.3. ENS role

The role of the ENS is to act as a stage between the UAS and the SHS. The ENS controls and monitors the SHS and provides information to the SHS about the user. This information includes the user session ID, IP address, device ID, and whether the authentication status is valid or invalid.

4.1.4. SHS role

The SHS is the closest layer to the SH devices, such as lights, televisions, air conditioning units, printers, and closed-circuit television. The SHS has a direct connection to the smartphone user. Once the user has an active and valid session ID, the user will utilize the session ID to communicate with the SHS and control and automate the home environment remotely and securely. The SHS utilizes an excellent authentication scheme and very confined methods so SH users can access the devices remotely and securely and then utilize the home server components.

4.2. Security analysis of the proposed authentication scheme

There are various types of attacks that could compromise the security of SH environments. This section presents the most widely known types of attacks. It discusses how the proposed authentication scheme could interact with different types of attacks.

4.2.1. Man-in-the-middle (MITM) and denial-of-service (DoS) attacks

An intruder could be between any two components in the proposed authentication scheme. All the data transmitted between the proposed scheme are encrypted. The only side the attacker can invade is if the intruder finds the session key. In that case, the attacker can use the session key to communicate with the SHS and hack the SH devices. The proposed authentication scheme solves this issue by utilizing the timestamp condition, which will be calculated: if the timestamp is in the range, that means the connection is legitimate; otherwise, the connection is dropped.

In the instance that an attacker forges information and then uses a secret key to send a request to the home server, the intruder initiates the request and sends it to the SHS. The SHS then verifies the timestamp and analyzes if they are the same, in which case the transaction is accepted; otherwise, it is rejected. Once the request reaches the SHS, the SHS verifies the SK, which is the session key for the SHS, and verifies its session key ID. A timestamp condition does not satisfy the upper limit requirement of the timestamp if an attacker compromises the verification procedure, as shown in the following equation: $[(T2 - T1) \leq \Delta T]$ where $T2$ and $T1$ are the first and second instances. If $T2$ and $T1$ are in the accept state, both can authenticate and communicate messages with each other securely. Similarly, in a DoS attack, if the attacker starts sending an enormous number of requests that do not match the timestamp condition, the system will drop the connection.

4.2.2. Impersonation attacks

Impersonation attacks can happen in three different ways: i) user impersonation; ii) SHS impersonation; and iii) device impersonation. For a user impersonation attack, the intruder computes the identities, such as authentication biometrics, user ID, or device ID, and calculates the current timestamp. However, with the proposed scheme, all the requests will fail since the identities of the device and the user are continuously updated because of the timestamp condition, and the value of the identity is regenerated randomly every time and, therefore, the intruder cannot detect it.

In the case of an SHS impersonation attack, the attacker attempts to decipher an authentication message. The attacker also calculates the timestamp and makes this request on behalf of the SHS to the user end as the following $IID = h(IID_{intruder}) || IID_d, Function = h(Biometric)$. The user validates the attacker's authentication request. However, the secret key and timestamp are not computed using real keys. The computational keys and secret credentials of the SHS cannot be guessed. Finally, the attacker is capable of violating security; however, the proposed scheme protects confidentiality against this threat.

In the case of a device impersonation attack, the intruder attempts an authentication message by $B = h(ID_{user} || random\ N || Time || SK)$. Subsequently, the intruder calculates the timestamp and then sends an authentication request to the user that is pretending to have originated from the SHS. The user will verify the authentication request as the following $h(ID_{user} || random\ N || Time || SK)$. However, the timestamp and secret key are not computed using the actual keys. It is impossible to guess the session key and, therefore, even if the attacker breaches the system, the proposed scheme will still be maintained.

4.2.3. Anonymity and untraceable attacks

Anonymity and untraceable attacks occur when an attacker passively listens to the network, without any interaction. Assuming that the attacker sniffs traffic between the user and the UAS, the attacker will not be able to read the messages since the traffic is encrypted by the user identity. A random number is generated every time, which will make decrypting the messages impossible for an intruder. Therefore, if an attacker breaches the network, the proposed scheme will protect the privacy of the user's information and messages. In the instance that an intruder observes and eavesdrops on the communications between the trusted user and the SHS, all messages are computed using a secret pseudo-identity and a random number generator, making eavesdropping impossible. Using a timestamp with each requested packet will enable such assaults to be resisted and retain anonymity and addresses the fear of an attack being untraceable.

4.2.4. Device compromise attacks

An attacker may also conduct device compromise attacks by capturing user devices and then attempting to steal their secret parameters and unique IID bits. The attacker then transmits a login request to the SHS ($ID_{intruder}$, ID_{device} , ID_{user} , and biometrics). The SHS validates the request and computes the variable from the IDs. However, the SHS will reject an unauthorized request since the attacker did not use the trusted user and device secret identities, which only the trusted user knows. Existing techniques do not offer security against device compromise attacks; however, the proposed authentication scheme can provide security against this type of attack such that an attacker cannot circumvent the authentication process. The advantages of the proposed authentication scheme, especially in device compromise attacks, come from having several layers of authentication and multiple identities.

4.2.5. Replay attacks

An attacker may intercept all communication, acquire secret parameters, and then launch a replay attack by transferring all the identities stored in the user's smartphones, such as 56-bit-IID and 8-bit-IID at timestamp T_1 to the SHS. A replay attack cannot be attempted due to the verification of the message timestamp and the time interval $[(T_2 - T_1) \leq \Delta T]$, where T is the mutually agreed-upon upper limit between the trusted entities. This time-sensitive condition applies to all messages received during the conversation. Finally, the SHS computes a time-bound token, rejects the attacker's token, and denies session key access. The benefits of having a mutually agreed time are crucial in the proposed authentication scheme, since it makes the authentication unique and secure and provides a defense against multiple attacks.

4.3. Analysis of the performance of the proposed authentication scheme

Similarly to the security analysis above, this section discusses the performance analysis of the proposed authentication scheme. This will help in determining the feasibility of the proposed scheme through a functional comparison and by considering the communication costs. Further details are discussed below.

4.3.1. Functional comparison

The security functionality of the proposed scheme was compared to Kumar and Chouhan [28] authentication scheme. The proposed authentication scheme utilizes the benefits of the biometrics authentication in a smartphone, which provides convenient and enhanced security for the SH user. The convenience of the proposed authentication scheme and its security are a result of the segregation of the authentication server. By placing the UAS between the user and the ENS, this step plays a vital role in segregating the control of the monitoring from the authentication.

The proposed scheme allows for multiple layers of control that provide defense in depth. After segregating the authentication service from the control and monitoring service, the scheme obtains strong in-

depth security by changing the architecture. However, adding an authentication server in a different component will result in higher costs, as more resources are needed. Furthermore, this will result in higher latency, mainly if the session is not generated, because the user will wait for the session creation and to be granted access in the ENS and on the user side.

4.3.2. Communication cost

The proposed scheme assumes that smartphone-based identities are a factor, which includes user biometrics and unique identification bits for both the user and the device. Smartphone IDs are included in each packet without increasing its size or the overhead. The proposed scheme utilizes the parameters as existing schemes to calculate the communication cost of the designed protocol. For example, the gateway identity is 32 bits, the timestamp is 32 bits, the hash is 32 bits, and the session key (SK) is 32 bits. A nonce r and XOR operation also take up 32 bits and the length of the shared keys is 160 bits. In the proposed scheme, three messages are used for authentication and login purposes compared to five messages in similar schemes. This reduces the communication cost to 959 bits, which is significantly lower than that of previous methods.

4.4. Summary

As previously mentioned, the aim of this research is to increase the security of edge IoT-based SH networks while reducing complexity to achieve a higher usability level. It can clearly be seen in the analysis of the security comparison that the proposed authentication scheme can handle different types of attacks. It also proved its ability to provide a high level of protection to edge IoT-based SH networks. With regard to usability and the cost of implementing the proposed scheme, it was evident that the proposed scheme is capable of providing higher security functionality at a reasonable cost. The scheme also achieved a reduction in communication costs compared to previous schemes, which, in turn, makes it more feasible in real-world scenarios.

5. CONCLUSION

The primary objective of this research is to offer a method for the protection of a network from attackers and the provision of safe access to SH services while maintaining a very convenient user experience. In the proposed scheme, a smartphone offers biometric authentication to smart devices/appliances using their unique ID bits, allowing the server to identify them without resulting in extra expense. Moreover, the session key construction of secret keys and identities increases the network's resistance to various threats. The overhead costs of this scheme are identical to those of the conventional IPv6. The AVISPA-based security analysis given in this scheme ensures that this scheme is safe and achievable.

The collected findings suggest that the proposed authentication scheme offers greater security than the scheme provided by earlier scholars. The suggested scheme increases the security and enhances the usability of the home automation business. It allows home users to use home automation services from a remote place securely, without interruption from intruders. In addition, the strength of the proposed scheme is derived from the separation of the authentication server components. This provides higher security through the design of the SH environment, hence preventing several types of attacks and enhancing the security layers.

Three paths of research could be conducted in future work. The first path is to focus on enhancing the current authentication scheme by increasing the security and reducing the steps required for authentication to make it faster and more convenient. The second path is to start implementing the scheme in a real environment to demonstrate the results and measure whether the user experience is convenient or complex. It would also be instructive to attempt all the expected attacks and see the efficiency of the proposed scheme in practice. Finally, the third path is to apply the proposed authentication scheme in another sector, such as healthcare, which utilizes similar roles and persona.




REFERENCES

- [1] N. Alhindawi, "IoT based technique for network packet analyzer," *The International Arab Journal of Information Technology*, vol. 20, no. 4, pp. 678–685, 2023, doi: 10.34028/iajit/20/4/14.
- [2] "Internet of things (IoT)," *Gartner*, 2012. <https://www.gartner.com/en/information-technology/glossary/internet-of-things> (accessed May 1, 2024).
- [3] "What is the internet of things (IoT)?," *IBM*, 2024. <https://www.ibm.com/topics/internet-of-things> (accessed May 1, 2024).
- [4] C. Macgillivray, S. Rau, N. Turner, and A. Wright, "Overcoming challenges: best practices for IoT implementations," *White Paper, IDC*, 2016, Accessed: May 1, 2024. [Online]. Available: https://download.ni.com/evaluation/iot/IDC_Whitepaper.pdf
- [5] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, and F. S. Aliee, "IoT fundamentals: definitions, architectures, challenges, and promises," in *Intelligent Internet of Things*, Cham: Springer International Publishing, 2020, pp. 3–50.
- [6] C. Benitez, "The ultimate list of internet of things statistics for 2024," *Findstack by Soho Media Ltd*. <https://findstack.com/internet-of-things-statistics/> (accessed Mar. 21, 2024).




- [7] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec. 2015, pp. 336–341, doi: 10.1109/ICITST.2015.7412116.
- [8] O. O. Amoo, F. Osasona, A. Atadoga, B. S. Ayinla, O. A. Farayola, and T. O. Abrahams, "Cybersecurity threats in the age of IoT: A review of protective measures," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1304–1310, Feb. 2024, doi: 10.30574/ijrsra.2024.11.1.0217.
- [9] R. S. Chowhan and R. Tanwar, "Password-less authentication: methods for user verification and identification to login securely over remote sites," USA: IGI global, 2019, pp. 190–212.
- [10] "Passwordless authentication options for Microsoft Entra ID," *Microsoft Entra*, 2024. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless> (accessed Mar. 21, 2022).
- [11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
- [12] K. S. Roy and H. K. Kalita, "A survey on authentication schemes in IoT," in *2017 International Conference on Information Technology (ICIT)*, Dec. 2017, pp. 202–207, doi: 10.1109/ICIT.2017.56.
- [13] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *2012 10th International Conference on Frontiers of Information Technology*, Dec. 2012, pp. 257–260, doi: 10.1109/FIT.2012.53.
- [14] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of things (IoT): a literature review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.
- [15] S. Kuyoro, F. Osisanwo, and O. Akinsowon, "Internet of things (IoT): an overview," in *3rd International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM'2015), March 23-24, 2015 London (UK)*, Mar. 2015, pp. 23–24, doi: 10.15242/IEE.E0315045.
- [16] E. A. Kosmatos, N. D. Tselikas, and A. C. Boucouvalas, "Integrating RFIDs and smart objects into a unified internet of things architecture," *Advances in Internet of Things*, vol. 1, no. 1, pp. 5–12, 2011, doi: 10.4236/ait.2011.11002.
- [17] R. Aggarwal and M. L. Das, "RFID security in the context of 'internet of things,'" in *Proceedings of the First International Conference on Security of Internet of Things*, Aug. 2012, pp. 51–56, doi: 10.1145/2490428.2490435.
- [18] M. Graham and H. Haarstad, "Transparency and development: ethical consumption through Web 2.0 and the internet of things," *Open Development*, vol. 7, no. 1, pp. 79–112, 2011, doi: 10.7551/mitpress/9724.003.0007.
- [19] T. K. L. Hui, R. S. Sherratt, and D. D. Sánchez, "Major requirements for building smart homes in smart cities based on internet of things technologies," *Future Generation Computer Systems*, vol. 76, pp. 358–369, Nov. 2017, doi: 10.1016/j.future.2016.10.026.
- [20] J. J. Greichen, "Value based home automation for todays' market," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 3, pp. XXXIV--XXXVIII, 1992, doi: 10.1109/30.156666.
- [21] W. Stallings, L. Brown, M. Bauer, and M. Howard, *Computer security: principles and practice*, 2nd ed. USA: Pearson, 2012.
- [22] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in internet of things (IoT)," in *2017 1st Cyber Security in Networking Conference (CSNet)*, Oct. 2017, pp. 1–3, doi: 10.1109/CSNET.2017.8242006.
- [23] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, Jan. 2018, doi: 10.1016/j.future.2016.12.028.
- [24] G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker, and D. Al-Jumeily OBE, "A secure remote user authentication scheme for 6LoWPAN-based internet of things," *PLOS ONE*, vol. 16, no. 11, p. e0258279, Nov. 2021, doi: 10.1371/journal.pone.0258279.
- [25] S. Banerjee, C. Chunka, S. Sen, and R. S. Goswami, "An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards," *Wireless Personal Communications*, vol. 107, no. 1, pp. 243–270, Jul. 2019, doi: 10.1007/s11277-019-06252-x.
- [26] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *Journal of Information Security and Applications*, vol. 42, pp. 95–106, Oct. 2018, doi: 10.1016/j.jisa.2018.08.003.
- [27] G. Sharma and S. Kalra, "A lightweight user authentication scheme for Cloud-IoT based healthcare services," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. S1, pp. 619–636, Jul. 2019, doi: 10.1007/s40998-018-0146-5.
- [28] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 420–438, Jan. 2021, doi: 10.1007/s12083-020-00973-8.
- [29] I. T. E. J. Mohammed and Y. A. Mohamed, "A new system for user authentication using Android application," *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum, Sudan, 2021, pp. 1-5, doi: 10.1109/ICCCEEE49695.2021.9429637.
- [30] R. Bresciani and A. Butterfield, "Weakening the Dolev-Yao model through probability," in *Proceedings of the 2nd international conference on Security of information and networks - SIN '09*, 2009, pp. 293–297, doi: 10.1145/1626195.1626265.

BIOGRAPHIES OF AUTHORS






Maha Helal    received her PhD degree in information systems from the University of Salford in Manchester, UK. She also holds an MSc degree in managing information technology and a BSc degree in computer science. Currently, she is working as an assistant professor in the College of Computing and Informatics at the Saudi Electronic University. She was a guest editor for a Special Issue in the Journal of Decision Systems titled "Digital transformation". Her current research interests include IoT, big data, HCI, IS, AI and e-learning. She can be contacted at email: mhelal@seu.edu.sa.






Abdullah Aldawsari    obtained his BSc from King Saud University in Information Systems in the year 2016. He also received his MSc from the Saudi Electronic University and Colorado University in 2022. His research interests are in cybersecurity defense and internet of things (IoT). He can be contacted at email: is.aldawsari.abdullah@gmail.com.






Mousa Al-Akhras    obtained his B.Sc. and M.Sc. degrees in computer science from the University of Jordan, Amman, Jordan, in 2000 and 2003, respectively. He earned his Ph.D. degree in 2007 from De Montfort University, Leicester, UK. His Ph.D. specialization is artificial neural networks and communications. He was promoted to associate professor in 2012. From 2014 to 2022 he joined Saudi Electronic University (SEU) as the coordinator for M.Sc. in cyber security program. In October 2022, he returned to the University of Jordan. His research interests include problems in artificial neural networks and their applications in security, business, and health. He can be contacted at email: Mousa.akhras@ju.edu.jo.



Bayan Abu Shawar    holds a BSc and a master's degree in computer science from the University of Jordan, and a PhD from the School of Computing at the University of Leeds. Currently, she is an associate professor in the Cybersecurity Department in the College of Engineering at AL Ain University. Before Joining AL Ain University, she was an associate professor at Arab Open University in Jordan from 2004 until 2019. Her research interests include chatbots, natural language processing, information retrieval, artificial intelligence, question answering systems, cybersecurity, and learning management systems, and e-learning. She can be contacted at email: bayan.abushawar@aau.ac.ae.



Hani Omar    obtained his B.Sc. degree in computer science from Mutah University, Karak, Jordan in 2002 and received his M.Sc. in computer science from Albalqa Applied, Salt, Jordan in 2008. He earned his Ph.D. from National Chiao Tung University, Hsinchu, Taiwan in 2015. Currently, he is working as an assistant professor in the College of Information Technology at Zarqa University in Zarqa, Jordan. His current research interests include machine learning, and natural language processing. He can be contacted at email: h.omar@zu.edu.jo.