applied sciences

MDPI

Article

Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes

Vincent Omollo Nyangaresi [1], Zaid Ameen Abduljabbar [2,3,4,*], Keyan Abdul-Aziz Mutlaq [5], Junchao Ma [6,*], Dhafer G. Honi [2], Abdulla J. Y. Aldarwish [2] and Iman Qays Abduljaleel [7]

[1] Faculty of Biological & Physical Sciences, Tom Mboya University, Homabay 40300, Kenya
[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[3] Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
[4] Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 430074, China
[5] IT and Communication Center, University of Basrah, Basrah 61004, Iraq
[6] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[7] Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
* Correspondence: zaid.ameen@uobasrah.edu.iq (Z.A.A.); majunchao@sztu.edu.cn (J.M.)

Abstract: Highly sensitive information about people's social life and daily activities flows in smart home networks. As such, if attackers can manage to capture or even eavesdrop on this information, the privacy of the users can be compromised. The consequences can be far-reaching, such as knowing the status of home occupancy that can then facilitate burglary. To address these challenges, approaches such as data aggregation and signcryption have been utilized. Elliptic curve cryptography, bilinear pairing, asymmetric key cryptosystem, blockchain, and exponential operations are among the most popular techniques deployed to design these security solutions. However, the computational, storage and communication complexities exhibited by the majority of these techniques are too high. This renders these techniques unsuitable for smart home components such as smart switches and sensors. Some of these schemes have centralized architectures, which present some single points of failure. In this paper, symmetric key authentication procedures are presented for smart home networks. The proposed protocol leverages on cryptographic primitives such as one-way hashing and bitwise exclusive-Or operations. The results indicate that this scheme incurs the lowest communication, storage, and computation costs compared to other related state-of-the-art techniques. Empirically, our protocol reduces the communication and computation complexities by 16.7% and 57.7%, respectively. In addition, it provides backward key secrecy, robust mutual authentication, anonymity, forward key secrecy, and unlinkability. Moreover, it can effectively prevent attacks such as impersonation, session hijacking, denial of service, packet replays, man-in-the-middle, and message eavesdropping.

Keywords: anonymous; authentication; attacks; IoT; privacy; security; smart homes; symmetric key

Citation: Nyangaresi, V.O.; Abduljabbar, Z.A.; Mutlaq, K.A.-A.; Ma, J.; Honi, D.G.; Aldarwish, A.J.Y.; Abduljaleel, I.Q. Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes. *Appl. Sci.* **2022**, *12*, 12688. https://doi.org/10.3390/app122412688

Academic Editor: Christos Bouras

Received: 15 November 2022
Accepted: 8 December 2022
Published: 11 December 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

The Internet of Things (IoT) devices offer a myriad of services, such as smart lighting, remote surveillance, and door locking. A smart home is part of IoT application scenarios which comprises sensors, actuators, home appliances, and controllers that are accessed and controlled remotely. In smart homes, users may utilize various applications or voice commands to turn appliances on or off [1] or monitor temperature and humidity at home [2]. In so doing, smart homes potentially boost user comfort and quality of life. A typical smart home consists of Indoor Smart Devices (ISDs), users, Home Gateways (HGs), and Registration Authority (RA) which acts as a controller [2–4]. Here, the controllers

scrutinize sensor data before transmitting messages to home appliances for some action. Since smart home devices such as sensors are bandwidth, computational power, and memory constrained, remote users access sensor data via the home gateway. In essence, the HG offers long and short-distance wireless connectivity between the ISDs and remote users. For remote monitoring and access to the ISDs, users deploy internet-enabled tablets and smartphones [5] while the ISDs communicate with each other via Radio Frequency (RF) channels [6]. Before the actual deployment of smart home networks, all ISDs, gateways, and users are registered at the RA.

The goals of smart homes include a reduction in operational costs, increased energy efficiency, convenience, and comfort [2,5] through home systems automation. As such, massive information flows over smart home networks, which raises performance, privacy, and security issues [1,7]. This is because message exchanges take place over insecure public channels [1,2,8,9] and over longer distances, which increases latencies [7]. In addition, most ISDs do not incorporate security and privacy in their designs [10] or have weak embedded security [11]. Therefore, it becomes easy for attackers to tamper, eavesdrop and have unauthorized access to the transmitted data. It is also possible for adversaries to insert bogus messages and insert or delete exchanged data. Consequently, the preservation of perfect privacy and security in smart-phone, stored data, networks, and ISDs is paramount [9]. Unfortunately, much attention has only been paid to boosting the smartness of the devices and user comfort while little work is devoted to security and privacy issues [2]. Numerous security issues have been identified in smart home networks. These issues include a lack of proper user privacy, identity authentication, and access control [8,12–14]. These vulnerabilities have made it possible for attackers to deploy these networks to launch attacks such as Distributed Denial of Services (DDoS) [15] and spreading malware [11]. In addition, packet interception, deletion, modification, and bogus data injections are common [2].

To address the above security, performance, and privacy challenges, authentication of the communicating entities must be executed. This ensures that only authorized parties are able to establish connections to the smart home network [16–18]. It also helps in establishing the integrity of applications and devices. In addition, there is a need to preserve the confidentiality and availability of the exchanged messages [1]. Moreover, secure remote access can prevent disclosure of access privileges and private information [17] or illegal control of ISDs and subsequent illegitimate surveillance [19]. Therefore, many security solutions have been presented in literature based on techniques such as usernames and passwords and asymmetric and symmetric key crypto-systems. However, usernames and passwords are not effective for highly mobile IoT devices [17]. Similarly, most asymmetric and symmetric key techniques have high computational overheads, which are not ideal for ISDs [1]. Since the majority of the sensors deployed in smart homes are limited in terms of computation power [16,20], the authentication protocols need to be lightweight [2,19]. There is also a requirement to negotiate the session key among the communicating entities utilized to encrypt the exchanged packets [6]. Unfortunately, the conventional authentication and key agreement protocols have high computational requirements such as power consumption, memory, and processing capacity. In addition, some of them have design flaws that result in leakages of sensitive data.

To address power constraints in smart home IoT devices, the Long-Range (LoRa) technology known as Low-Power Wide-Area Network (LPWAN) has been implemented. As one of the LPWAN technologies, the Long-Range Wide-Area Network (LoRaWAN) uses very little power for long-range communication and is, therefore, highly efficient [21]. In addition, LoRaWAN offers open standard specifications and hence is crucial for networking hybrid autonomous communication architectures [22]. Another important LPWAN technology is the Narrow Band IoT (NB-IoT) that is heavily deployed in 3GPP cellular systems. It has high throughput and low complexities and can therefore help extend the battery lifetime of IoT devices. In addition, it provides better performance in terms of enhanced channel quality [23], long-range, high capacity, and low power [24]. In

general, LPWAN technologies have salient capabilities such as low-cost, long-range, low energy consumption, the transmission of low volumes of data, and support for a high number of devices. As such, these LPWAN technologies can play crucial roles in IoT applications such as smart homes.

Although LPWAN offers admirable features that render them applicable in smart home deployments, there are many security issues that need to be solved. For instance, LoRaWAN has numerous privacy and security vulnerabilities that can be utilized by adversaries to compromise the privacy of transmitted data, availability, and authentication [25]. For instance, its Activation by Personalization (ABP) activation mode uses static secret keys and addresses, which are stored in the end devices. Consequently, side-channeling through power analysis can retrieve these secrets and launch further attacks such as impersonation and spoofing. On its part, NB-IoT requires a large infrastructure and proprietary license [24]. Therefore, NB-IoT becomes costly to implement in realtime. In addition, lack of physical security, poor application, end-point security, and weak authorization and authentication are some challenges that are yet to be solved in NB-IoT [26].

It is evident that conventional IoT technologies, security protocols, and standards are unable to uphold privacy and security in smart homes [11]. Several hacks and software flaws have led to a lack of public confidence in smart home networks. As such, the design of efficient and secure message authentication protocols is still an open challenge.

1.1. Motivation

The intelligent sensors in smart home networks collect and transmit sensitive data that can expose the privacy of homeowners if captured by adversaries. As such, strong security solutions are needed to protect the various elements of these networks, such as the communication channels and the data residing in sensors. Therefore, many asymmetric and symmetric key-based protocols have been deployed to offer the required levels of security. However, most of these schemes are susceptible to many attacks. Some of these schemes also require the execution of computationally intensive cryptographic operations [4] that are not ideal for most smart home devices. Other researchers have also presented security protocols based on objects such as smart cards to secure smart home networks. However, these schemes are vulnerable to smart card theft or smart card loss attacks. It is also inconvenient for users to carry these cards around for multiple authentications. Although blockchain-based techniques can address these issues, privacy protection for the access policy remains an open challenge in these techniques. Moreover, the public key infrastructure-based schemes are unsuitable for deployment in smart home devices due to their computationally intensive cryptographic operations and storage requirements. There is, therefore,a need for a truly lightweight authentication scheme that can address some of these challenges.

1.2. Mechanisms and Objective Overview

The proposed protocol addresses security, performance, and privacy challenges in smart home networks. In so doing, smart homeowners can be assured that the exchanged packets cannot be compromised in transit. In so doing, security and privacy features such as confidentiality, integrity, availability, non-repudiation, and authentication are upheld. Since the majority of the sensors in the smart home network are resource-limited [11], only lightweight cryptographic operations are executed in our scheme. As such, the objective of the proposed protocol is to prolong the battery life of smart home sensors byreducing energy consumption.

1.3. Security Goals and Requirements

The numerous vulnerabilities, threats, and attacks in smart home networks might impede the adoption of smart home networks. Therefore, strong security techniques should be implemented to protect the transmitted as well the stored data in smart home

devices. To achieve this, an ideal authentication protocol should strive to offer the following security and privacy features:

Backward key secrecy: Suppose that an adversary has some access to the current session key. This backward key secrecy ensures that an attacker is unable to derive the session key utilized for the previous communication session based on the current session key.

Forward key secrecy: It should be computationally infeasible for the adversary equipped with the current session key to compute the session key for any subsequent communication [8].

Mutual authentication: Before the communicating entities can initiate any message exchanges, they should verify the legitimacy of each other.

Anonymity: During the authentication, key agreement, and communication processes, an attacker should be incapable of discerning the real identities of the communicating parties.

Unlinkability: It should be cumbersome for the adversary to relate the captured messages to any of the past as well as future messages emanating from the same communicating entities.

Robustness against attacks: A truly secure protocol should protect against conventional smart home attacks. These include denial of service, impersonation, man-in-the-middle (MitM), session hijacking, packet replays, and eavesdropping attacks.

1.4. Research Contributions

It is critical that memory, energy, communication, and computation complexities be kept at a minimum in smart home sensors and switches. Smart home networks comprise devices that are resource-limited in terms of memory, energy, and computation power. Such devices include smart switches and sensors; hence, any ideal authentication and key agreement (AKA) protocol must be lightweight. In addition, the massive data items exchanged over smart home networks are private andmay potentially reveal people's lifestyles if captured by adversaries. It is, therefore, important that data be protected while in transit between the remote users and the ISDs. In this regard, the following contributions are acclaimed in this paper:

- Lightweight cryptographic primitives are deployed in the proposed protocol so as to render it efficient for resource-limited indoor smart home sensors and switches.
- Session-specific parameters are incorporated in the developed protocol to offer dynamism to the session state parameters. This eventually works towards the elimination of packet replay attacks.
- Extensive formal verification of the proposed protocol is executed using the most common Burrows Abadi-Needham (BAN) logic, which shows the establishment of a message protection session key among the communicating parties.
- Informal security analysis is carried out, which demonstrates the resilience of the proposed protocol against packet replays, impersonation, eavesdropping, Denial of Service (DoS), session hijacking, and man-in-the-middle attacks.
- Comparative performance evaluation is executed, which shows that the proposed protocol offers enhanced security and privacy protection at lower energy, communication, and computation complexities.

The rest of this paper is structured as follows: Section 2 presents the related work, while the proposed scheme is discussed in Section 3. Similarly, Section 4 presents the security analysis of this protocol, while Section 5 discusses its performance evaluation. Finally, Section 6 concludes the paper and gives future research directions.

2. Related Work

Numerous security and privacy schemes have been developed to protect the packets exchanged over smart home networks. For instance, a 3-dimensional S-box scheduling

algorithm is presented in [27]. Although this scheme is efficient, its formal and informal security analyses are not carried out. In contrast, public key cryptosystems (PKC) based key agreement protocols are presented in [28–31]. However, PKC-based techniques have high communication and computational overheads [32]; hence they are unsuitable for ISDs. Although the protocol in [31] is resilient against attacks, it can neither withstand known-key attacks nor offer confidentiality, freshness checks, and anonymity [16,33]. Additionally, it incurs extremely high execution time and communication costs [16]. Although the protocol in [34] is robust against cloning, impersonation, traceability, and physical attacks, it involves extensive hashing operations and message exchanges which are not ideal for resource-constrained ISDs. Conversely, the device security protocol in [35] cannot offer secure mutual authentication and is susceptible to impersonation, stolen smart devices, and session key disclosure attacks [1].

To address the resource-constrained nature of ISDs, lightweight authentication protocols have been presented in [36,37]. Although the security model in [38] potentially protects user privacy, it has high power consumption due to the requirement for the installation of rechargeable batteries. Although the user authentication scheme in [39] can alleviate this problem, it is susceptible to a privileged insider, gateway bypass, offline password guessing, and replay attacks [40]. Therefore, a user authentication protocol has been proposed in [40] to address these issues. On the other hand, the scheme based on identity, password, and digital signatures is developed in [41]. However, it is based on PKI, which requires entities to maintain a pair of private and public keys, which increases its computation and communication complexities [42]. The protocols in [43–45] are efficient and can solve the problems in [41].However, the scheme in [43] cannot withstand de-synchronization attacks. In addition, it utilizes verification tables during authentication, which are susceptible to stolen verifier attacks [40]. Similarly, the protocol in [45] has some security issues that limit its applicability [41]. On its part, the scheme in [44] incurs low latency, storage costs, and power consumption, but its security analysis is not carried out.To boost efficiency and reliability, a smart card-based algorithm is developed in [46]. Although this approach has low computation and communication overheads, it cannot resist gateway spoofing, session key disclosure, and impersonation attacks. In addition, it cannot provide anonymity and secure mutual authentication [41]. The two-factor scheme in [47] is anonymous and can address anonymity issues in [46]. Unfortunately, it is vulnerable to password guessing, stolen user device, and impersonation attacks. In addition, it cannot provide mutual authentication [40].

Even though the anonymous security technique developed in [11] provides user anonymity and secure mutual authentication, it is susceptible to attacks such as impersonation, MitM, and session key disclosure [2]. On the other hand, the protocol in [48] assumes that the short-range channel between the ISDs and HGs is secure and that these devices are trustworthy. However, these assumptions are not viable as the open wireless channel is susceptible to a myriad of attacks, and the devices are not tamper-proof and may have inbuilt backdoors [6]. To offer protection against malicious activities in distributed smart environments, a scheme based on implicit certificates is developed in [16]. However, certificate revocation and storage require large memory and elongated execution time [49]. Alternatively, a privacy-preserving scheme is introduced in [50] and [51]. However, a single trusted third party is responsible for access control and authorization, which presents a single point of failure. In addition, these protocols have scalability issues [19,52]. Biometric-based protocols have been introduced to overcome the shortcomings inherent in static credentials-based authentication schemes [53,54]. Although these schemes have faster response times, many smart devices still lack inbuilt biometric authentication capabilities. In addition, they are not privacy–preserving [55] and present challenges in revoking compromised biometric information. Moreover, many users regard biometric authentication as intrusive and a violation of their privacy. To offer secure communication, a robust protocol is developed in [56]. Unfortunately, this protocol is vulnerable to stolen user devices and privileged insider attacks. The scheme in [57] can solve this problem by

upholding confidentiality and user and device authenticity. In addition, it prevents server spoofing, user impersonation, man-in-the-middle, replays, and offline password-guessing attacks. Unfortunately, it is vulnerable to de-synchronization attacks.

Based on digital certificates, a security protection scheme is introduced in [58]. In this approach, subsequent session keys are derived using some master keys and hence cannot assure forward key secrecy upon disclosure of these keys. In addition, a malfunctioning key derivation function (KDF) may lead to connection termination. On the other hand, the security technique in [59] is noted to be vulnerable to de-synchronization attacks [60]. To curb this challenge, a novel security preservation scheme is presented in [60]. Although the approach employed by the authors in [14] can uphold data confidentiality, it is unable to sustain authentication parameters privacy [61]. This problem is solved by the blockchain-based protocols in [62,63]. However, the deployed blockchain technology incurs heavy computation and storage overheads [64].

On its part, the temporal identity-based solution presented in [65] is vulnerable to attacks such as known-key and DoS. This is because it uses static parameters during the session key generation process. Due to computationally intensive cryptographic operations and heavy signaling during the authentication procedures, this approach incurs high communication and computation costs. A scheme based on fuzzy extraction is introduced in [66]. However, vulnerability to traceability attacks and inability to provide identity protection, as well as session key agreement, are its major challenges [67]. Conversely, the scheme in [8] dynamically renews the session key to thwart replay attacks. However, this approach has high computation costs due to a myriad of cryptographic operations involved. Table 1 presents a summary of the cons and pros of some of these schemes.

Table 1. Pros and cons of current schemes.

Scheme	Pros	Cons
[8]	Thwarts replay attacks	High computation costs
[11]	Provides user anonymity and secure mutual authentication	Susceptible to impersonation, MitM, and session key disclosure attacks
[14]	Upholds data confidentiality	Cannot provide authentication parameters privacy
[16]	Protects against malicious activities in distributed smart environments	Elongated execution time
[27]	Efficient	Its formal and informal security analyses are not carried out
[34]	Robust against cloning, impersonation, traceability, and physical attacks	High communication costs
[38]	Protects user privacy	High power consumption
[43]	Efficient	Cannot withstand de-synchronization attacks
[46]	Boosts efficiency and reliability	Cannot resist gateway spoofing, session key disclosure, and impersonation attacks.
[47]	Offers anonymity	Vulnerable to password guessing, stolen user device and impersonation attacks
[50,51]	Privacy-preserving	Single point of failure & scalability issues
[53,54]	Faster response time	Not privacy-preserving
[57]	Upholds confidentiality, user, and device authenticity	Vulnerable to de-synchronization attacks
[62,63]	Privacy-preserving	Heavy computation and storage overheads

In summary, the current authentication and key agreement protocols cannot offer complete security and privacy protection at low energy, execution time, and communication overheads. For instance, the asymmetric key protocols in [31,33] have higher costs compared with their symmetric counterparts in [14,59,60]. However, the communication

and computation complexities of these symmetric protocols are still unsuitable for smart home devices such as sensors and smart switches. Although LoRaWAN and NB-IoT technologies can address the inefficiency issues in current schemes, these technologies have numerous security challenges. For instance, LoRaWAN is susceptible to attacks such as bit-flipping and replay. As explained in [25], LoRaWAN authentication procedures are vulnerable to network flooding, man-in-the-middle, eavesdropping, sinkhole, jamming, replay, and spoofing. On the other hand, the schemes in [8,11,14,16] have been shown to have numerous security and performance issues. High communication and computation costs are the performance limitations of the majority of these schemes. On the other hand, lack of forward key secrecy and anonymity, coupled with susceptibility to impersonation, MitM, and DoS, are serious security and privacy issues in these protocols. In contrast, our protocol deploys transient parameters such as nonces, timing information, and secret values during the derivation of the session key to preserve forward key secrecy. In addition, shared secret keys are deployed to encrypt user and device identities to uphold their anonymity. This enciphering and re-computation of user identity using random nonces and exclusive OR operation with mobile device identity renders it hard for an attacker to eavesdrop on these identities for any possible impersonation attempt. To curb MitM attacks, the contents of the authentication verification beacons are concatenated before being hashed. This makes it computationally infeasible for the attacker to reverse the one-way hash to obtain these parameters for launching MitM attacks. Regarding the DoS attack, our scheme derives the verification token and sends it to the trusted authority. Here, this token is re-computed and compared with its received equivalent. If these parameters are not equivalent, the communication process is immediately terminated.

3. The Proposed Scheme

The proposed network model is made up of the Smart Home Devices (SHDs), the Smart Home Owner (SHO), Mobile Device (MD), the Trusted Authority (TA), and the wireless network. Here, wireless connectivity can be the internet which facilitates SHO and SHDs interactions. The SHOs utilize software controls in their MDs to access SHDs services. On the other hand, the TA acts as the Home Gateway (HG), as shown in Figure 1.

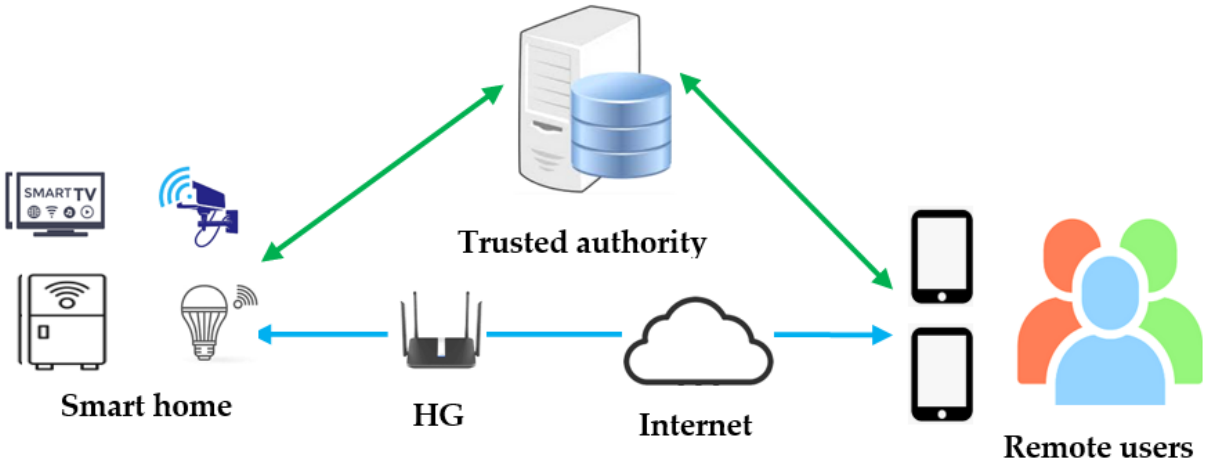

Figure 1. Network model.

The remote user commands are transmitted to the HG before being forwarded to the SHDs. In this arrangement, the HG manages all SHDs and is assumed to be a trusted entity with slightly higher memory, energy, and computation capabilities compared with SHDs. The communication link between the remote user and the HGs are assumed to be

insecure. The MDs can be smartphones, laptops, or tablets. Table 2 presents the notations deployed here and their descriptions.

Table 2. Notations and their descriptions.

Notation	Description
TA	Trusted authority
SHD	Smart home device
ID_U	User identity
ID_M	Mobile device identity
ID_{TA}	TA's identity
h(.)	Hashing operation
T_M	Timer
ψ	MD & TA shared secret key
ϕ	SHD & TA shared secret key
$\mathbb{N}_i$	Random nonce
ID_S	SHD identity
$T_1 \ldots T_7$	Timestamps
T_{Th}	Threshold timestamp
E_ψ	Encryption using ψ
$\oplus$	XOR operation
||	Concatenation operation

Before the onset of the packet exchanges between the SHDs and SHOs, the MDs and SHDs must be registered at the TA, as outlined in Section 3.1 below. Thereafter, Authentication and Key Agreement (AKA) procedures are executed, as evidenced in Section 3.1. The block diagram in Figure 2 gives a summary of these steps.

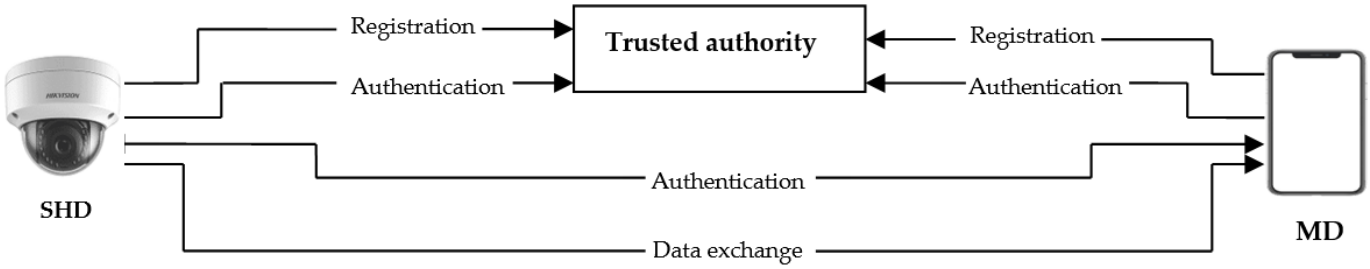

Figure 2. Execution block diagram.

As shown in Figure 2, the chronology of events includes registration, authentication, anddata exchange between the smart home device and the smart home owner's mobile device. During registration, the trusted authority generates and distributes the security parameters to the smart home device and the mobile device. To accomplish this, secure communication channels are utilized. During the authentication process, these security parameters are deployed to derive some security tokens used to validate the authenticity of the communicating parties. After successful authentication procedures, the smart home and mobile device can trust one another and commence data exchange.

3.1. SHDs and MDs Registration Phase

The registration phase consists of four major steps, as discussed below.

Step 1: The TA instantiates timer T_M and derives the shared secret key ψ deployed between the MD and TA before generating user identity ID_U and MD identity ID_M. This is followed by the derivation of $\mathcal{d} = E_\psi (ID_U)$ and $\mathcal{e} = E_\psi (ID_M)$, which are actually ID_U and ID_M

encrypted using ψ. Next, the SHO composes registration request $SOReg_{Req}$ that is then sent to TA with security parameters $\mathcal{d}$ and $\mathcal{e}$.

Step 2: Upon receipt of Reg_{Req}, TA increments T_M and computes ephemeral $S = E_\psi (T_M^*)$. Next, TA generates nonce $\mathbb{N}_1$ before deriving its current session secret value $\mathbb{P}_{TA} = h(ID_U||ID_M||\mathbb{N}_1)$ that essentially binds ID_U and ID_M. This is followed by the derivation of ID_U's current session secret value $\mathbb{Q}_U = E_\psi (ID_U, ID_M, \mathbb{P}_{TA}, S)$ and security parameter $T_P = (\psi||\mathbb{N}_1)$. The TA terminates SHO registration by sending registration response $SOReg_{Res}$ with T_P and $\mathbb{Q}_U$ to the SHO, which are then buffered into MD's repository (*Rep*). Meanwhile, TA also buffers all the computed and generated security tokens in its *Rep*.

Step 3: For the SHD to register to the TA, it generates the random number $\mathbb{N}_2$ and its session identity ID_S before calculating security token $U = E_\psi (ID_S||\mathbb{N}_2)$. Next, the SHD sends its registration request $SHReg_{Req}$ together with U to the trusted authority.

Step 4: Upon receipt of this token, the TA generates random nonce $\mathbb{N}_3$ and its identity ID_{TA}, then derives SHD's current session secret value $H_S = h(ID_S||\mathbb{N}_3)$ together with its secret session tokens $\mathbb{Z}_S = E_\Phi(ID_S, H_S, \mathbb{N}_3)$ and $V = E_\Phi (ID_{TA}||\mathbb{N}_3)$. Afterward, TA sends the registration response $SHReg_{Res}$ together with security parameter $\mathbb{Z}_S$ and ID_{TA} to the SHD for storage. Figure 3 presents the message flow during the registration process.

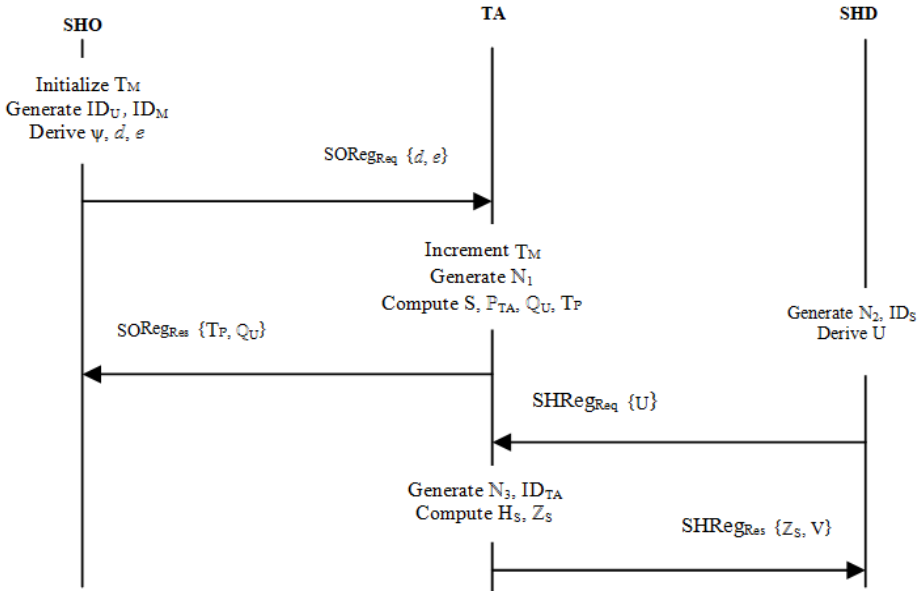

Figure 3. Registration message flows.

As depicted in Figure 3, 4 messages are exchanged among the SHO, TA, and SHD during the registration phase. Note that ID_U and ID_M are encrypted using ψ to yield security tokens $\mathcal{d}$ and $\mathcal{e}$, respectively, before being coupled to the communication channel. Similarly, parameters ID_U, ID_M, $\mathbb{P}_{TA}$,and *S* are encrypted using ψ before their transmission over the open wireless communication links. On the other hand, ψ is masked in nonce $\mathbb{N}_1$ to yield security parameter T_P. In addition, to securely transmit ID_S to the TA, the SHD masks it in nonce $\mathbb{N}_2$ before encrypting it using ψ. Finally, security parameters ID_{TA}, ID_S, and H_S are masked in nonce $\mathbb{N}_3$, then encrypted using Φ before being sent to the SHD.

3.2. Mutual Authentication

Whenever the SHO wishes to access the SHDs services, the following nine steps are invoked, as discussed below.

Step 1: The MD generates nonce $\mathbb{N}_4$ before computing security parameter $\mathbb{R}_U = \mathbb{N}_4 \oplus ID_M$ and MD's authentication verification beacon $P_U = h(\mathbb{Q}_U||\mathbb{R}_U||\psi||T_1||\mathbb{N}_4||T_M)$. Next, the

computed parameters, together with timestamp T_1 and buffered token $\mathbb{Q}_U$, are transmitted to the TA together with the MD authentication request, $MAuth_{Req}$, as evidenced in Figure 4.

Step 2: On getting these parameters, the TA determines timestamp $T_2$and computes $\Delta T = T_2 - T_1$ before validating it against some set threshold T_{Th}. This step is critical for the prevention of packet replay attacks. If an attacker launches this attack against the proposed protocol using the captured security parameters, the freshness checks of timestamps together with threshold T_{Th} will render this attack futile.

Step 3: The TA re-computes nonce $\mathbb{N}_4 = \mathbb{R}_U \oplus ID_M$before $\mathbb{Q}_U = D_\psi$ (ID_U, ID_M, $\mathbb{P}_{TA}$, S) is decrypted using ψ to yield its constituents that are thenvalidated against their buffered equivalents in *Rep*. Here, provided that ID_M is not in *Rep*, the request is flagged as an impersonation attempt.

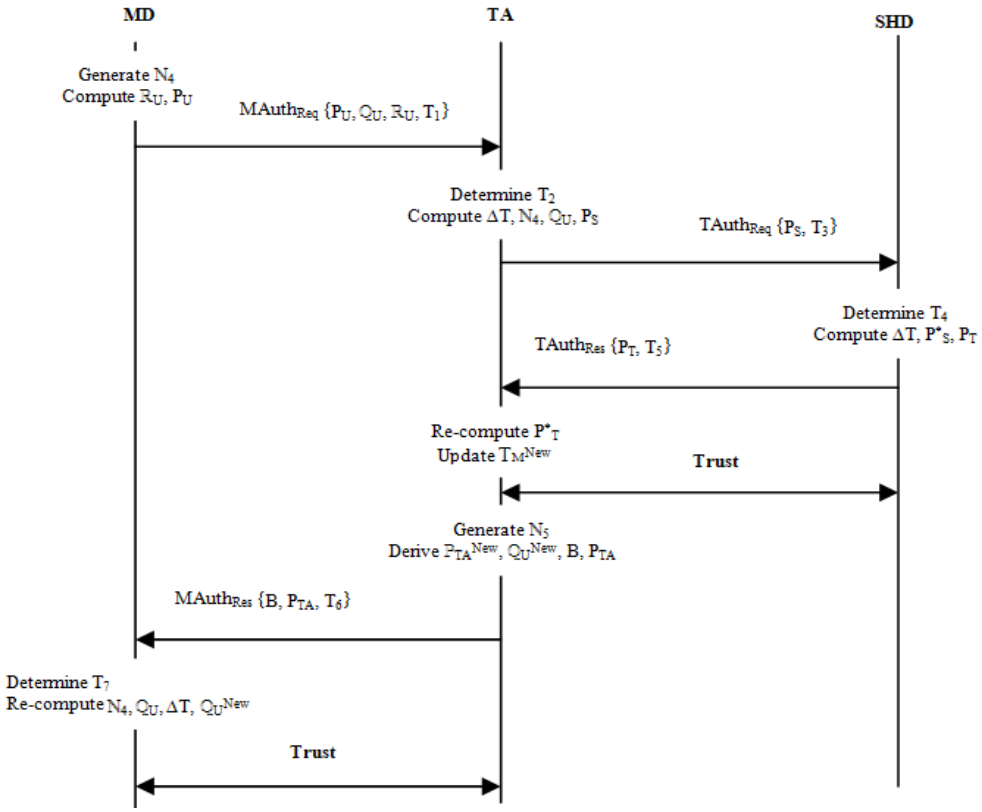

Figure 4. Mutual authentication message flows.

Next, TA checks whether T_M is within its *Rep*, and if this is the case, it proceeds to retrieve nonce $\mathbb{N}_4 = \mathbb{R}_U \oplus ID_M$ before validating the received P_U against its buffered value.

Step 4: To usher in SHD authentication with TA, the verification of P_U must be successful.When this happens, SHD's authentication verification beacon $P_S = h(\mathbb{Z}_S||T_3||ID_{TA})$ is derived and transmitted to the SHD with TA's authentication request, $TAuth_{Req}$.

Step 5: Upon receipt of this beacon, SHD determine the current timestamp T_4 before calculating $\Delta T = T_4 - T_3$, which is then validated. Provided that this validation is successful, $P^*_S = h(\mathbb{Z}_S||T_3||ID_{TA})$ is re-computed, after which it is validated against its received counterpart P_S. Here, successful verification leads to the computation of another authentication verification beacon $P_T = h(\mathbb{Z}_S||T_5||ID_{TA})$ sent to TA together with timestamp T_5 and TA's authentication response $TAuth_{Res}$.

Step 6: After getting these parameters, $P^*_T = h(\mathbb{Z}_S||T_5||ID_{TA})$ is re-calculated before its validation against its received counterpart P_T. If this verification succeeds, SHD and TA mutual authentication is successful, and they can now trust each other. Next, the deployed

parameter T_M is refreshed as T_M^{New} and buffered to preserve perfect forward key secrecy.

Step 7: To accomplish TA and MD mutual authentication, TA generates nonce $\mathbb{N}_5$ before refreshing previous parameters with their new values $\mathbb{P}_{TA}^{New}$ = h ($ID_U||ID_M||\mathbb{N}_5$) and $\mathbb{Q}_U^{New}= E_\psi$ (ID_U, ID_M,$\mathbb{P}_{TA}^{New}$,T_M^{New}). At the same time, P_{TA} = h ($\mathbb{Q}_U^{New}||ID_M||\mathbb{N}_4||T_6||\psi$) is recalculated, and additional security token B = $\mathbb{Q}_U^{New}\oplus ID_M$ is derived. This step is very crucial for the preservation of backward and forward key secrecy. Here, an attacker that has captured $\mathbb{P}_{TA}$and $\mathbb{Q}_U$ deployed in the current authentication session may attempt to reuse them to determine the previous as well as the subsequent session secret keys {$\mathbb{P}_{TA}^{Prev}$,$\mathbb{Q}_U^{Prev}$} and {$\mathbb{P}_{TA}^{Next}$,$\mathbb{Q}_U^{Next}$} respectively. However, updating these session secret keys incorporates random nonce $\mathbb{N}_5$, rendering them session-specific. Lastly, MD's authentication response $MAuth_{Res}$, security parameters B and P_{TA}, together with timestamp T_6, are sent to the MD. Meanwhile, the TA updates its *Rep* with these new security parameters $\mathbb{P}_{TA}^{New}$, $\mathbb{Q}_U^{New}$, $\mathbb{N}_5$, and T_M^{New}.

Step 8: Upon receipt of these parameters, the MD re-derive $\mathbb{N}_4 = \mathbb{R}_U\oplus ID_M$ before decrypting $\mathbb{Q}_U=D_\psi$ (ID_U, ID_M, $\mathbb{P}_{TA}$,T_M) to obtain its constituents which are then verified against their buffered counterparts in *Rep*. Provided that this verification is successful, the MD determines T_7 that is employed to derive $\Delta T = T_7 - T_6$ that is then validated against replay attacks. Next, $\mathbb{Q}_U^{New}= B\oplus ID_M$ is re-computed for subsequent authentication.

Step 9: The P_{TA} received from TA is verified such that if this process is successful, the MD and TA have mutually authenticated each other and can trust each other. However, if all the retrieved parameters are in *Rep* except MD's ID_M, the implication is that the SHO may be utilizing an MD that is yet to be registered at the TA, and hence its registration is prompted.

As shown in Figure 3, 4 messages are exchanged during the AKA phase. All the parameters in message {P_U,$\mathbb{Q}_U$, $\mathbb{R}_U$,T_1} are sufficiently protected before their transmission over the communication links. For instance, P_U is in the hashed format while $\mathbb{Q}_U$is in encrypted form using ψ. On the other hand, $\mathbb{R}_U$ is exposed to XOR operation with nonce $\mathbb{N}_4$ and hence is fairly random.Similarly, message {P_S, T_3} is protected since P_S is in hashed form and timestamp T_3 is randomly selected. The same applies to message {P_T, T_5} sent to TA from SHD. Finally, in message {B,P_{TA},T_6} sent from the TA to MD is protected through hashing (P_{TA}) and XOR operation (B), while timestamp T_6 is randomly chosen.

4. Security Analysis

To show that the proposed protocol offers strong privacy and security protection, formal verification and informal security analyses are carried out.

4.1. Formal Security Analysis

In this section, the widely deployed Burrows–Abadi–Needham (BAN) logic is utilized to demonstrate that the beacons exchanged are protected against any form of eavesdropping. Therefore, the communicating entities can trust each other as they communicate over insecure channels. Table 3 presents the BAN logic notations (BLNs) deployed in this formal verification process.

Table 3. BAN logic notations.

SNo.	Symbol	Description
BLN_1	SK	One-time session key
BLN_2	D|≡E	D believes statement E
BLN_3	D| ~E	D once said statement E
BLN_4	D◁ E	D sees statement E

BLN_5	#E	Statement E is fresh
BLN_6	<E>F	Statement E is combined with secret statement F
BLN_7	$\{E\}_G$	Statement E is protected by secret key G
BLN_8	$D \overset{G}{\leftrightarrow} H$	D and H share secret key G
BLN_9	$D \Rightarrow E$	D has jurisdiction over E

For easy of analysis, all the messages exchanged during the AKA procedures are transformed into some idealized format (IME) as shown in Table 4.

Table 4. Idealized message exchanges.

IME_1	SHO→TA: P_U, $\mathbb{Q}_U$: < ID_U, ID_M, $\mathbb{N}_1$> ψ, $\mathbb{R}_U$<$\mathbb{N}_4$> ID_M, T_1
IME_2	TA→SHD: P_S,T_3
IME_3	SHD→TA: P_T,T_5
IME_4	TA→SHD: B:<$\mathbb{Q}_U^{New}$> ID_M, $\mathbb{P}_{TA}$,T_6

Thereafter, the initial assumptions (ITA) in Table 5 were made to facilitate easier analysis using BAN logic.

Table 5. Initial state assumptions.

SNo.	Initial Assumption
ITA_1	SHO|≡#($\mathbb{N}_4$)
ITA_2	TA|≡#($\mathbb{Q}_U$)
ITA_3	SHD|≡#(P_T)
ITA_4	TA|≡SHD⇒(P_S)
ITA_5	TA|≡SHO⇒$\mathbb{Q}_U$
ITA_6	SHD|≡TA⇒P_T
ITA_7	SHO|≡TA⇒$\mathbb{Q}_U$

To provide enhanced protection, the security goals (SGs) in Table 6 are formulated.Therefore, the formal verification procedures simply serve to demonstrate how these goals are attained in the proposed protocol.

Table 6. Security goals.

SNo.	Security Goal
SG_1	$TA \mid \equiv SHO \overset{\mathbb{Q}_U}{\leftrightarrow} TA$
SG_2	$TA \mid \equiv SHO \mid \equiv SHO \overset{\mathbb{Q}_U}{\leftrightarrow} TA$
SG_3	$SHD \mid \equiv TA \overset{\mathbb{Z}S}{\leftrightarrow} SHD$
SG_4	$SHD \mid \equiv TA \mid \equiv TA \overset{\mathbb{Z}S}{\leftrightarrow} SHD$
SG_5	$TA \mid \equiv SHD \overset{\mathbb{Z}S}{\leftrightarrow} TA$
SG_6	$TA \mid \equiv SHD \mid \equiv SHD \overset{\mathbb{Z}S}{\leftrightarrow} TA$
SG_7	$SHO \mid \equiv TA \overset{\mathbb{Q}_U}{\leftrightarrow} SHO$
SG_8	$SHO \mid \equiv TA \mid \equiv TA \overset{\mathbb{Q}_U}{\leftrightarrow} SHO$

Based on the above-idealized message exchanges (IME) and ITA, the BAN logic rules (BLR) in Table 7 were utilized to attain the security goals in Table 6 above.

Table 7. BAN logic rules.

Rule	Description
$\frac{D\mid\equiv H\Rightarrow E, D\mid\equiv H\mid\equiv E}{D\mid\equiv E}$	Jurisdiction rule (JR)
$\frac{D\mid\equiv \#(E)}{D\mid\equiv \#(E,F)}$	Fresh-promotion rule(FPR)
$\frac{D\mid\equiv \mathrm{D}\overset{G}{\leftrightarrow}\mathrm{H}, \mathrm{D}\triangleleft\{\mathrm{E}\}_G}{D\mid\equiv H\mid\sim E}$	Message-meaning rule (MMR)
$\frac{D\mid\equiv \#(E), D\mid\equiv H\mid\sim E}{D\mid\equiv H\mid\equiv E}$	Nonce verification rule (NVR)

Based on IME$_1$, the seeing rule (SR) in BLN$_4$ is deployed to yield BAN Logic 1 (BLP$_1$):

BLP$_1$: TA$\triangleleft$P$_U$, $\mathbb{Q}_U$: < ID_U, ID$_M$, $\mathbb{N}_1$>ψ, $\mathbb{R}_U$<$\mathbb{N}_4$> ID$_M$, T$_1$

Hinged on ITA1, MMR and is applied to BLP$_1$ to yield BLP$_2$:

BLP$_2$: TA$\mid\equiv$ SHO$\mid\sim\mathbb{N}_4$

The application of FPR in BLP$_2$ results in BLP$_3$:

BLP$_3$: TA$\mid\equiv$ SHO$\mid\equiv\mathbb{N}_4$

Based on BLP$_3$, JR is applied to obtain BLP$_4$:

BLP$_4$: TA$\mid\equiv\mathbb{N}_4$

From ITA$_2$ andITA$_5$, JR is applied on BLP$_4$ yields BLP$_5$:

BLP$_5$: TA$\mid\equiv$ SHO $\overset{\mathbb{Q}_U}{\leftrightarrow}$ TA

On the other hand, using NVR on BLP$_5$, BLP$_6$ is obtained:

BLP$_6$: TA $\mid\equiv$ SHO$\mid\equiv$ SHO $\overset{\mathbb{Q}_U}{\leftrightarrow}$TA

Based on IME$_2$ and ITA$_4$, SR is applied to yield BLP$_7$:

BLP$_7$: SHD$\triangleleft$P$_S$,T$_3$

The application of MMR on BLP$_7$results inBLP$_8$:

BLP$_8$: SHD$\mid\equiv$ TA$\mid\sim\mathbb{Q}_U$

Based on BLP$_8$, the FPR is deployed to yield BLP$_9$:

BLP$_9$: SHD$\mid\equiv$ TA$\mid\equiv\mathbb{Q}_U$

Next, using JR on BLP$_9$ results in BLP$_{10}$:

BLP$_{10}$: SHD$\mid\equiv\mathbb{Q}_U$

Applying JR on BLP$_{10}$, BLP$_{11}$ is obtained:

BLP$_{11}$: SHD $\mid\equiv$ TA $\overset{\mathbb{Z}S}{\leftrightarrow}$SHD

However, the application NVR on BLP$_{11}$ results in BLP$_{12}$:

BLP$_{12}$: SHD $\mid\equiv$ TA$\mid\equiv$ TA $\overset{\mathbb{Z}S}{\leftrightarrow}$SHD

Conversely, based on IME$_3$, SR is deployed to yield BLP$_{13}$:

BLP$_{13}$: TA$\triangleleft$P$_T$,T$_5$

Afterwards based on ITA$_3$, MMR is deployed in BLP$_{13}$ to obtain BLP$_{14}$:

BLP$_{14}$: TA$\mid\equiv$ SHD$\mid\sim$P$_T$

According to BLP$_{14}$ and ITA$_6$, FPR is applied to produce BLP$_{15}$:

BLP$_{15}$: TA$\mid\equiv$ SHD$\mid\equiv$P$_T$

Using JR on BLP$_{15}$, BLP$_{16}$ is obtained:

BLP$_{16}$: TA$\mid\equiv$P$_T$

On the other hand, applying JR on BLP_{16}yields BLP_{17}:

BLP_{17}: $TA \mid \equiv SHD \overset{\mathbb{Z}S}{\leftrightarrow} TA$

The application of NVR on BLP_{17} yields BLP_{18}:

BLP_{18}: $TA \mid \equiv SHD \mid \equiv SHD \overset{\mathbb{Z}S}{\leftrightarrow} TA$

Based on IME_4, the SR is applied to obtain BLP_{19}:

BLP_{19}: $SHO \triangleleft B: <\mathbb{Q}_U^{New}> ID_M, \mathbb{P}_{TA}, T_6$

Using MMR on BLP_{19} results in BLP_{20}:

BLP_{20}: $SHO \mid \equiv TA \mid \sim \mathbb{Q}_U$

According to BLP_{20}, FPR is applied to get BLP_{21}:

BLP_{21}: $SHO \mid \equiv TA \mid \equiv \mathbb{Q}_U$

However, the deployment of JR on BLP_{21}yields BLP_{22}:

BLP_{22}: $SHO \mid \equiv \mathbb{Q}_U$

Based on BLP_{22} and ITA_7, JR is applied to obtain BLP_{23}:

BLP_{23}: $SH0 \mid \equiv TA \overset{\mathbb{Q}_U}{\leftrightarrow} SHO$

On the other hand, the application of NVR on BLP_{23} yields BLP_{24}:

BLP_{24}: $SH0 \mid \equiv TA \mid \equiv TA \overset{\mathbb{Q}_U}{\leftrightarrow} SHO$

It has been shown through BLP_1 to BLP_{24} that SHO, TA, and SHD execute mutual authentication amongst themselves and negotiate the common session key. This is the key utilized to encipher all the messages exchanged among the communicating entities. Table 8 presents the BLP and security goals achieved.

Table 8. Attainment of security goals.

SL	BLP
SG_1	BLP_5
SG_2	BLP_6
SG_3	BLP_{11}
SG_4	BLP_{12}
SG_5	BLP_{17}
SG_6	BLP_{18}
SG_7	BLP_{23}
SG_8	BLP_{24}

As shown in Table 8, the BAN logic that was carried out has demonstrated the capability of the proposed protocol to achieve all the eight security goals formulated above.

4.2. Informal Security Analysis

This sub-section presents the evaluation of the security posture of this protocol against the most common attack vectors in smart home networks. This is achieved through the formulation and proof of the following lemmas.

Lemma 1: *Backward and forward key secrecy are preserved.*

Proof: The aim of upholding forward key secrecy is to prevent an attacker from using the current session key to accurately derive the session for the subsequent communication session. In our scheme, TA's current session secret value $\mathbb{P}_{TA}$ and ID_U's current session secret value $\mathbb{Q}_U$ are refreshed after every successful authentication. The computation of these session secrets incorporates random nonces and some timing information T_M that is

updated after every successful authentication. Consequently, constructing any valid $\mathbb{P}_{TA}$ and $\mathbb{Q}_U$ parameters is computationally infeasible. □

Lemma 2: *Strong mutual Authentication is executed.*

Proof: In our protocol, TA validates the authenticity of smart home users by computing security tokens $\mathbb{Q}_U$ and $P_U$such that the authentication process is terminated if these parameters are illegitimate. In addition, all smart home users authenticate TA through $\mathbb{P}_{TA}$ and $\mathbb{Q}_U^{New}$. In this process, only TA and MD have knowledge of security parameter ψ. To render this authentication dynamic, nonce $\mathbb{N}_1$, $\mathbb{N}_4$, and auto-incremented parameter T_M are deployed and refreshed after each successful authentication.□

Lemma 3: *Packet replays attacks are prevented.*

Proof: The success of this attack requires that security parameters $\mathbb{Q}_U$ and P_U must be captured by an attacker. However, this is impossible since $\mathbb{Q}_U$ is enciphered using secret key ψ. After every successful authentication, parameters $\mathbb{Q}_U$ and $\mathbb{P}_{TA}$ are substituted by their refreshed counterparts $\mathbb{Q}_U^{New}$ and $\mathbb{P}_{TA}^{New}$, respectively. In addition, freshness checks using timestamps and random nonce renders packet replay attacks infeasible. □

Lemma 4: *The proposed scheme provides device anonymity.*

Proof: To successfully register the user, identity ID_U and mobile device identity ID_M are enciphered using shared secret parameter ψ. This happens by forwarding these two values to the trusted authority. Similarly, the SHD's identity ID_S is encrypted using Φ before its transmission over the communication channel. On the other hand, during the authentication phase, beacons such as $\{P_U, \mathbb{Q}_U, \mathbb{R}_U, T_1\}$ and $\{P_S, T_3\}$ are exchanged. Suppose that an attacker eavesdrops on the first message. However, since user identity $\mathbb{R}_U$ is masked in other parameters, including the timestamp, it is impossible for an attacker to determine with high precision the smart home user's identity. In addition, ID_U's current session secret value $\mathbb{Q}_U$is encrypted using shared secret key ψ. Consequently; an attacker is incapable of accurately discerning the true identity of the smart home users and their mobile devices.□

Lemma 5: *This protocol prevents impersonation attacks.*

Proof: For an adversary to effectively impersonate the remote smart homeowner, user identity ID_U and mobile device identity ID_M must be captured. However, these parameters are enciphered in $\mathcal{d} = E_\psi(ID_U)$ and $\mathcal{e} = E_\psi(ID_M)$ using shared secret keys ψ before being sent over the channel to the TA during the registration phase. During the initial phases of the AKA procedures, $\mathbb{R}_U$ is computed using nonce $\mathbb{N}_4$ through exclusive OR operation with ID_M. As such, these two identities cannot directly eavesdrop from the communication channel and impersonation of the SHO and MD flops. □

Lemma 6: *This protocol is robust against eavesdropping attacks.*

Proof: In this scheme, the current secret value $\mathbb{Q}_U = E_\psi(ID_U, ID_M, \mathbb{P}_{TA}, S)$is enciphered using shared secret ψ. It is then utilized during the authentication phase to accompany the MD's authentication request $MAuth_{Req}$. Additionally, all the packets and parameters exchanged during AKA procedures are transient. Consequently, they cannot yield meaningful information that may facilitate the computation of next-session authentication parameters.□

Lemma 7: *Man-in-the-middle attacks are thwarted.*

Proof: The assumption made in this attack is that an adversary has captured current session secret value $\mathbb{Q}_U = E_\psi(ID_U, ID_M, \mathbb{P}_{TA}, S)$ and MD's authentication verification beacon $P_U = h(\mathbb{Q}_U||\mathbb{R}_U||\psi||T_1||\mathbb{N}_4||T_M)$. The aim is then to modify the contents of these parameters before forwarding them to the unsuspecting trusted authority TA. However, all the contents of $\mathbb{Q}_U$ are enciphered using secret key ψ. Since this key cannot be obtained by the adversary, this attack flops. Additionally, security parameters in P_U are concatenated before being hashed. As such, a MitM attack using P_U is infeasible due to the difficulty of reversing the one-way hash function. □

Lemma 8: *Denial of service and session hijacking attacks are prevented.*

Proof: The goal of the attacker is to knock off the smart home device SHD by hijacking its session during the AKA procedures. To achieve this, the attacker derives a fake verification beacon $P_T^F = h(\mathbb{Z}_S^F||T_5^F||ID_{TA}^F)$, which is then sent to the TA. On getting this security parameter, the TA has to re-compute it through $P^*_T = h(\mathbb{Z}_S||T_5||ID_{TA})$, as shown in Figure 3. Afterward, it is compared with the value received from the SHD in $TAuth_{Res}$.Here, if $P^*_T \neq P_T$, the session is aborted and hence session hijacking using bogus P_T^F leads to session termination for this particular attacker and not for the legitimate SHD. □

5. Performance Evaluation

In this section, resilience against attacks, energy consumption, communication, and computation overheads are utilized to assess the proposed protocol. This choice is informed by the fact that these parameters are some of the most common metrics for evaluating authentication and key agreement schemes.

5.1. Computation Overheads

During the AKA procedures, one-way hashing and symmetric encryption are the only operations executed.For symmetric encryption, Advanced Encryption Standard (AES) is utilized. However, for one-way hashing operations, a secure hash algorithm (SHA-1) is used. To make a comparative evaluation with other related schemes straightforward, the values in [40] are used. As pointed out in [40], the execution time for symmetric encryption or decryption (T_{ED}) = 0.0215 ms, ECC multiplication (T_{EM}) = 0.4276 ms, message authentication code (T_{MA}) = 0.0215 ms,one way-hashing (T_H) = 0.052 ms andfuzzy extraction (T_{FE}) = 0.0215 ms as shown in Table 9.

Table 9. Cryptographic execution time.

Cryptographic Operation	Execution Time (ms)
Symmetric encryption or decryption (T_{ED})	0.0215
ECC point multiplication (T_{EM})	0.4276
Message authentication code (T_{MA})	0.0215
One way-hashing (T_H)	0.052
Fuzzy extraction (T_{FE})	0.0215

As per Figure 4, the MD executes $1T_H$ and $1T_{ED}$ operations, while the TA executes $4T_H$and $2T_{ED}$ operations. On the other hand, the SHD executes $2T_H$ operations. As such, the total computation cost is $7T_H + 3T_{ED}$, which takes 0.4285 ms, as evidenced in Table 10.

Table 10. Computation costs.

Scheme	Cryptographic Operations	Total Computation Time (ms)
Shuai et al. [39]	$16T_H+3T_{EM}$	2.1148
Kaur et al. [40]	$16\ T_H+3T_{EM}$	2.1148
Wazid et al. [43]	$29\ T_H+4T_{ED}+T_{FE}$	1.6155

Wu et al. [47]	17 T_H+6T_{ED}	1.0130
Sureshkumar et al. [56]	17 T_H+16T_{EM}	7.7256
Proposed	7T_H+3T_{ED}	0.4285

As shown in Table 9, the scheme in [56] requires 17 one-way hashing operations and 16 ECC point multiplication operations and hence incurs the highest computation overheads, as shown in Figure 5. The schemes in [39,40] have the second highest computation costs of 2.1148, followed by the protocols in [43,47] with 1.6155 ms and 1.0130 ms, respectively.

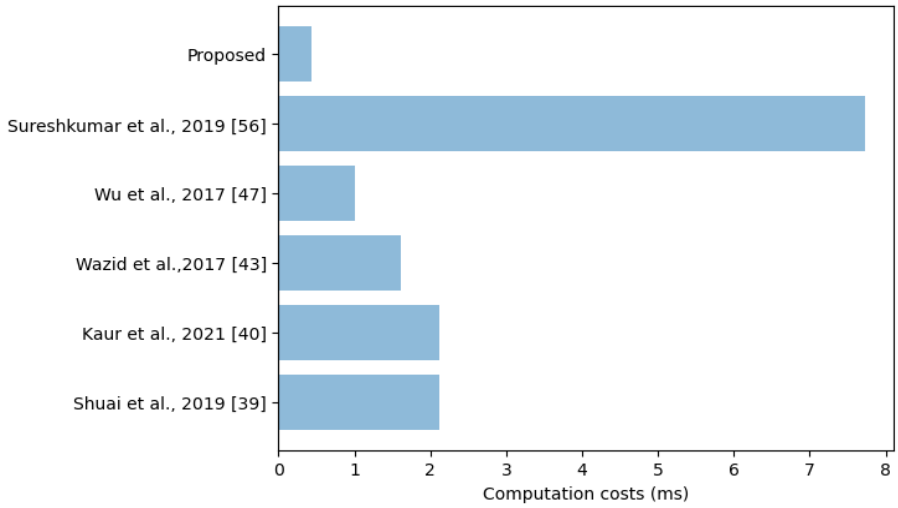

Figure 5. Computation costs comparisons

Conversely, the proposed protocol requires only seven one-way hashing operations and has the lowest computation overheads. It is, therefore, the most efficient in terms of computation complexities during the authentication and key negotiation phase.

5.2. Communication Overheads

Based on Figure 3, the following messages are exchanged during the AKA phase: {P_U, $\mathbb{Q}_U$, $\mathbb{R}_U$,T_1}, {P_S, T_3}, {P_T, T_5} and {B, P_{TA},T_6}. Using the values in [40], all user and device identities =128 bits, pseudo-random numbers =128 bits, symmetric key output =256 bits, hashing output = 160 bits, certificates =128 bits, nonce =160 bits, signatures = 160 bits, and timestamp = 32 bits. Therefore, Here, P_U= P_S = P_T = P_{TA} =160 bits, $\mathbb{Q}_U$= 256 bits, $\mathbb{R}_U$= 160 bits, T_1= T_3=T_5= T_6= 32 bits, while B = 256 bits. As such, the cumulative communication complexity of the proposed protocol is 1440 bits. Table 11 compares this value with other state-of-the-art schemes.

Table 11. Communication costs.

Scheme	**Total Costs (Bits)**
Shuai et al. [39]	1728
Kaur et al. [40]	1856
Wazid et al. [43]	2268
Wu et al. [47]	2048
Sureshkumar et al. [56]	3296
Proposed	1440

Based on the graphs in Figure 6, the protocol in [56] has the highest communication costs of 3296 bits. This is followed by the schemes in [39,40,43,47] with2268 bits, 2048 bits, 1856 bits, and 1728 bits,respectively.

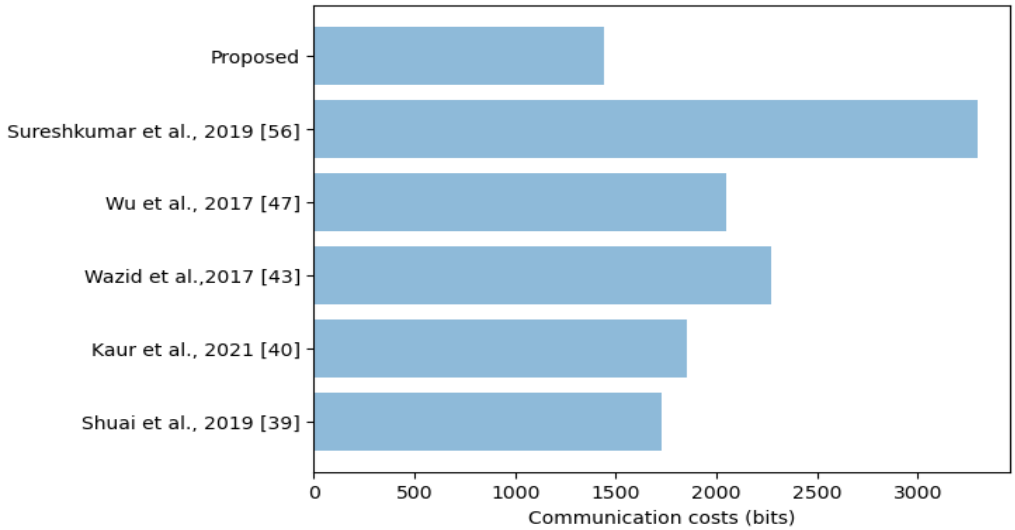

Figure 6. Communication costs comparisons.

On the other hand, the proposed protocol incurs the lowest communication overheads of only 1440 bits during the mutual authentication and key negotiation phase. Therefore, it makes the most effective usage of the available bandwidth.

5.3. Storage Overheads

In the proposed protocol, the SHD stores $\{\mathbb{Z}_S\ ID_{TA}\}$ in its memory. Using the values in [40], $\mathbb{Z}_S$ = 256 bits and ID_{TA} = 128 bits. Therefore, the cumulative storage overhead in the proposed protocol is 384 bits. Table 12 presents the storage overheads of the other related schemes.

Table 12. Storage overheads.

Scheme	Total Costs (Bits)
Shuai et al. [39]	512
Kaur et al. [40]	384
Wazid et al. [43]	640
Wu et al. [47]	576
Sureshkumar et al. [56]	960
Proposed	384

As shown in Figure 7, the protocol in [56] requires the largest storage space of 960 bits. This is followed by the schemes in [39,43,47] with 640 bits, 576 bits, and 512 bits, respectively.

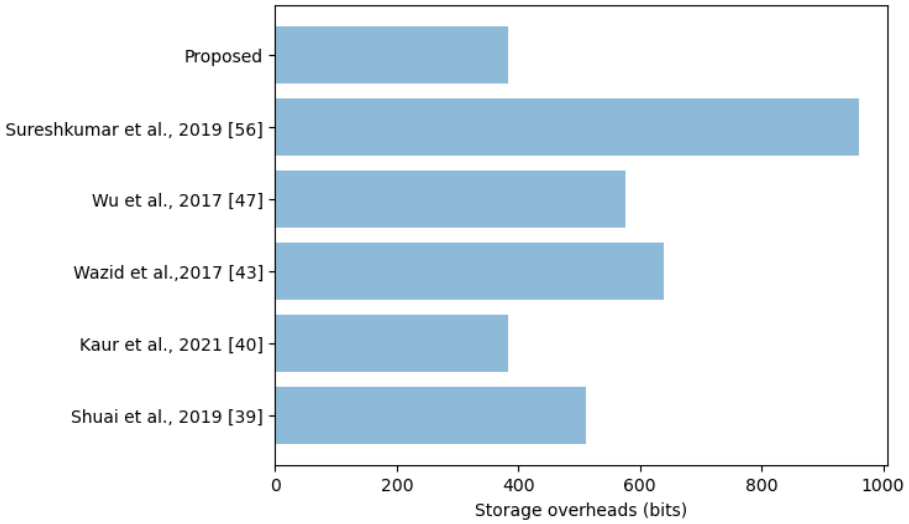

Figure 7. Storage overheads comparisons.

On the other hand, the scheme in [40] and the proposed protocol require the smallest storage space of only 384 bits. As such, they are the most ideal for deployment in memory-constrained smart home devices.

5.4. Attacks Resilience

In this sub-section, security comparative evaluation is accomplished to show the robustness of the proposed protocol against conventional smart home attacks. As shown in Table 13, the scheme in [47] offers only three security features and is robust against two attacks only. On the other hand, the protocol in [39] provides only four security features and resilience to only three attack vectors.

Table 13. Security features comparisons.

	[39]	[40]	[47]	[56]	Proposed
Security feature					
Backward key secrecy	-	-	-	-	√
Forward key secrecy	√	√	√	√	√
Mutual Authentication	√	√	×	√	√
Secret key agreement	√	√	√	√	√
Device anonymity	√	√	√	√	√
Protection against:					
Packet replays	×	√	×	√	√
Impersonation	√	√	×	√	√
Eavesdropping	-		-	-	√
Man-in-the-middle	-		-	-	√
Denial of service	√	√	√	√	√
Session hijacking	√	√	√	√	√

Legend, √ Effective, × Ineffective, - Not considered.

This is followed by the schemes in [40,56], which offer four security features and resilience against four attacks. On the other hand, the proposed protocol provides five security features and is robust against six attack vectors. It is, therefore, the most secure among other related schemes.

5.5. Experimentations

In this sub-section, the simulation results of the proposed protocol are presented. Owing to the wide acceptance of the network simulation (NS) tool, its latest version, NS3 (3.32),has been deployed. The host machine is an HP Elitebook Core i7 with 8GB of RAM running on Ubuntu 20.04 LTS. Within the coordinate system, the TA is placed at the origin, while the remote users assume a random mobility model. The communication is over IEEE 802.11, operating at a frequency of 2.4 GHz, while the maximum range for the remote users is a square of 180 meters, whose center is the TA. The speed of the remote users varies from 0 m/s to 5 m/s. On the other hand, the SHDs are randomly placed at locations between 25m and 120 m away from the TA. The number of remote users is varied from 5 to 30, while the number of SHDs ranges from 5 to 25. The simulation is then executed for 10 min as the end-to-end latency and throughput are measured. The obtained end-to-end latency results are shown in Figure 8.

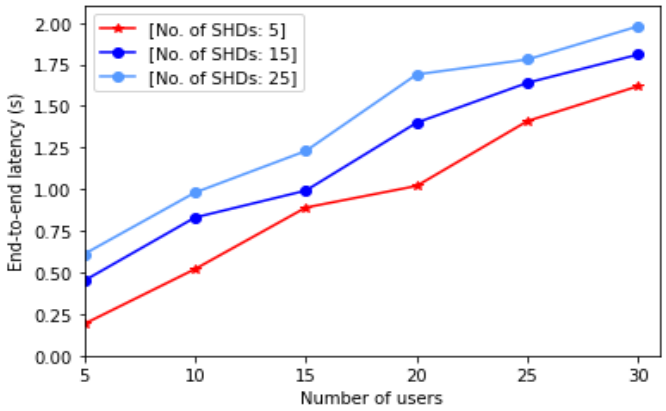

Figure 8. End-to-end latency.

Based on the graphs in Figure 8, the value of end-to-end latency increases with the number of SHDs. It is also evident that as the number of users increases, so does the end-to-end latency. This is explained by the processing delays at the TA as the number of authentication requests surges. The graphs are not entirely linear due to other transmission impairments, such as network congestion and packet losses that may trigger re-transmissions. Figure 9 shows the values for the measured throughput as the number of users and SHDs increments.

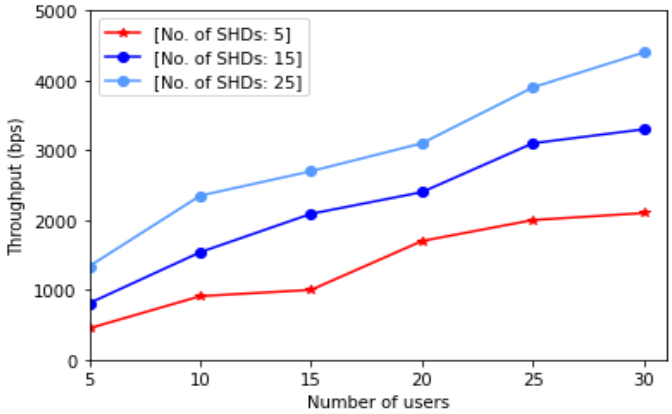

Figure 9. Network throughput.

It is evident from Figure 9 that throughput increases with both the number of users and the number of SHDs. This is attributed to the many bits sent and received across the

network when users and devices increase. However, network congestions and packet drops within the network imply that the graphs are not always linear.

6. Discussion

Smart home IoT devices are exposed to numerous attacks due to their vulnerable environment, low computation power, the tendency of users to utilize default device credentials, and insecure networks. Therefore, many security schemes have been developed to secure the smart home network environment. However, most of these schemes still have numerous flaws that render them vulnerable to attacks. Performance degradation occasioned by highly extensive cryptographic operations is another major issue in smart home networks. To this end, highly efficient technologies such as NB-IoT and LoRaWAN have been developed. However, many vulnerabilities exist in these LPWAN technologies that can be exploited to bring the entire network down. For instance, LoRaWAN uses three keys, *AppKey*, *NwkSKey*, and *AppSKey*, that are exposed to risks during message transmissions, key management procedures, key generation phase at the onset of communication sessions, and in storage at the end devices. If these keys are compromised through side-channeling, then other keys derived using them as the basis can be compromised as well. For instance, the compromise of *NwkSKey* can expose the entire LoRaWAN to attacks. This is because the adversaries are now able to decrypt the exchanged messages. In addition, the LoRaWAN gateway periodically transmits beacons to the network server, and therefore these beacons can be intercepted to launch numerous attacks.

Another serious issue in smart homes is that much attention has been paid to mutually authenticating the remote user to the gateway node, while the mutual authentication between this gateway node and the IoT sensors is largely ignored. In addition, some application layer protocols in IoT, such as the Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (COAP), do not have adequate security protection. As such, they have to depend on the underlying transport layer security protocols. Unfortunately, these protocols exhibit high computation overheads. To this end, a highly efficient protocol has been developed in this paper, which has been demonstrated to offer sufficient privacy and security protection at the lowest computation, storage, and communication costs. Considering the lowest overheads attained in other related schemes, Table 14 presents the percentage improvements achieved by the proposed protocol.

Table 14. Percentage improvements.

Metric	Achieved by	Best Performance	Proposed Protocol Score	Improvement
Computation Costs	Wu et al. [47]	1.0130 ms	0.4285 ms	57.7%
Communication Costs	Shuai et al. [39]	1728	1440	16.7%
Storage overheads	Kaur et al. [40]	384	384	0%

As shown in Table 14, the proposed protocol reduced the computation and communication costs by 42.3% and 16.7%, respectively. Considering the security comparative evaluation in Table 14 above, then it is clear that the proposed protocol records the best performance and also offers salient security features. It is also demonstrated to resist the highest number of attacks. It is, therefore, the most suitable for deployment in the smart home network, where devices are not only resource-limited but also exposed to numerous attacks.

7. Conclusions

Over the recent past, there have been numerous security protocols developed to address security and privacy threats in smart homes. Unfortunately, the majority of these security solutions have performance challenges or still have some security and privacy weaknesses. In this paper, a symmetric key-based authentication protocol is presented. The formal security analysis of the proposed protocol has been accomplished using BAN logic. Based on this formal analysis, it has been demonstrated that the communicating parties negotiate shared session keys for traffic protection over the public internet. In addition, the protocol has been informally analyzed to demonstrate its resilience against common smart home attacks such as packet replays, impersonation, eavesdropping, man-in-the-middle, denial of service, and session hijacking. It has also been demonstrated to provide backward key secrecy, mutual authentication, secret key agreement, device anonymity, and forward key secrecy. Moreover, its performance evaluation has shown that it reduces communication and computation complexities by 16.7% and 57.7%, respectively. Future work lies in the exploration of other cryptographic primitives that can further reduce the reported computation overheads. There is also a need for other innovative ways of assuring the same level of security and privacy using very few message exchanges to reduce communication and storage overheads. The current work was limited to performance evaluation using computation, storage, and communication overheads. There is, therefore,a need to evaluate this protocol using other metrics that were not within the scope of the current work.

Author Contributions: V.O.N. and Z.A.A.; methodology, conceptualization, and writing—original draft preparation, K.A.-A.M.; software, and data curation, I.Q.A. and D.G.H.; validation, and writing—review and editing, J.M.; formal analysis, investigation, supervision, project administration, and funding acquisition, A.J.Y.A.; resources, and visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Natural Science Foundation of Top Talent of SZTU (grant No. 20211061010016).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: All individuals included in this section have consented to the acknowledgment.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors* **2021**, *21*, 1488.
2. Yu, S.; Das, A.K.; Park, Y. Comments on "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes". *IEEE Access***2021**, *9*, 49154–49159.
3. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Lightweight and secure password based smart home authentication protocol: LSP-SHAP. *J. Netw. Syst. Manag.* **2019**, *27*, 1020–1042.
4. Nyangaresi, V.O.; Ogundoyin, S.O. Certificate Based Authentication Scheme for Smart Homes.In Proceedings of the *2021 3rd Global Power, Energy and Communication Conference (GPECOM)*, Antalya, Turkey, 5–8 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 202–207.
5. Qin, Z.; Hu, L.; Zhang, N.; Chen, D.; Zhang, K.; Qin, Z.; Choo, K.K.R. Learning-aided user identification using smartphone sensors for smart homes. *IEEE Internet Things J.* **2019**, *6*, 7760–7772.
6. Huang, Z.; Zhang, L.; Meng, X.; Choo, K.K.R. Key-free authentication protocol against subverted indoor smart devices for smart home. *IEEE Internet Things J.* **2019**, *7*, 1039–1047.
7. Li, Y.; Zhang, Z.; Wang, X.; Lu, E.; Zhang, D.; Zhang, L. A secure sign-on protocol for smart homes over named data networking. *IEEE Commun. Mag.* **2019**, *57*, 62–68.
8. Nyangaresi, V.O. Lightweight Key Agreement and Authentication Protocol for Smart Homes.In Proceedings of the 2021 IEEE AFRICON, Arusha, Tanzania, 13–15 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.

9. Poh, G.S.; Gope, P.; Ning, J. Privhome: Privacy-preserving authenticated communication in smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1095–1107.
10. Do, Q.; Martini, B.; Choo, K.R. Cyber-physical systems information gathering: A smart home case study. *Comput. Netw.* **2018**, *138*, 1–12.
11. Iqbal, W.; Abbas, H.; Deng, P.; Wan, J.; Rauf, B.; Abbas, Y.; Rashid, I. ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes. *IEEE Internet Things J.* **2020**, *8*, 9622–9633.
12. Wang, J.; Li, Y.; Jia, Y.; Zhou, W.; Wang, Y.; Wang, H.; Zhang, Y. Overview of smart home security. *Comput. Res. Dev.* **2018**, *55*, 2111–2124.
13. Ali, B.; Awad, A. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817.
14. Nyangaresi, V.O. ECC Based Authentication Scheme for Smart Homes. In Proceedings of the2021 International Symposium ELMAR,Zadar, Croatia,13–15 September 2021;IEEE:Piscataway, NJ, USA, 2021; pp. 5–10.
15. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495.
16. Gaba, G.S.; Kumar, G.; Monga, H.; Kim, T.H.; Kumar, P. Robust and lightweight mutual authentication scheme in distributed smart environments. *IEEE Access* **2020**, *8*, 69722–69733.
17. Ashibani, Y.; Kauling, D.; Mahmoud, Q.H. Design and implementation of a contextual-based continuous authentication framework for smart homes. *Appl. Syst. Innov.* **2019**, *2*, 4.
18. Nyangaresi, V.O. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *J. Syst. Archit.* **2022**, *133*, 102763.
19. Lin, C.; He, D.; Kumar, N.; Huang, X.; Vijayakumar, P.; Choo, K.K.R. HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet Things J.* **2019**, *7*, 818–829.
20. Nyangaresi, V.O.; Petrovic, N. Efficient PUF Based Authentication Protocol for Internet of Drones. In Proceedings of the2021 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 13–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
21. Islam, R.; Rahman, M.W.; Rubaiat, R.; Hasan, M.M.; Reza, M.M.; Rahman, M.M. LoRa and server-based home automation using the internet of things (IoT). *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 3703–3712.
22. Almuhaya, M.A.; Jabbar, W.A.; Sulaiman, N.; Abdulmalek, S. A survey on Lorawan technology: Recent trends, opportunities, simulation tools and future directions.*Electronics* **2022**, *11*, 164.
23. Ayoub, W.; Mroue, M.; Nouvel, F.; Samhat, A.E.; Prévotet, J.C. Towards ip over lpwans technologies: Lorawan, dash7, nb-iot.In Proceedings of the 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC), Beirut, Lebanon, 25–27 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 43–47.
24. Reddy, G.P.; Kumar, Y.V.P.; Chakravarthi, M.K. Communication Technologies for Interoperable Smart Microgrids in Urban Energy Community: A Broad Review of the State of the Art, Challenges, and Research Perspectives. *Sensors* **2022**, *22*, 5881.
25. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.P.; Chehab, A. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet Things* **2020**, *12*, 100303.
26. Mentsiev, A.U.; Magomaev, T.R. Security threats of NB-IoT and countermeasures. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2020; Volume 862, p. 052033.
27. Rahman, Z.; Yi, X.; Billah, M.; Sumi, M.; Anwar, A. Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics* **2022**, *11*, 1083.
28. Zhang, L.; Li, J. Enabling robust and privacy-preserving resource allocation in fog computing. *IEEE Access* **2018**, *6*, 50384–50393.
29. Zhang, L.; Meng, X.; Choo, K.K.R.; Zhang, Y.; Dai, F. Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 634–647.
30. Abbasinezhad-Mood, D.; Nikooghadam, M. An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an ARM Cortex-M microcontroller. *IEEE Trans. Smart Grid***2017**, *9*, 6194–6205.
31. Dey, S.; Hossian, A. Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sens. Lett.* **2019**, *3*, 1–4.
32. Nyangaresi, V.O.; Mohammad, Z. Privacy Preservation Protocol for Smart Grid Networks. In Proceedings of the2021 International Telecommunications Conference (ITC-Egypt),Alexandria, Egypt, 13–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
33. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Comput. Commun.* **2021**, *166*, 154–164.
34. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2019**, *6*, 580–589.
35. Xiang, A.; Zheng, J. A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks. *Electronics* **2020**, *9*, 989.
36. Shahidinejad, A.; Ghobaei-Arani, M.; Souri, A.; Shojafar, M.; Kumari, S. Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment. *IEEE Consum. Electron. Mag.* **2021**, *11*, 57–63.
37. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet Things J.* **2021**, *9*, 2649–2656.

38. Yang, J.; Huang, G.; Wei, C. "Privacy-aware electricity scheduling for home energy management system. *Peer—PeerNetw. Appl.* **2018**, *11*, 309–317.
39. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146.
40. Kaur, D.; Kumar, D. Cryptanalysis and improvement of a two-factor user authentication scheme for smart home. *J. Inf. Secur. Appl.* **2021**, *58*, 102787.
41. Saqib, M.; Jasra, B.; Moon, A.H. A lightweight three factor authentication framework for IoT based critical applications. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 6925–6937.
42. Nyangaresi, V.O. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. *SN Comput. Sci.* **2022**, *3*, 364.
43. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Susilo, W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 391–406.
44. Prakasam, P.; Madheswaran, M.; Sujith, K.P.; Sayeed, M.S. Low Latency, Area and Optimal Power Hybrid Lightweight Cryptography Authentication Scheme for Internet of Things Applications. *Wirel. Pers. Commun.***2022**, *126*, 351–365.
45. Mishra, D.; Vijayakumar, P.; Sureshkumar, V.; Amin, R.; Islam, S.K.; Gope, P. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimed. Tools Appl.* **2018**, *77*, 18295–18325.
46. Bae, W.I.; Kwak, J. Smart card-based secure authentication protocol in multi-server IoT environment. *Multimed. Tools Appl.* **2020**, *79*, 15793–15811.
47. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimed. Syst.* **2017**, *23*, 195–205.
48. Li, C.; Ji, X.; Zhou, X.; Zhang, J.; Tian, J.; Zhang, Y.; Xu, W. Hlcauth: Key-free and secure communications via home-limited channel. In Proceedings of the Proceedings of the 2018 on Asia Conference on Computer and Communications Security, ACM, Incheon, Republic of Korea,4 June 2018; pp. 29–35.
49. Nyangaresi, V.O. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In Proceedings of the 2022 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 20–22 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
50. Rachedi, A.; Hasnaoui, A. Advanced quality of services with security integration in wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2015**, *15*, 1106–1116.
51. Rachedi, A.; Benslimane, A. Multi-objective optimization for security and QoS adaptation in wireless sensor networks. In Proceedings of the2016 IEEE International conference on communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–7.
52. Gauhar, A.; Ahmad, N.; Cao, Y.; Khan, S.; Cruickshank, H.; Qazi, E.A.; Ali, A. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. *IEEE Access* **2020**, *8*, 58800–58816.
53. Nyangaresi, V.O. Terminal independent security token derivation scheme for ultra-dense IoT networks. *Array* **2022**, *15*, 100210.
54. Miettinen, M.; Nguyen, T.D.; Sadeghi, A.R.; Asokan, N. Revisiting Context-Based Authentication in IoT. In Proceedings of the-Proceedings of the 55th Annual Design Automation Conference, San Francisco, CA, USA, 24–29 June 2018; pp. 1–6.
55. Zhou, K.; Ren, J. PassBio: Privacy-Preserving User-Centric Biometric Authentication. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 3050–3063.
56. Sureshkumar, V.; Amin, R.; Vijaykumar, V.R.; Sekar, S.R. Robust secure communication protocol for smart healthcare system with FPGA implementation. *Future Gener. Comput. Syst.* **2019**, *100*, 938–951.
57. Kumar, V.; Malik, N.; Singla, J.; Jhanjhi, N.Z.; Amsaad, F.; Razaque, A. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography* **2022**, *6*, 37.
58. Sciancalepore, S.; Piro, G.; Boggia, G.; Bianchi, G. Public key authentication and key agreement in IoT devices with minimal airtime consumption. *IEEE Embed. Syst. Lett.* **2017**, *9*, 1–4.
59. Wazid, M.; Das, A.K.; Vasilakos, A.V. Authenticated key management protocol for cloud-assisted body area sensor networks. *J. Netw. Comput. Appl.* **2018**, *123*, 112–126.
60. Lyu, Q.; Zheng, N.; Liu, H.; Gao, C.; Chen, S.; Liu, J. Remotely access "my" smart home in private: An anti-tracking authentication and key agreement scheme. *IEEE Access* **2019**, *7*, 41835–41851.
61. Irshad, A.; Usman, M.; Chaudry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-loop-driven low-cost and secure biometric user access to server. *IEEE Trans. Reliab.* **2020**, *70*, 1014–1025.
62. Rahman, Z.; Khalil, I.; Yi, X.; Atiquzzaman, M. Blockchain-based security framework for a critical industry 4.0 cyber-physical system. *IEEE Commun. Mag.* **2021**, *59*, 128–134.
63. Rahman, Z.; Yi, X.; Khalil, I. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet Things J.***2022**, 1–10.10.1109/JIOT.2022.3147186
64. Nyangaresi, V.O.; Ahmad, M.; Alkhayyat, A.; Feng, W.Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. *Expert Syst.* **2022**, *39*, e13126.
65. Alshahrani, M.; Traore, I. Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain. *J. Inf. Secur. Appl.* **2019**, *45*, 156–175.
66. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Park, Y. An efficient, anonymous and robust authentication scheme for smart home environments. *Sensors* **2020**, *20*, 1215.

67. Fadi, A.T.; Deebak, B.D. Seamless authentication: ForIoT-big data technologies in smart industrial application systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2919–2927.