




Article

Fortifying Smart Home Security: A Robust and Efficient User-Authentication Scheme to Counter Node Capture Attacks

Iqra Asghar ¹, Muhammad Ayaz Khan ², Tahir Ahmad ^{3,*} , Subhan Ullah ⁴ , Khwaja Mansoor ul Hassan ¹ and Attaullah Buriro ^{5,*} 

- ¹ Department of Cybersecurity, Air University Islamabad, Islamabad 44000, Pakistan; iqraasghar064@gmail.com (I.A.); mansoor.hassan@mail.au.edu.pk (K.M.u.H.)
² Department of Computer Science, Air University Islamabad, Islamabad 44000, Pakistan; ayaz.khan@mail.au.edu.pk
³ Center for Cybersecurity, Brunno Kessler Foundation, 38123 Trento, Italy
⁴ Faculty of Computer Science, National University of Computer and Emerging Sciences (NUCES-FAST), Islamabad 44000, Pakistan; subhan.ullah@nu.edu.pk
⁵ Faculty of Engineering, Free University Bozen-Bolzano, 39100 Bolzano, Italy
* Correspondence: ahmad@fbk.eu (T.A.); attaullah.buriro@unibz.it (A.B.)

Abstract: In smart home environments, the interaction between a remote user and devices commonly occurs through a gateway, necessitating the need for robust user authentication. Despite numerous state-of-the-art user-authentication schemes proposed over the years, these schemes still suffer from security vulnerabilities exploited by the attackers. One severe physical attack is the node capture attack, which allows adversaries to compromise the security of the entire scheme. This research paper advances the state of the art by conducting a security analysis of user-authentication approaches regarding their vulnerability to node capture attacks resulting in revelations of several security weaknesses. To this end, we propose a secure user-authentication scheme to counter node capture attacks in smart home environments. To validate the effectiveness of our proposed scheme, we employ the BAN logic and ProVerif tool for verification. Lastly, we conduct performance analysis to validate the lightweight nature of our user-authentication scheme, making it suitable for IoT-based smart home environments.



Citation: Asghar, I.; Khan, M.A.; Ahmad, T.; Ullah, S.; Mansoor ul Hassan, K.; Buriro, A. Fortifying Smart Home Security: A Robust and Efficient User-Authentication Scheme to Counter Node Capture Attacks. *Sensors* **2023**, *23*, 7268. <https://doi.org/10.3390/s23167268>

Academic Editor: Xiaojie Wang

Received: 14 July 2023

Revised: 14 August 2023

Accepted: 18 August 2023

Published: 19 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: smart home security; user authentication; node capture attack

1. Introduction

The Internet of Things (IoT) has rapidly expanded, with many interconnected physical nodes exchanging data and information [1]. The growth of IoT devices is expected to reach approximately 38.6 billion connections by 2025 [1]. These devices find applications in both consumer and industrial domains, and the smart home environment is emerging as a prominent usecase [2–4]. Smart homes have numerous interconnected devices that enable remote users to manage and control their home appliances.

As the number of devices within IoT networks continues to increase, it becomes crucial to address management and security concerns for remote users. Security, in particular, poses a significant challenge for IoT networks, necessitating secure information exchange with attributes such as confidentiality, integrity, and availability to resist potential security attacks [5,6]. Among the security challenges in IoT, ensuring data privacy, authentication, authorization, and access control are critical [7,8]. Authentication, a fundamental security requirement, is especially challenging in smart home environments due to the resource-constrained nature of the devices [9,10].

To overcome these challenges and achieve secure user authentication, numerous user-authentication schemes for IoT-based smart home environments have been proposed in the literature. However, these authentication schemes often focus on general security

attributes and neglect the threat of node capture attacks, particularly severe in resource-constrained devices within smart home environments. Without protection against node capture attacks, an adversary can compromise an authentication scheme, underscoring the need to design user-authentication schemes that provide mutual authentication and resist such attacks' consequences.

The proposed scheme in this work is a lightweight authentication solution designed to address the security challenges faced in the smart home environment. Figure 1 illustrates a simplified IoT smart home environment architecture comprising smart devices, a gateway, and a mobile user. Smart devices can be tamper-proof or non-tamper-proof, collecting information for the mobile user in the environment. The gateway is a robust and tamper-proof node, bridging remote users (i.e., a participant who accesses and retrieves information from the deployed smart devices through the gateway) and smart devices. It is responsible for system monitoring and control. The proposed authentication scheme aims to provide user authentication, key agreement, sound repairability, no location tracking, user anonymity, forward secrecy, no password exposure, resistance to known attacks, and resistance to node capture attacks. The proposed scheme offers robust protection against unauthorized access and malicious activities by incorporating these essential security features. Furthermore, the scheme is designed to be computationally and communicationally efficient, making it suitable for resource-constrained environments.

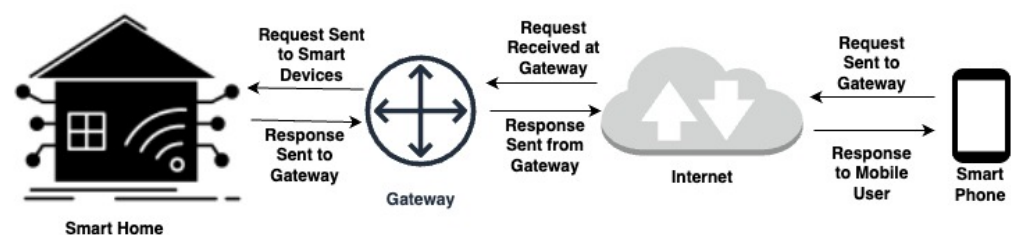


Figure 1. IoT-based smart home network.

The contributions of this paper are as follows, emphasizing the innovation brought forth by our study:

- We comprehensively analyze prevailing authentication mechanisms vulnerable to node capture attacks in IoT-based smart home environments. Our assessment identifies the shortcomings and security gaps present in these mechanisms.
- We introduce a novel user-authentication scheme designed to counter node capture attacks and fortify the security posture of IoT-based smart homes. This scheme is a pioneering response to the evolving threats in this domain.
- Our proposed scheme undergoes rigorous formal and informal analyses to validate its security strength. This ensures that our solution meets the stringent security requirements expected in smart home environments.
- We demonstrate a marked improvement in computation and communication costs compared to existing approaches through meticulous performance analysis. This efficiency enhancement is a significant advancement in IoT-based smart home security.

Paper Organization: The rest of the paper is organized as follows: Section 2 provides an overview of the existing literature on the topic. Section 3 explains the fundamental idea behind our proposed authentication scheme, emphasizing its lightweight nature. Section 4 discusses the underlying threat model for conducting formal and informal security analyses. Section 5 performs a security analysis of the suggested scheme to evaluate its robustness against potential attacks using BAN logic and ProVerif. Section 6 presents an informal security analysis of the proposed authentication scheme, further exploring its strengths and weaknesses. Section 7 reports on the performance evaluation of our approach, focusing on computation and communication costs. Section 8 summarizes our major findings and discusses potential future research directions.

2. Related Work

Many user-authentication schemes have surfaced in the literature in IoT-based smart home environments. These schemes share the goal of providing robust authentication mechanisms, although they exhibit varying effectiveness and security vulnerabilities. In this section, we explore the notable contributions in the field and present a meticulous comparative analysis of their respective schemes.

Vaidya et al. [11] proposed a password-based authentication protocol for smart homes, employing HMAC-based one-time passwords and smart card technology. They claim mutual authentication features and forward secrecy, which prevents the exploitation of stolen smart cards and clock-synchronization attacks. However, further analysis revealed vulnerabilities in their scheme, including susceptibility to password-guessing and user-impersonation attacks. Kim et al. [12] studied and analyzed these security vulnerabilities and proved that Vaidya et al.'s protocol is vulnerable to password-guessing and user-impersonation attacks. They proposed a solution incorporating hash-based one-time password algorithms and hash chaining to address these weaknesses. However, the Kim et al. scheme is still vulnerable to the same issues identified in Vaidya et al.'s protocol.

Li [13] proposed a key establishment scheme for secure smart home energy management systems. This scheme manages and stores multiple keys and certificates, enabling secure device communication. However, the scheme suffers from computation overhead due to the large number of keys and certificates it handles. Additionally, it lacks the crucial feature of mutual authentication between the user device and smart devices, leaving it susceptible to impersonation attacks. Similarly, Santoso et al. [14] designed an elliptic curve cryptography (ECC)-based user-authentication scheme for IoT-based smart home systems and addressed the issues of mutual authentication. Their protocol achieves mutual authentication between IoT devices and mobile users with the help of a central gateway node (GWN). However, their scheme does not provide user anonymity and untraceability features, making it vulnerable to insider attacks like smart card theft.

Similarly, Kumar et al. [15] also proposed a lightweight authentication and session key establishment protocol for IoT-based smart home systems. Their scheme claims resistance against notable attacks like key-stolen attacks. However, it does not provide mutual authentication between the mobile user and smart device and lacks user anonymity and untraceability features. The mutual authentication issues have been further addressed. Wazid et al. [16] designed a lightweight remote user-authentication protocol suitable for resource-constrained IoT-based smart home systems devices. The weakness in their scheme is reliance on a verification table on the GWN node for authentication purposes. This introduces other vulnerabilities that make the scheme susceptible to synchronization attacks. All the above schemes lack user anonymity and untraceability features.

Table 1 presents a comparative analysis of the discussed user-authentication schemes for IoT-based smart home systems. The table includes an evaluation of each scheme based on mutual authentication, user anonymity, untraceability, and identified vulnerabilities.

The comparative analysis shows that the existing user-authentication schemes for IoT-based smart home systems have various vulnerabilities and lack essential security features. Therefore, there is a need for an improved user authentication protocol that addresses these flaws and provides a higher level of security. In the following sections, we propose a novel and improved user-authentication scheme for IoT-based smart home systems, which mitigates identified vulnerabilities and enhances overall security. We also perform a detailed security analysis of our proposed scheme.

Table 1. Comparative analysis of user-authentication schemes for IoT-based smart home systems.

Scheme	Mutual Authentication	User Anonymity	Untraceability	Vulnerabilities
Vaidya et al. [11]	Yes	No	No	Password-guessing, user-impersonation
Kim et al. [12]	Yes	No	No	Password-guessing, user impersonation
Li [13]	No	No	No	Computation overhead, lack of mutual authentication
Santoso et al. [14]	Yes	No	No	Insider attacks, lack of user anonymity
Kumar et al. [15]	No	No	No	Lack of mutual authentication, user anonymity
Wazid et al. [16]	Yes	No	No	Synchronization attacks

3. Threat Model

The threat model is an essential component of the security analysis, providing a clear understanding of the attacker's assumptions and capabilities within the protocol's context. In this section, we define the threat model based on the Dolev–Yao model [17] and outline the assumptions made regarding the adversary, referred to as Eve.

Assumptions

- **Communication Interception:** Eve can intercept, inject, remove, or send new messages when two participants communicate over the public channel. This means that any information exchanged over the public channel is susceptible to manipulation or eavesdropping by Eve.
- **Parameter Understanding:** Eve can understand all the parameters exchanged over the public channel. This implies that Eve can analyze and comprehend the content of the messages transmitted between participants.
- **Attacker Identity:** Eve can be an outsider or a dishonest participant within the system. This encompasses the possibility of external attackers attempting to compromise the system's security and internal attackers with insider knowledge or unauthorized access.
- **Gateway Security:** The gateway, which plays a crucial role in the protocol, is assumed to be a secure entity. This means Eve cannot compromise the gateway or gain unauthorized access to its resources or sensitive information.
- **Secret Parameter Protection:** Eve cannot access the secret parameters used in the protocol. These secret parameters are assumed to be securely transmitted between the relevant parties and are not accessible or known to Eve.

By outlining these assumptions, the threat model provides a clear understanding of the capabilities and limitations of the attacker within the proposed protocol. It helps identify potential vulnerabilities and design appropriate security measures to mitigate them.

4. Proposed User-Authentication Scheme

The proposed protocol follows a general network model used in smart home environments, as depicted in Figure 1. Based on the analysis of state-of-the-art solutions, we have

designed a user-authentication scheme to address the identified security vulnerabilities. Figure 2 presents the proposed user authentication protocol. Additionally, Table 2 provides a guide to the notations and abbreviations used in the protocol.

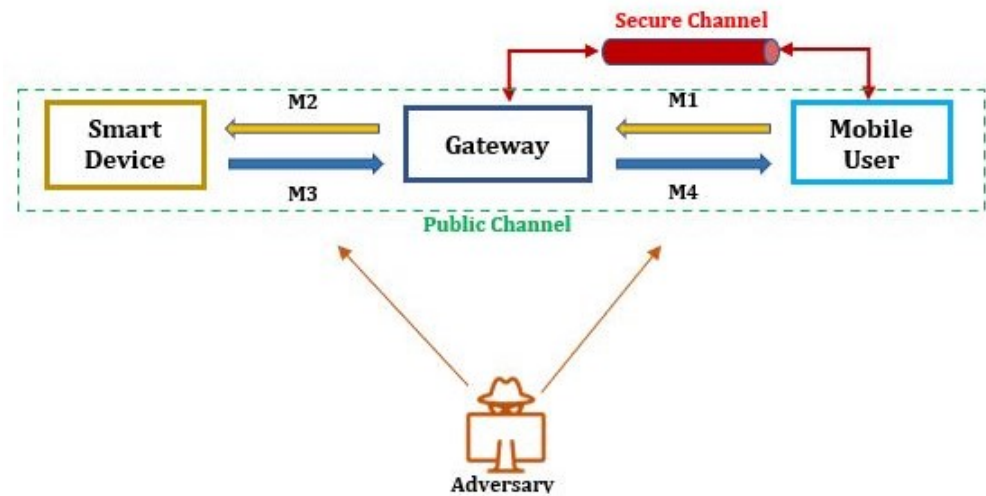


Figure 2. Proposed user authentication protocol.

Table 2. Notation guide of proposed protocol.

Notations	Description
ID_{U_i}	User Identity
U_i	User
TID_{U_i}	Temporary Identity
K_{UG}	Shared Keys between Gateway and Mobile User
K_{GS}	Shared Keys between Gateway and Smart Device
k	Secret key of Gateway
t	Timestamp
L_C	Current Location
X_n	History of Location
V_1, V_2, V_3, V_4	Verification Parameter
SD_i	Smart Device
SID_j	Smart Device Identity
ID_{GW}	Gateway Identity
$TID_{U_i(new)}$	New Temporary Identity
$r_{U_i}, N_H, r_{U_i}, N_v$	Random Numbers
\oplus	The exclusive XOR Operation
\parallel	Concatenation
h	Hash

4.1. Assumptions

- During the pre-deployment phase of smart devices in the network, it is assumed that the gateway has shared its identity credential and the hash of the shared key $h(K_{GS})$ with the smart devices.
- Each smart device has a unique identity and a shared key K_{GS} established between the device and the gateway.
- The identity of the gateway (ID_{GW}) is known to all participants.
- Every mobile user knows the identities of the smart devices.
- The gateway is considered a trusted entity within the smart home network.
- Both tamper-resistant and non-tamper-resistant smart devices are in the smart home network. Tamper-resistant devices are secure against node capture attacks, while non-tamper-resistant devices are vulnerable.

- The registration stage of the proposed protocol is carried out over a secure channel.
- The mobile user has the mechanism to extract and calculate location information and is capable of storing location history.

4.2. Stages of the Proposed Protocol

The proposed user authentication protocol consists of two stages:

4.2.1. Registration Stage

In the registration stage, the gateway issues security credentials to mobile devices. When a new mobile user (U_i) attempts to access a smart device, they must register the mobile device with the gateway. The registration process, illustrated in Figure 3, involves the following steps:

Step 1: The new mobile user (U_i) submits their unique ID_{U_i} to the gateway. $M_1 = \{ID_{U_i}\}$

Step 2: The gateway generates two random numbers (N_H and r_{u_i}) and computes the shared secret key (K_{UG}) shared between the user and the gateway. The gateway also computes the temporary identity TID_{U_i} by encrypting the user's identity (ID_{U_i}) concatenated with the random number (r_{u_i}) using the secret key (k).

$$K_{UG} = h(ID_{U_i} || N_H) \oplus ID_{GW}$$

$$TID_{U_i} = E_k(ID_{U_i} || r_{u_i})$$

Step 3: The gateway stores and sends the message (M_2) to the requesting user (U_i).

$$M_2 = \{TID_{U_i}, K_{UG}\}$$

After receiving the message (M_2) from the gateway, the user stores it on their mobile device.

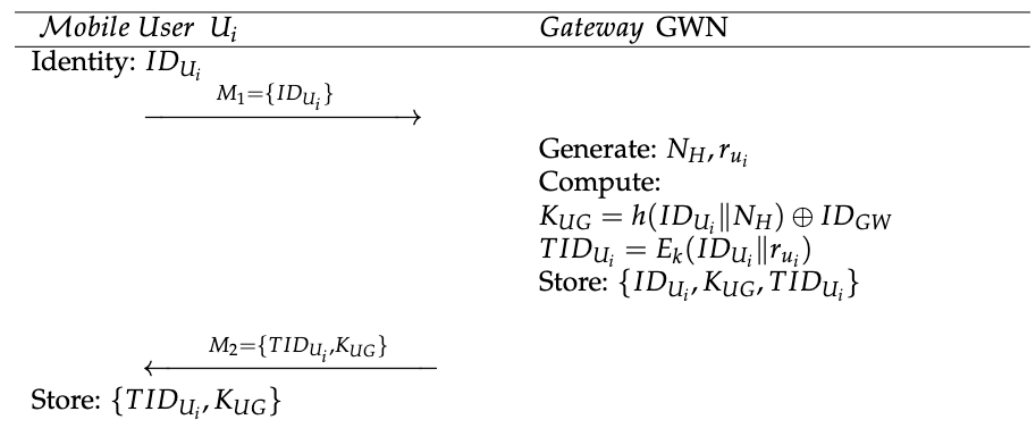


Figure 3. Registration stage of the protocol.

4.2.2. Authentication Stage

A registered mobile user can access a smart device after successful mutual authentication and establishing a session key with the smart device through the gateway. This stage, illustrated in Figure 4, involves the following steps:

At the Mobile User Side:

Step 1: The mobile device generates a random number (N_v) and calculates the parameter (N_y).

$$N_y = N_v \oplus K_{UG}$$

Step 2: The mobile device obtains its current location (L_C) and computes the parameter (N_C). With this parameter, the gateway can easily derive the current location using the shared secret key (K_{UG}) stored at the gateway. The mobile user also manages the session's location history (X_n).

$$N_C = L_C \oplus K_{UG}$$

$$X_n = h(X_{n-1} \| L_C)$$

Step 3: The mobile user selects a smart device (SID_j) and computes the parameter (SD_q). The parameter Y_n is the hash of the user's location parameters and the entities' identities.

$$Y_n = h(ID_{GW} \| TID_{U_i} \| L_C \| X_n)$$

$$SD_q = Y_n \oplus SID_j \oplus K_{UG}$$

Step 4: The mobile user computes the verification parameter (V_1) after generating the timestamp (T_1). Then, the mobile user sends the message (M_1) to the gateway.

$$V_1 = h(TID_{U_i} \| K_{UG} \| ID_{GW} \| T_1)$$

Message M_1 Passed from Remote User to Gateway

At the Gateway Side:

Step 1: Upon receiving the message (M_1), the gateway generates the timestamp (T_2). It checks the condition $T_2 - T_1 \leq \Delta T$ and verifies the TID_{U_i} using its secret key (k) and the shared key (K_{UG}) derived from the parameter N_y . The gateway also checks the verification parameter (V_1).

$$N_v = K_{UG} \oplus N_y$$

$$V_1 \stackrel{?}{=} h(TID_{U_i} \| K_{UG} \| ID_{GW} \| T_1)$$

Step 2: After successfully verifying V_1 , the gateway derives the current location from the parameter N_C and recalculates the location history (X_n) using the previous location history value stored on the gateway from the previous session.

$$L_C = K_{UG} \oplus N_C$$

Step 3: The gateway calculates the parameter Y_n and compares the calculated value with the derived parameter Y_n (from the user's parameter U_G) to verify the mobile user based on their location parameters. Then, the targeted smart device identity is extracted from SD_q .

$$Y_n = K_{UG} \oplus U_G \| TID_{U_i}$$

$$Y_n \stackrel{?}{=} h(ID_{GW} \| TID_{U_i} \| L_C \| X_n)$$

$$SID_j = Y_n \oplus SD_q \oplus X_n$$

Step 4: After the above conditions are satisfied, the gateway computes the verification parameter V_2 .

$$V_2 = h(h(K_{GS}) \| SID_j \| ID_{GW} \| TID_{U_i} \| T_2)$$

Message (M_2) Passed from Gateway to Smart Device

At the Smart Device Side:

Step 1: The smart device generates the timestamp (T_3) and compares it with the receiving time (T_2) of the message (M_2). It also verifies the verification parameter (V_2). All smart devices store their identities and the hash of their shared secret keys.

$$T_3 - T_2 \leq \Delta T$$

$$V_2 \stackrel{?}{=} h(h(K_{GS}) \| SID_j \| ID_{GW} \| TID_{U_i} \| T_2)$$

Step 2: After successfully verifying V_2 , the smart device computes the verification parameter V_3 and sends message M_3 to the gateway.

$$V_3 = h(h(K_{GS})\|SID_j\|ID_{GW}\|TID_{U_i}\|T_3)$$

Message Passed from Smart Device to Gateway

At the Gateway Side:

Step 1: Upon receiving the message M_3 , the gateway checks the condition $T_4 - T_3 \leq \Delta T$. It verifies the timestamp and the verification parameter V_3 . If the verification fails, the session is terminated.

$$T_4 - T_3 \leq \Delta T$$

$$V_3 \stackrel{?}{=} h(h(K_{GS})\|SID_j\|ID_{GW}\|TID_{U_i}\|T_3)$$

Step 2: If the above conditions are satisfied, the gateway updates the temporary identity by encrypting the saved user identity (ID_{U_i}) with its secret key (k) along with a new random number (r_{new}).

$$TID_{U_i(new)} = E_k(ID_{U_i}\|r_{new})$$

Step 3: The gateway computes the parameter Z_n and the verification parameter V_4 . It then sends the message (M_4) to the mobile user.

$$Z_n = K_{UG} \oplus TID_{U_i(new)}$$

$$V_4 = h(N_v\|T_4\|K_{UG}\|Z_n)$$

Message Passed from Gateway to Mobile User

At the Mobile User Side:

Step 1: The mobile user generates the timestamp (T_5) and compares it to the timestamp (T_4).

$$T_5 - T_4 \leq \Delta T$$

Step 2: The mobile user extracts the value of the new temporary identity ($TID_{U_i(new)}$) from the parameter Z_n and verifies the verification parameter V_4 .

$$TID_{U_i(new)} = Z_n \oplus K_{UG}$$

$$V_4 \stackrel{?}{=} h(N_v\|T_4\|K_{UG}\|Z_n)$$

Step 3: If the condition $TID_{U_i(new)} = TID_{U_i}$ is satisfied, the session is terminated. Otherwise, it implies that the mobile user has successfully authenticated the smart device. Finally, the mobile user updates the temporary identity.

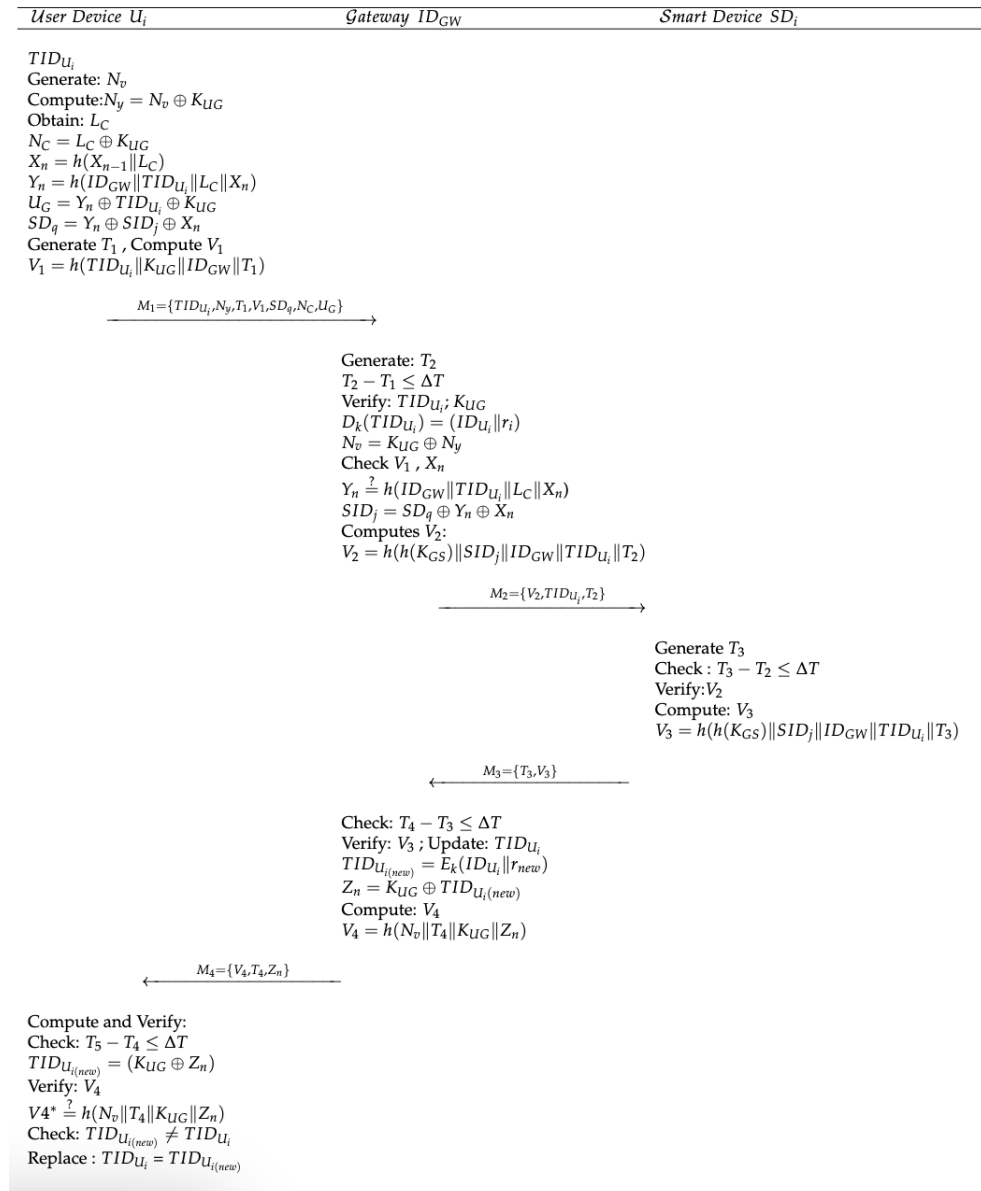


Figure 4. Proposed authentication scheme.

5. Security Analysis of the Proposed Scheme

The security analysis of the proposed protocol is conducted to assess its strength and resilience against various attacks. The analysis is performed by considering a threat model (defined in Section 3) and employing BAN logic [18,19] and ProVerif [20,21].

5.1. Security Analysis with BAN Logic

BAN logic provides a set of defined rules for the formal analysis of authentication protocols [18]. It applies various logical rules to determine whether a protocol achieves its authentication goals [19]. The BAN logic notations are shown in Table 3. In the proposed scheme, eight goals are derived using BAN logic, as outlined below:

- Goal 1: $GWN | \equiv U_i \xrightarrow{TID_{U_i}} GWN$
- Goal 2: $GWN | \equiv U_i | \equiv U_i \xrightarrow{TID_{U_i}} GWN$
- Goal 3: $SID_j | \equiv GWN \xrightarrow{TID_{U_i}} SID_j$
- Goal 4: $SID_j | \equiv GWN | \equiv GWN \xrightarrow{TID_{U_i}} SID_j$

- Goal 5: $GWN | \equiv SID_j \xleftrightarrow{TID_{U_i}} GWN$
- Goal 6: $GWN | \equiv SID_j | \equiv SID_j \xleftrightarrow{TID_{U_i}} GWN$
- Goal 7: $U_i | \equiv GWN \xleftrightarrow{TID_{U_i}} U_i$
- Goal 8: $U_i | \equiv GWN | \equiv GWN \xleftrightarrow{TID_{U_i}} U_i$

Table 3. Notation Guide for BAN Logic.

Notations	Description
$P \equiv X$	P believes on X
$P \triangleleft X$	P sees that X
$P \sim X$	P once said X
$P \Rightarrow X$	P has total jurisdiction on X
$\#(X)$	X is updated and fresh
(X, Y)	x,y is component of formula(x,y)
$(X)_k$	Hash of message X using a key K
$\langle X \rangle_y$	X is combined with y
$P \xleftrightarrow{K} Q$	P and Q are using shared key K for communication process
TID_{U_i}	Session key TID_{U_i} is used one time in a current session
$\frac{P \equiv P \xleftrightarrow{K} Q, P \triangleleft \langle X \rangle_K}{P \equiv Q \sim X}$	Message Meaning rule
$\frac{P \equiv \#(X)}{P \equiv \#(X, Y)}$	Freshness Concatenation rule
$\frac{P \equiv \#(X), P \equiv Q \sim X}{P \equiv Q \equiv X}$	Nonce verification
$\frac{P \equiv Q \Rightarrow X, P \equiv Q \equiv X}{P \equiv X}$	Jurisdiction rule

The idealized form of the protocol is analyzed using BAN logic, and the results are as follows:

Part 1: Idealized Protocol Form

- M-1: $U_i \rightarrow GWN: TID_{U_i}, V_1, T_1, N_y : \langle N_v \rangle KUG, SD_q : \langle Y_n, SID_j, X_n \rangle, U_G : \langle Y_n, TID_{U_i} \rangle KUG$
- M-2: $GWN \rightarrow SID_j: TID_{U_i}, V_2, T_2$
- M-3: $SID_j \rightarrow GWN: V_3, T_3$
- M-4: $GWN \rightarrow U_i: V_4, T_4, Z_n : \langle TID_{U_i(new)} \rangle KUG$

Part 2: Assumptions

The following assumptions are considered for the analysis:

- A1: $U_i | \equiv (N_v)$
- A2: $GWN | \equiv (r_i)$
- A3: $SID_j | \equiv (T_3)$
- A4: $GWN | \equiv SID_j \Rightarrow T_3$
- A5: $GWN | \equiv U_i \Rightarrow N_v$
- A6: $SID_j | \equiv GWN \Rightarrow T_2$
- A7: $SID_j | \equiv U_i \Rightarrow N_V$
- A8: $U_i | \equiv SID_j \Rightarrow T_3$
- A9: $U_i | \equiv GWN \Rightarrow r_i$

Using the BAN logic rules, the analysis proceeds as follows:

Message 1:

M-1: $U_i \rightarrow GWN: TID_{U_i}, N_y : \langle N_v \rangle KUG, SD_q : \langle Y_n, SID_j, X_n \rangle, T_1$ is U_i 's timestamp

By applying the Seeing rule, the following is obtained:

- S-1: $GWN \triangleleft TID_{U_i}, N_y : \langle N_v \rangle KUG, T_1, V_1$

By applying the Message Meaning rule and S-1, the following is obtained:

- S-2: $GWN| \equiv U_i| \sim N_v$

By applying the Freshness Concatenation rule and S-2, the following is obtained:

- S-3: $GWN| \equiv U_i| \equiv N_v$

By applying the Jurisdiction rule and S-3, the following is obtained:

- S-4: $GWN| \equiv N_v$

By applying S-4 and the Session Key rule, the following is obtained:

- S-5: $GWN| \equiv U_i \xleftrightarrow{TID_{U_i}} GWN$ (**Goal 1**)

By applying the Nonce Verification rule, the following is obtained:

- S-6: $GWN| \equiv U_i| \equiv U_i \xleftrightarrow{TID_{U_i}} GWN$ (**Goal 2**)

Message 2:

M-2: $GWN \rightarrow SID_j: TID_{U_i}, T_2, V_2$. T_2 is the timestamp of GWN

By applying the Seeing rule, the following is obtained:

- S-7: $SID_j \triangleleft TID_{U_i}, T_2, V_2$

By applying the Message Meaning rule and S-7, the following is obtained:

- S-8: $SID_j| \equiv GWN| \sim T_2$

By applying the Freshness Concatenation rule and S-8, the following is obtained:

- S-9: $SID_j| \equiv GWN| \equiv r_i$

By applying the Jurisdiction rule and S-9, the following is obtained:

- S-10: $SID_j| \equiv r_i$

By applying S-10 and the Session Key rule, the following is obtained:

- S-11: $SID_j| \equiv GWN \xleftrightarrow{TID_{U_i}} SID_j$ (**Goal 3**)

By applying the Nonce Verification rule and S-11, the following is obtained:

- S-12: $SID_j| \equiv GWN| \equiv GWN \xleftrightarrow{TID_{U_i}} SID_j$ (**Goal 4**)

Message 3:

M-3: $SID_j \rightarrow GWN: V_3, T_3$, T_3 is the timestamp of SID_j

By applying the Seeing rule, the following is obtained:

- S-13: $GWN \triangleleft V_3, V_4, T_3$

By applying the Message Meaning rule and S-13, the following is obtained:

- S-14: $GWN| \equiv SID_j| \sim T_3$

By using S-14 and the Freshness Concatenation rule, the following is obtained:

- S-15: $GWN| \equiv SID_j| \equiv T_3$

By applying the assumption S-15 and the Jurisdiction rule, the following is obtained:

- S-16: $GWN| \equiv T_3$

By applying S-16 and the Session Key rule, the following is obtained:

- S-17: $GWN| \equiv SID_j \xleftrightarrow{TID_{U_i}} GWN$ (**Goal 5**)

By applying the Nonce Verification rule, the following is obtained:

- S-18: $GWN| \equiv SID_j| \equiv SID_j \xleftrightarrow{TID_{U_i}} GWN$ (**Goal 6**)

Message 4:

M-4: $GWN \rightarrow U_i: V_4, T_4, Z_n :< TID_{U_i(new)} > KUG, T_4$ is the timestamp of GWN
 By applying the Seeing rule, the following is obtained:

- S-19: $U_i \triangleleft V_4, Z_n < TID_{U_i(new)} > KUG, T_4$

By applying the Message Meaning rule and S-19, the following is obtained:

- S-20: $U_i | \equiv GWN | \sim TID'_{U_i(new)}$

By applying S-20 and the Freshness Concatenation rule, the following is obtained:

- S-21: $U_i | \equiv GWN | \equiv TID_{U_i(new)}$

By applying the Jurisdiction rule and S-21, the following is obtained:

- S-22: $U_i | \equiv TID_{U_i(new)}$

By applying the Session Key rule, the following is obtained:

- S-23: $U_i | \equiv GWN \xleftrightarrow{TID_{U_i(new)}} U_i$ (**Goal 7**)

By applying the Nonce Verification rule, the following is obtained:

- S-24: $U_i | \equiv GWN | \equiv GWN \xleftrightarrow{TID_{U_i(new)}} U_i$ (**Goal 8**)

After analyzing the scheme using BAN logic, it can be concluded that the proposed protocol achieves mutual authentication and securely establishes session key agreement.

5.2. Security Analysis with ProVerif

ProVerif is an automatic tool used for analyzing the security of cryptographic protocols [20]. It verifies that an attacker cannot extract sensitive data from encrypted messages as long as the key remains secret [21]. The detailed process of all queries and their respective results can be found in Table 4.

The following is the interpretation of the query-wise result of the ProVerif analysis.

- Query 1: The query “not attacker(TIDUinew[])” returns true, indicating that the new identity (TIDUinew) is secure from attacks.
- Query 2: The query “inj-event(end_U(IDUi[])) ==>inj-event(start_U(IDUi[]))” returns true, indicating that the connection functions securely for starting and closing on the user mobile.
- Query 3: The query “inj-event(end_GWN(IDGW[])) ==>inj-event(start_GWN(IDGW[]))” returns true, indicating that the connection on the gateway node is securely opened and closed.
- Query 4: The query “inj-event(end_SD(SIDj[])) ==>inj-event(start_SD(SIDj[]))” returns true, indicating that the connection on the smart devices is securely opened and closed.

The ProVerif analysis confirms that the proposed protocol is secure and achieves the intended security properties of secrecy and authentication.

Table 4. Security analysis through ProVerif.

Query	ProVerif Response
1-Query inj-event(end_U(TIDUinew[])) ==\textgreater inj-event(start_U(TIDUinew[])) Completing...Starting query not attacker(TIDUinew[])	RESULT not attacker(TIDUinew[]) is true.
2-Query inj-event(end_U(IDUi[])) ==>inj-event(start_U(IDUi[])) Completing... Starting query inj-event(end_U(IDUi[])) ==>inj-event(start_U(IDUi[])) &==>inj-event(start_U(IDUi[])) is true.	&RESULT inj-event(end_U(IDUi[]))

Table 4. Cont.

Query	ProVerif Response
3-Query inj-event(end_GWN(IDGW[]))=>inj-event(start_GWN(IDGW[])) Completing... Starting query inj-event(end_GWN(IDGW[]))=>inj-event(start_GWN(IDGW[])) &==>inj-event(start_GWN(IDGW[])) is true.	&RESULT inj-event(end_GWN(IDGW[]))
4-Query inj-event(end_SD(SIDj[]))=>inj-event(start_SD(SIDj[])) Completing... Starting query inj-event(end_SD(SIDj[]))=>inj-event(start_SD(SIDj[])) &==>inj-event(start_SD(SIDj[])) is true.	&RESULT inj-event(end_SD(SIDj[]))

6. Informal Security Analysis

This section presents a security requirements analysis for user authentication protocols, focusing on the resistance to node capture attacks. Both general and specific functional and security requirements have been utilized to achieve the intended security properties of the schemes. Our proposed approach achieves all the security requirements, especially resistance to known attacks and node capture attacks, by comparing with the existing approaches [15,16,22–24], as shown in Table 5. Therefore, the rest of the discussion primarily focuses on how the proposed scheme withstands node capture attacks.

6.1. Resistance to Node Capture Attack

To evaluate the proposed user authentication protocol's resilience against node capture attacks, we adopt the approach presented by Wang et al. [25]. The detailed explanation of each attack target is as follows:

6.1.1. Mobile User (Attack Target)

Exploited Vulnerabilities → Attack Consequences

- Insecure Identity Transmission $\xrightarrow{\text{Attack}}$ Break User Anonymity
In the proposed protocol, the mobile user does not use its original identity but instead employs a temporary identity updated by the gateway in each session.
- Insecure Transmission of Secret Key $\xrightarrow{\text{Attack}}$ Obtain Secret Key
The mobile user does not directly transmit its shared secret key K_{UG} in the exchanged messages. Instead, K_{UG} is used to encrypt various parameters (N_Y, N_C, U_G, V_1) with the help of random numbers and other secret parameters. Therefore, the key K_{UG} remains secure and cannot be extracted by an adversary.

6.1.2. Smart Device (Attack Target)

- Improper Distribution of Secret Key $\xrightarrow{\text{Attack}}$ Obtain Secret Key of All Target Smart Devices
Each smart device possesses a unique shared secret key with the gateway. If a node capture attack compromises a smart device (SID_j), the adversary cannot compromise the shared secret key of other smart devices.
- Exposure of User's Secret Parameter $\xrightarrow{\text{Attack}}$ Impersonate the User
During the authentication phase, the mobile user's secret parameters are not forwarded in exchanged messages. These secret parameters encrypt the parameters exchanged over the public channel and a random number. If a compromised smart device attempts to compute the user's secret parameters, it will fail to extract any

relevant information. Hence, an adversary cannot impersonate the mobile user in the proposed protocol.

- **Mobile User Fails to Identify Smart Devices** $\xrightarrow{\text{Attack}}$ **Impersonation of All Smart Devices**
During the authentication phase, the mobile user selects the smart device to authenticate mutually. The mobile user possesses knowledge of the identities of all the smart devices connected to the network. Suppose the user fails to identify the smart device correctly based on its identity. In that case, it indicates that an adversary has either changed the identity of the smart device or the smart device is unresponsive when receiving authentication messages from the gateway. However, impersonating a compromised smart device does not lead to the impersonation of all smart devices within the system. This is due to each smart device's unique shared secret keys.

6.1.3. Gateway (Attack Target)

- **Insecure Transmission of Secret Key k** $\xrightarrow{\text{Attack}}$ **Break User Anonymity, Obtain Secret k**
The gateway, considered a secure entity in the proposed scheme, does not transmit its secret key k but uses it only for session key K_{UG} computation. For the computation of exchanged messages, the gateway employs the shared secret keys $(K_{UG}, h(K_{GS}))$.

Table 5. Security comparison table.

Requirements	[15]	[16]	[22]	[23]	[24]	Proposed Scheme
F1	×	✓	✓	✓	✓	✓
F2	✓	✓	✓	✓	✓	✓
F3	✓	✓	✓	×	✓	✓
F4	×	×	×	×	✓	✓
S1	×	✓	×	✓	×	✓
S2	×	×	✓	×	×	✓
S3	×	×	×	✓	×	✓
S4	✓	×	×	×	×	✓
S5	×	×	×	×	×	✓

F1: Mutual Authentication, F2: Key Agreement, F3: Sound Repairability, F4: No Location Tracking, S1: User Anonymity, S2: Forward Secrecy, S3: No Password Exposure, S4: Resistance to known Attack, S5: Resistance to Node Capture Attack; ✓: Yes provides, ×: Does not provide.

6.1.4. Session Key (Attack Target)

- **Forward Secrecy Issue** $\xrightarrow{\text{Attack}}$ **Obtain Previous Session Key of SID_j**
The proposed scheme achieves forward secrecy, as discussed in the security requirements above. An adversary cannot derive the session key computation from a previous session since only the trusted entity, the gateway, can compute the session key.
- **Improper Distribution of Smart Device Secret Keys** $\xrightarrow{\text{Attack}}$ **Obtain Previous Session Key of All Smart Devices**
With its unique identity, each smart device must be registered with the gateway before joining the environment. The gateway distributes a unique secret key corresponding to each smart device's identity. Additionally, the session key is updated during each session. Consequently, even if an adversary manages to capture a node and obtain the session key, it does not compromise the security of the entire system.

6.1.5. Availability (Attack Target)

- **Insecure Transmission of Updated Session Key** $\xrightarrow{\text{Attack}}$ **Modify Session Key**

The gateway entity updates the session key using its secret key. The new session key ($TID_{U_i(new)}$) is transmitted to the user by encrypting it with the shared secret key (K_{UG}). Only the user can obtain the session key by decrypting it with K_{UG} . As a result, an adversary cannot access or modify the updated session key, ensuring its integrity.

7. Performance Analysis of the Proposed Protocol

This section compares the proposed protocol with previously proposed security protocols [15,16,22–24] in terms of communication and computation costs [26].

7.1. Communication Costs Analysis

The comparison of communication cost is shown in Table 6. Communication cost refers to the number of bits and messages exchanged during a single scheme transaction. The bits and messages are calculated based on the approximate values of functions and parameters used in the proposed protocol [27]. The following are the values of the functions and parameters: ECC point value: 320 bits, hash digest (SHA-1) value: 160 bits, nonce/identities value: 128 bits, timestamp value: 32 bits, random number value: 64 bits. In the proposed protocol, four messages are exchanged: message M_1 transmitted with 160 bytes, message M_2 transmitted with 40 bytes, message M_3 transmitted with 36 bytes, and message M_4 transmitted with 47.

The proposed protocol exhibits lower communication costs than the mentioned protocols, except for the Fakroon et al. [24] scheme. Although Fakroon et al. have lower communication costs than the proposed protocol, they fail to provide the required general security requirements. In contrast, the proposed protocol satisfies the necessary security requirements for IoT smart home systems.

Table 6. Comparison of communication costs of the protocols.

Protocols	M_1	M_2	M_3	M_4	Total-Bytes	Messages
Kumar et al. [15]	512	448	192	-	1152	3
Wazid et al. [16]	60	120	64	160	404	4
Shuai et al. [22]	108	84	36	68	296	4
Banerjee et al. [23]	52	84	52	100	288	4
Fakroon et al. [24]	92	56	56	56	260	4
Proposed Protocol	160	40	36	47	283	4

7.2. Computation Costs Analysis

The comparison of computation cost is shown in Table 7. The computation costs of the protocols are calculated for each party involved, including the smart user, gateway, and smart device. The computation cost of the proposed protocol is calculated as follows: $4h_{U_i} + 4h_{GWN} + 2SE_{GWN} + 1h_{SD} = 9h + 2S_{ED}$. Table 8 shows the computation cost of proposed approaches compared to the state-of-the-art approaches [15,16,22–24].

The computation time experiment by Kilinc and Yanik [28] is used to calculate computational time. The experiment was conducted on the Ubuntu operating system with an Intel dual-core Pentium processor, with specifications including a 2.20GHz processor and 2048MB RAM. According to the experiment, the computational time of different cryptographic primitives is as follows: time for hash (T_h) is 0.0023 ms, time for bilinear function (T_B) is 5.811 ms, time for MAC (T_{MAC}) is 0.0046 ms, time for modular exponentiation (T_{me}) is 3.8500 ms, and time for encryption/decryption (T_k) is 0.0046 ms.

The execution/running time of the proposed protocol is 0.0299 ms. The comparison of the computational cost of the proposed approach with respect to the state-of-the-art

approaches [15,16,22–24] is given in Table 8. According to the experimental results, the proposed approaches outperform all the previous approaches.

Table 7. Comparison of computation costs of the protocols.

Computation Cost	Total _{CC}
[15]	$4T_{S_{ED}} + 1T_{hmac} + 4T_h$
[16]	$22T_h + 4T_{S_{ED}} + T_{fe}$
[22]	$16T_h + 3T_m$
[23]	$24T_h + 1T_b$
[24]	$33T_h$
Proposed Scheme	$9T_h + 2T_{S_{ED}}$

U_{iCC} : Computation Cost of Mobile User, GWN_{CC} : Computation Cost of Gateway, SD_{CC} : Computation Cost of Smart Device, $Total_{CC}$: Total Computation Costs.

Table 8. Comparison of computation costs in milliseconds.

Computation Cost	Total Cost in Milliseconds
[15]	0.0322 ms
[16]	0.0736 ms
[22]	11.586 ms
[23]	5.866 ms
[24]	0.0759 ms
Proposed Scheme	0.029 ms

8. Conclusions and Future Work

This paper comprehensively analyzed state-of-the-art user-authentication schemes in the context of smart home systems. Our analysis identified several limitations and security vulnerabilities in existing schemes, highlighting the need for an improved solution. To address these shortcomings, we propose a secure and enhanced user-authentication scheme tailored for smart home environments. We performed a thorough security analysis of our protocol using formal computational models such as BAN logic and ProVerif tools. The evaluation demonstrated that our scheme effectively mitigates various security vulnerabilities, providing robust protection against attacks. Furthermore, we conducted a performance analysis to assess the computational and communication costs of the proposed scheme. The results indicated that our protocol achieves efficiency in resource utilization, making it suitable for deployment in IoT-based smart home environments.

Our future work will primarily focus on the dynamic aspects of user authentication within smart home environments. This entails exploring adaptive authentication mechanisms capable of accommodating changes in user profiles, roles, and permissions within the smart home system. Additionally, we plan to investigate techniques to improve the scalability and interoperability of user-authentication schemes, facilitating seamless integration with a diverse array of smart home devices and platforms. By addressing these areas, our objective is to bolster the security, usability, and flexibility of user authentication in smart homes. Ultimately, we aim to contribute to developing robust and efficient authentication solutions for future IoT applications, thereby safeguarding the privacy and security of smart home users.

Author Contributions: Conceptualization, Data curation, Software, Writing—original draft, Investigation, Validation and Visualization, I.A.; Data curation, Writing—original draft, Investigation, Validation and Visualization, M.A.K.; Writing—original draft, Writing—review and editing, Funding acquisition, Validation, and Visualization, T.A.; Methodology, Supervision, Resources, Writing—

original draft, and Visualization, S.U.; Software, Investigation, Writing—original draft, and Validation, K.M.u.H.; Methodology, Formal Analysis, Resources, Writing—original draft, Validation, and Investigation, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Open Access Publishing Fund of the Free University of Bozen-Bolzano.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Available upon request.

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

References

1. Tankovska, H. Worldwide Connected Devices by Access Technology. 2020. Available online: <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/> (accessed on 26 October 2020).
2. Gomez, C.; Paradells, J. Wireless home automation networks: A survey of architectures and technologies. *IEEE Commun. Mag.* **2010**, *48*, 92–101. [\[CrossRef\]](#)
3. Ning, H.; Shi, F.; Zhu, T.; Li, Q.; Chen, L. A novel ontology consistent with acknowledged standards in smart homes. *Comput. Networks* **2019**, *148*, 101–107. [\[CrossRef\]](#)
4. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.R.; Jin, Y. Security analysis on consumer and industrial IoT devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, Macau, China, 25–28 January 2016; pp. 519–524.
5. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
6. Das, R.; Gadre, A.; Zhang, S.; Kumar, S.; Moura, J.M. A deep learning approach to IoT authentication. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), IEEE, Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
7. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), IEEE, Aalborg, Denmark, 11–14 May 2014; pp. 1–8.
8. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), IEEE, Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3.
9. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements and solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), IEEE, Huddersfield, UK, 7–8 September 2017; pp. 1–6.
10. Khan, M.A.; Ullah, S.; Ahmad, T.; Jawad, K.; Buriro, A. Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol. *Sensors* **2023**, *23*, 5518. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Vaidya, B.; Park, J.H.; Yeo, S.S.; Rodrigues, J.J. Robust one-time password authentication scheme using smart card for home network environment. *Comput. Commun.* **2011**, *34*, 326–336. [\[CrossRef\]](#)
12. Kim, H.J.; Kim, H.S. AUTH HOTP-HOTP based authentication scheme over home network environment. In Proceedings of the International Conference on Computational Science and Its Applications, Santander, Spain, 20–23 June 2011; pp. 622–637.
13. Li, Y. Design of a key establishment protocol for smart home energy management system. In Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, 5–7 June 2013; pp. 88–93.
14. Santoso, F.K.; Vun, N.C. Securing IoT for smart home system. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 1–2.
15. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2015**, *16*, 254–264. [\[CrossRef\]](#)
16. 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**, *14*, 391–406. [\[CrossRef\]](#)
17. Herzog, J. A computational interpretation of Dolev–Yao adversaries. *Theor. Comput. Sci.* **2005**, *340*, 57–81. [\[CrossRef\]](#)
18. Wessels, J.; Bv, C.F. Application of BAN-logic. *CMG Financ. BV* **2001**, *19*, 1–23.
19. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. London Math. Phys. Sci.* **1989**, *426*, 233–271.
20. Blanchet, B. Automatic verification of security protocols in the symbolic model: The verifier proverif. In *Foundations of Security Analysis and Design VII*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 54–87.
21. Blanchet, B.; Smyth, B.; Cheval, V.; Sylvestre, M. *Proverif 1.86 pl3: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial*; 2012. Available online: https://teams.microsoft.com/l/message/19:067ea4cd-56c9-4651-8b7f-b518f384be71_45d796d8-ca8e-48fb-85f1-33f37e9c61e4@unq.gbl.spaces/1692411073655?context=%7B%22contextType%22%3A%22chat%22%7D (accessed on 16 August 2023).

22. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146. [[CrossRef](#)]
23. 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. [[CrossRef](#)] [[PubMed](#)]
24. Fakroon, M.; Alshahrani, M.; Gebali, F.; Traore, I. Secure remote anonymous user authentication scheme for smart home environment. *Internet Things* **2020**, *9*, 100158. [[CrossRef](#)]
25. Wang, C.; Wang, D.; Tu, Y.; Xu, G.; Wang, H. Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 507–523. [[CrossRef](#)]
26. Rifa-Pous, H.; Herrera-Joancomartí, J. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet* **2011**, *3*, 31–48. [[CrossRef](#)]
27. Singelée, D.; Seys, S.; Batina, L.; Verbauwhede, I. The communication and computation cost of wireless security. In Proceedings of the Fourth ACM Conference on Wireless Network Security, Hamburg, Germany, 14–17 June 2011; pp. 1–4.
28. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1005–1023. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.