Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Authentication Protocol for Smart Home Devices Constrained using ECC

Velaga Sohith Raghava[1], Pulakandam Venkata Siva Naga Hemanth[2], and Palanisamy Santhi[3]

Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai.

Abstract. The In smart home devices, communication between the user and the home devices can be taken place inaccessibly. The principle issue is about security. So many protocols have been formulated for the com- munication process, but the passwords are easy to decrypt as they have a very low chance of combination, which means we can use brute force to decrypt them. Another principal issue is resource restraint because the devices used in communication are very slow in processing. In this paper, we introduced the lightweight protocol using a one-way hash and the concept of an elliptic curve. Prover if is used for formal verification of the protocol, guaranteeing a rigorous mathematical evaluation of its correctness. Furthermore, in the context of smart home environments, informal security research verifies its resilience against most privacy and security concern.

Keywords: *ECC · Smart Homes· Privacy · Authentication · Security · Mobile · Gateway.*

1 Introduction

As we have previously discussed, a smart home is not less than your fictional world because we can use smart home devices to control our sensors and appli- cations when we are away from home, saving electricity. However, in order to use smart fans in conjunction with other smart home devices, sensors must be connected to the device. In addition to saving you money, it gives you safety. Al- though we may include a great deal of gadgets into our smart homes, there are a few things we must have, such cameras, control sensors, and smart TV controls. To simply control these gadgets, consumers may download apps and connect to the devices via the internet. As these technologies become more common, people will be able to use the power of their smartphones and other mobile computing devices to communicate with their Our lives are made easier by smart homes. This is one side of the story, but it also has a vulnerability since it is part of the cyber world, and as such, we may anticipate cyberattacks on these smart home gadgets. Researchers have also discovered design flaws in smart home appliances that might allow for invasions.

Similarly, highlights how security vulnerabilities are caused by the numerous functionalities of these devices and the unique connections they make inside the Internet of Things. Furthermore, in the event that we have an easily guessable password, an unauthorized individual may get entry into our house. The primary fault is that there should be protection for data transit between smart devices in a smart home. Given all of the system's vulnerabilities, an attacker may choose to launch a denial-of-service attack (DDOS attack) against a smart home device by sending an excessive number of requests to the device. The greatest worry about privacy is that personal information of the user may be read by an attacker when instructions or messages are transmitted over wireless connection.

Security: A variety of security systems use low-entropy keys for user authen- tication. This makes it reasonably easy for attackers to get these passwords that are vulnerable using shoulder surfing attacks. extra Hardware: Some authenti- cation methods need additional equipment, such as smart card readers, which

can be compromised by side-channel breaches and intercepted verification cre- dentials. Constraints on Available Resources: It is difficult to implement strong encryption and security measures because smart home devices are so varied and have restricted in resources features like limited transmission ranges, low battery life, and sluggish CPU speeds. Addressing these obstacles and improving safety and confidentiality in smart homes increases the effectiveness of authentication systems is required for networks. This enhancement might result in better ef- ficiency and reduced vulnerability to intrusions. In the following parts of this paper, we will examine these issues and potential solutions in greater depth in order to throw light on the vital junction between safety and advancements in the context of smart homes.

In order to protect users' security and privacy in smart homes, we will investi- gate the weaknesses in these cutting-edge ecosystems, examine how breaches af- fect confidentiality, and offer suggestions for enhancing authentication processes. The examination of the various facets of smart homes, including their benefits and downsides, establishes the groundwork for a comprehensive comprehension of the vital privacy and security concerns. Through proactive resolution of these issues, we may fully utilize smart homes while preserving the privacy of our digital lives in these networked environments.

1.1 Problem Statement

Concerning open wireless network connections in particular, the main concern is the confidentiality of sensitive information carried over these networks. There is a significant risk that adversary may use a range of methods to gain access to and capture this confidential information. There is a serious risk to privacy when credentials are exploited by outsiders to gain control of data and utilize it for their own purposes. Many security mechanisms have been proposed for home devices to address this risk, however, they frequently demand high processing power. Smart cards provide an extra degree of security, but one disadvantage is that authorized users could misplace them, which could result in security lapses. The creation of lightweight authentication systems with improved privacy protection is required to address these issues.

Threat model As discussed earlier, there is chance that outsider can get the information

1. Secure channels are used for messages sent and received during the first registration phase, guaranteeing that the setup procedure is protected from interception and manipulation.

2. The security of the trusted authority is not dependent on specific devices in the event that mobile terminals or smart home devices are stolen. Rather, it is dependent on a comprehensive security framework intended to thwart unwanted access or alteration.

3. The trusted authority can use security techniques like encryption and routine upgrades to lessen the impact of hacked devices on the system, even though smart home devices and terminals may not always be trusted.

4. The reliable authority has safeguards against external assaults on gadgets. To preserve the integrity of the system, this comprises functions including hardware-level security, secure boot procedures, and tamper-evident pack- aging.

5. The trusted authority maintains stringent access controls and carries out frequent audits to spot and stop harmful activity, especially in cases where authorised entities have powers.

6. It is accepted that although registration messages are secure, there may be weaknesses during mutual authentication. In order to mitigate this, the system incorporates supplementary security protocols, including secure key exchange protocols or further encryption layers, to protect messages trans- mitted during mutual authentication.

Security requirements As the above mentioned above the model their ma- jor principle components included Two- way authentication process when con- sumers' smart home gadgets and the data they exchange together, Therefore, it's critical that they ensure the messages they're delivering are secure and au- thentic. They accomplish this through the use of unique keys or codes known as "security tokens." By serving as covert stamps, these tokens ensure that the messages are authentic and unaltered by tampering. It is comparable to sealing a letter with a unique seal to ensure that it hasn't been opened or tampered with during delivery.

Establishing a secure session is the first step in the crucial negotiation process for data transfer between the end consumer and the smart home appliance. Keys must be swapped before communicating. In order to guarantee that the end user and the smart home gadget are able to communicate with the data that has been shared, these keys are necessary for decoding the data that is encrypted throughout the complete session.

To preserve end users' privacy, secure their smart home gadgets from surveil- lance, and dissuade potential attackers, the system employs nominal identities. By acting as false or transient IDs for individuals and objects, nominal identities offer an extra degree of secrecy in interaction. These pseudonymous identities provide protection for real user and device identities, allowing secure interactions without fear of unwanted tracking. Implementing robust security measures, such as data encryption and secure protocols, contributes to enhancing the effective- ness of the nominal identification system.

An intruder cannot correlate specific communication sessions with specific en- tities since they are anonymous. It is likely that the assailant is able to discreetly monitor the communication channel and intercept messages. The objective is to make it very difficult for the attacker to establish direct connections to sessions and the entities that are engaged in the transmission. To do this, protective measures including identity concealment, encoding, and the use of temporary identifiers are employed. Each of them strives to protect communication, con- ceal the identity of the persons participating, and the link between sessions.

1.2 Paper contributions

a) To address security and privacy concerns associated with traditional smart home security methods, a secure key exchange and identity authentication mechanism has been devised. This protocol ensures safe communication channels and access to the smart home network only for authorized compa- nies through the encrypted transmission of secret keys. This technique was developed to address the shortcomings of conventional smart home security solutions, which may not have included robust authentication, encryption, or privacy safeguards. Modern security measures are incorporated into the new protocol, which makes smart house construction easier than ever while also providing upgrades over current systems.

b) A preliminary examination of security feature analysis indicates that the suggested approach is resistant to typical smart home threats such as fabri- cation, side channel exploitation, and impersonating. In addition, it validates that this protocol permits non-traceability, anonymous functioning, and the anonymity of previous and future key interactions.

c) Another finding from an analysis of the efficiency examinations is that the proposed protocol uses a lot less processing, communication, and storage resources than competing protocols. In terms of total productivity and re- source use, this study shows how successful and efficient the recommended strategy is.

2 Related Works

Various protocols have been developed to prevent violations of privacy and secu- rity in smart home networks due to their confidentiality and sensitive nature. As an illustration, [19] provides a strong multiple-factor Elliptic Curve Cryptogra- phy method meant for authentication of users. On the other hand, [20] presents a

multi-layer security architecture meant to boost dependability and efficiency in Internet of Things contexts. The Development of an Authentication Protocol in [21] to enhance anonymity.

Nevertheless, this scheme's efficacy is weakened by the high communication expenses involved. An ECC-based mutual authentication system is developed by [22] in order to mitigate the high costs of communication mentioned in [21]. A comparable system based on ECC is described in [3]. However, the approach outlined in [3] is susceptible to identifying passwords and spoofing attacks. In contrast, [23] presents the development of an entity authentication scheme with the aim of enhancing Safety and confidentiality in connection with smart homes. In order to offer secure communication, [24] implements a protocol based on biometrics. Despite the provision of unlikability and anonymity by the protocol described in [24], it remains susceptible to physical assaults that may result in the disclosure of stored keys.

In light of this, various schemes [26]-[28] and the three-factor protocol de- scribed in [25] have been devised to tackle the issues raised in [24]. However, due to the necessity of storing user and device information in large databases, these protocols have a negative impact on storage efficiency. Conversely, [29] introduces a multimedia app security system based on ECC, But this method is vulnerable to guessing passwords and does not offer mutual authentication. The systems presented above mostly utilize Public Key Encryption. which intro- duces challenges related to key escrow [30]. In [31], a lightweight authentication protocol is proposed as a solution to these problems.

Additionally, this method is demonstrated to provide noteworthy privacy and security attributes. In the process of developing authentication protocols, efficacy must also be taken into account. In light of this, the authors of [5] have proposed a smart home ECC-based scheme that is effective. However, this type of proto- col is susceptible to packet replays, authorized insider assistance, and dictionary attacks [2]. Moreover, its methods for key agreements are not safe, and it does not offer forward key secrecy. A user authentication technique is offered in [2] as a way to lessen these challenges. Moreover, password-based systems have been put in place to offer linked home authentication. For instance, [32] creates a password-based smart home security system. Unfortunately, this technique has significant computational and communication overheads and is vulnerable to offline guessing of passwords attacks. To mitigate many of these issues, smart homes have been protected using chaotic cryptography. For instance, a chaotic map-based method is described in [27]. Ultimately, this strategy is open to ap- proved insider threats and offline prediction of passwords [28]. On the other hand, [29] offers a practical approach to device authentication with unsecure cloud platforms.

In reference [30], a protocol for session key negotiation is also developed for the smart home system. However, the approach in [30] does not offer complete forward key secrecy, anonymity, or mutual authentication. On the other hand, the PKI-based technique that was suggested in reference [31] requires a signif- icant amount of computing work [32]. Unfortunately, blockchains could put a significant computational and memory load on low-resource IoT devices. On the other hand, a plan for identity-based confidentiality has been developed.

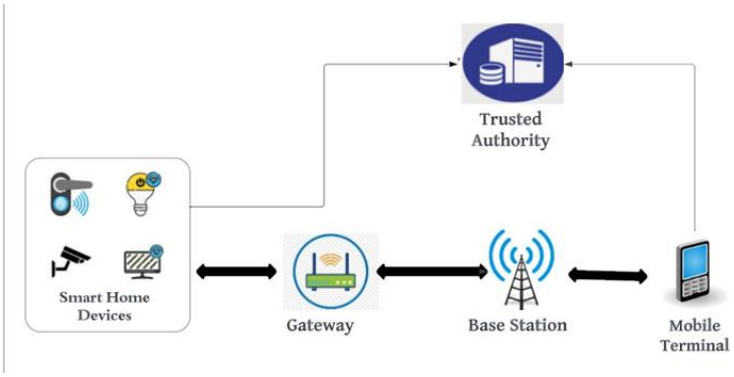

Fig. 1: Network architecture

3 The proposed protocol

The primary actors in the proposed protocol are the Trusted Authority, Smart Home Devices, Gateway Node and the Mobile Terminal of the remote user. In this instance, the Gateway Node serves as the focal point, enabling communica- tion between Mobile Terminal s and Smart Home Devices. Smart Home Devices are put in houses to provide numerous activities with control and monitoring. But the Mobile Terminal makes it possible for the distant users to access their Smart Home Devices and carry out the necessary monitoring and management. Conversely, the Trusted Authority provides the necessary security token gener- ation and allows Mobile Terminals and Smart Home Devices to register. The network architecture of the suggested protocol is shown in 1.

Commercial mobile networks, like 5G, can serve as the communication link between the remote user and the smart home gadgets. Because this communi- cation route is open, the messages that are exchanged must be shielded from a variety of security and privacy threats. There are three main stages to the actual implementation of the suggested protocol: setting up mutual authentica- tion, key negotiations and the network's security. Detailed explanations of these stages may be found in the next subsections. The symbols and their explanations used in this study are listed in Table 1. The steps of key exchange, two-way au- thentication, and system configuration are described in depth in the subsequent sections.

Symbols.

Symbol	Description
MT	Mobile terminal
ID_{MT}	Mobile terminal identity
SHD	Smart home device
MTMK	Master key for a mobile terminal
SID_{HD}	Distinct identity of smart home device
PID_{SHD}	Pseudo-identity of smart home device
SSV	Temporary session key variable for smart home device
||	Pairing Method
T_{Si}	Timestamp *i*
S_{SHD}	Secret key for smart home devices
PK_{MT}	generated at the mobile terminal session key
PK_{SHD}	Session key derived at the smart home device
ΔT	Acceptance for transmission delay
h (.)	One- way hashing function
⊕	XOR operation
UE_{ID}	Unique identity of the trusted authority
R_i	Random number *i*

Fig. 2: secrecy, authenticity, non-repudiation, and anonymity, it might result in significant escrow issues.

3.1 System Configuration

During this phase, security attributes are generated for both the distant user's mobile device and smart home gadget, by a trusted entity. This procedure con- sists of the following three steps:

1. Creation of Identity and Key:

The trustworthy entity creates the primary key (PK_{MT}) for the mobile terminal (MT) and sets its unique identity (UE_{ID}). Simultaneously, substi- tute identities (SID_{SHD}) are selected for smart home devices in addition to unique identities (SID_{HD}) assigned to each device.

Derivation of Keys and Selection of Session Variables:

The entity designates SSV as the transient session variable associated with the smart home device. The algorithm subsequently calculates the concealed key (*SHD*) of the smart home device by employing a hashing function (*H*) with SID_{HD} and PK_{MT} as inputs. Subsequently, it determines the security

attributes for each smart home device: $\sigma = MTMK \oplus 1$, $B1 = (SID_{SHD})\sigma$, and $B2 = SID_{SHD} \oplus H(SID_{SHD}||PK_{MT})$.

2. Encrypted Attribute Transfer:

The entity transmits in a secure manner to the smart home device a collec- tion of attributes denoted SID_{HD}, $B1$, UE_{ID}, *SHD*, *SSV* , and to the mobile terminal a collection of attributes UE_{ID}, $B2$, PK_{MT} , *SSV* . These attributes are securely stored in the memory of their respective devices once they are received.

3.2 Two-way Authentication and Key Exchange

Involving key negotiation and mutual authentication, the secure remote user terminal and smart home gadget maintain an active relationship. Both devices retrieve the security parameter configuration that was previously stored in their memory during the system configuration phase. Two-way Authentication and Key Exchange occur in the following order:

1. Initiation of the Smart Home Device

The device produces a random variable R_1 and a current timestamp TS_1. $X_1 = R_1 \oplus h(HID||SSV)$, $X_2 = h(SSV)$, and $X_3 = h(SID||X_1||ID_U||R_1||TS_1)$

are computed as parameters. The message MSG_1 is composed of the following components: X_1, X_2, X_3, and TS_1. It is transmitted securely to the Trusted Authority (TR).

2. Interaction between the TR and the Mobile Terminal

The TR appends its identity ID_{TR} to the MSG_1 received from the smart home device and generates the authentication message

$MSG_2 = X_1, X_2, X_3, TS_1, ID_{TR}$. This message is transmitted to the mobile terminal through public channels.

3. Verification of the Mobile Terminal

Upon receiving MSG_2, the mobile terminal acquires the initial timestamp TS_2. The message's freshness is verified through the computation of $|TS_2 - TS_1| \leq \Delta T$, where ΔT represents the utmost permissible transmission la- tency. If this condition is not met, the session is terminated. Otherwise, the

stored ID_{TR} is compared to the one extracted from MSG_2. If they match, the process advances to step 4.

4. Validation and Derivation of the Key (Mobile Terminal)

The mobile terminal calculates the parameters $SID = X_2 \oplus h(HID||MK_{MT})$

and $R_1 = X_1 \oplus h(SHD||SSV)$ and derives $HID = (X_1 \cdot MK_{MT})$. It verifies

that $X_3 \stackrel{?}{=} h(SID||HID||SHD||R_1||TS_1)$. If the verification fails, the session is terminated. Otherwise, the session key is computed using a random number R_2 generated by the mobile terminal

$SK_{MT} = h(SID||HID||SHD||R_1||R_2||TS_1||TS_2)$.

5. Update Parameters

The smart home device's new pseudo-identity HID^* is generated by the

mobile terminal, which also calculates $X_1^* = (HID^*)\sigma$ and $X_2^* = SID \oplus h(HID^*||MK_{MT})$. X_1 and X_2 are updated with X_1^* and X_2^*, respectively.

$Y_1 = (R_2||HID^*) \oplus h(SHD||SSV||R_1)$ and $Y_2 = h(X_1^*||SK_{MT})$ are then calculated. It replaces SSV with SK_{MT} in memory and generates the MSG_3

message (X_1, Y_1, Y_2, TS_2) that is transmitted to the TR through public chan- nels.

6. Verification and Interaction of the TR

The TR validates the smart home device pseudo-identity HID using the X_1 extracted from MSG_3. The message MSG_4 is composed of Y_1, Y_2, and TS_2 and is transmitted to the smart home gadget via open channels.

7. Validation of Smart Home Devices

Upon receiving MSG_4, the smart home device computes the current times- tamp TS_3 and verifies that $|TS_3 - TS_2| \leq \Delta T$. A failed assessment will result in the termination of the session. If the assessment is successful, the session key SK_{SHD} is generated as $(R_2||X^*) = Y_1 \oplus h(SHD||SSV||R_1)$ and $(R_2||X^*) = h(SHD||R_1||R_2||TS_1||TS_2)$. It performs validation when $Y_2 \stackrel{?}{=} h(X^*||SK_1)$. X_1 is updated with X^*, SSV_1 is substituted with SHD_1 the computed session key SK_{SHD}, and the secure communication procedure proceeds if the operation is successful.

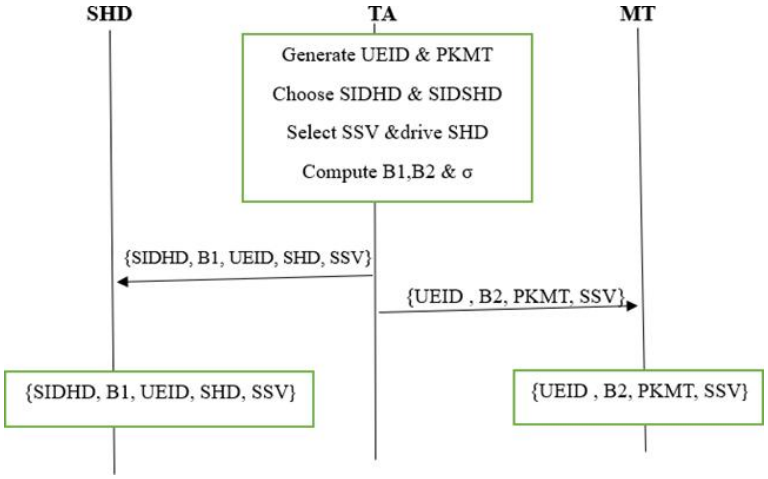

Fig. 3: Period of system setup.

4 Security analysis

This section examines the formal and informal security aspects of the suggested protocol. This section uses the ProVerif tool for analysis because it is widely used for formal study of authentication methods. Conversely, twelve lemmas are formulated and proven in order to carry out informal analysis, as explained below.

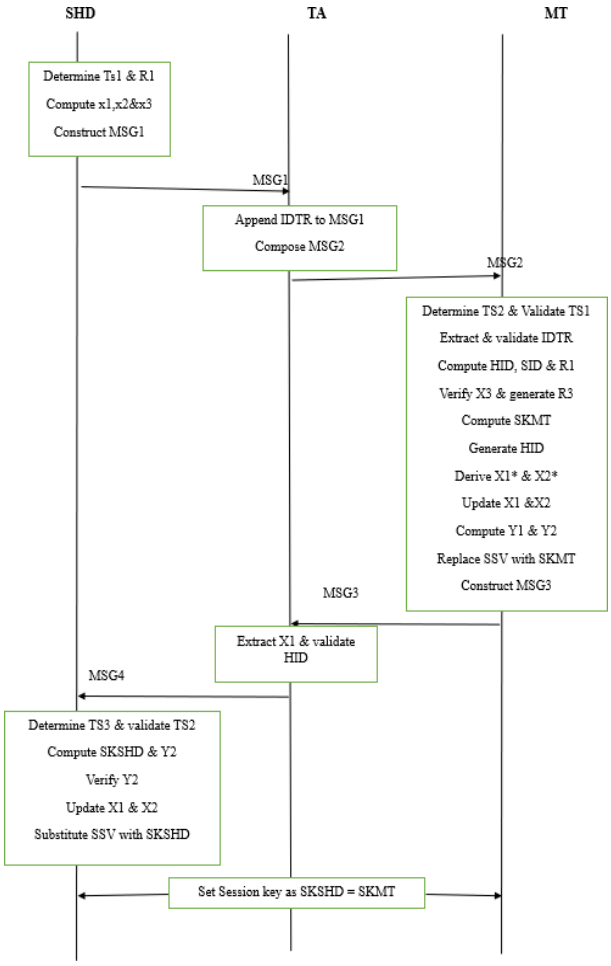

Fig. 4: The time period of exchanging keys and mutual authentication

4.1 Authorized verification of security

The analysis tool is used in this part to confirm that the suggested protocol offers the cryptographic security features it claims. The reason this tool was chosen is that it supports a wide range of cryptographic primitives, including encryption, decryptions, digital signatures, and one-way hash functions. Mutual authentication, anonymity, key secrecy, and session key strength are all confirmed in this way. The deployment of Secure Channels occurs during the registration step. Public Channels are used, nevertheless, during the mutual authentication and key negotiation stages. Thus, these two channels are used for the protocol's initial testing. First, mutual authentication is carried out after the SHD and MT processes have been started. The channels and variables used in this procedure are shown in Fig. 4.Conversely, Fig. 5 illustrates the inquiries and events.

```
(** events **)
event begin_SHD ( bitstring ) .
event end_SHD ( bitstring ) .
event begin_MT ( bitstring ) .
event end_MT ( bitstring ) .
(** queries  **)
Query id: bitstring; event (end_SHD(id)==>event  (Start_MT(id))
Query sid: bitstring; inj-event (end_MT(sid)==>inj-event  (Start_SHD(sid)).
```

Fig. 5: Queries and events in the proposed protocol.

The two communicating entities, mobile terminal and smart home device, are modelled here, together with their events. The begin_mobile terminal and end_mobile terminal events are used to authenticate the SHD when taking the MT into account. Conversely, the SHD uses the begin_Smart home device and end_Smart home device events to authenticate the MT. Protecting the mobile port master key (MKMT) and the home device identity (id) is crucial for the proposed protocol.

Attacker of queries (MKMT).Attacker query(id).The SHD and MT authen- tication processes are explained in Figs. 6 and 7, respectively. The trusted au- thority TA acts as a mediator in the mutual authentication process between the SHD and the MT.

In essence, the TA simply transmits the message to MSG1 after appending its identifying IDTR. Similar to this, the TA just takes security token X2 out of message MSG3 and verifies SHD identification.

Therefore, in order to improve simplicity during these proofs, the TA can be removed. The questions in Fig. 8 are used to assess how strong the security elements of the suggested protocol. The Smart home device and Mobile terminal authentication process are exucated started and stopped based on the outcomes in (1) and (2). However, the results in (3) suggest that the negotitied session key between the communicating entries cannot be leaked or captured by an adverse query.

```
(*** Authentication procedure SHD ***)
Let SHD=
event begin_SHD(IDSHD) ;
let B1=XOR (R1, h (SSHD,TKV)) in
let B2= h (TKV) in
let B3= h (IDSHD,A1,B2,IDTA,R1,TS1) in
out (PCh, (A1,B1,B3,TS1)) ;
in (PCh, (R1D1: bitstring, R1D2: bitstring,R1T2: bitstring)) ;
new TS3: bitstring
let Con (R1R2, R1A1)=XOR(D1,h(Con(SSHD, TKV, R1)) in
let SKSHD = h (Con(IDSHD, PIDSHD, SSHD, R1, R2, TS1, TS2) in
if h(con (R1A1, SKSHD))=R1D2 Then
(** Substitute A1 with NA1, and stores session key SKSHD **)
(**Also refreshes TKV with SKSHD **)
event end_SHD(IDSHD);
else
0.
```

Fig. 6: Authentication procedures for smart home device.

4.2 Evaluation of security concerns

In communication networks, if appropriate security is not implemented, a mul- titude of assaults can be conducted in communication networks. Therefore, the evaluation of the suggested system against several attack models is given in this part. To do this, the following twelve lemmas are formulated and proven, and

their security properties are evaluated.

Lemma 1. *Parties engaged in communication actively authenticate one an- other.*

Proof. The trustworthy authority, the smart home device, and the mobile inter- face of the remote users are engaged in the communication process. The mobile interface takes the Trusted Authority's identification ID_{TR} from message $MSG2$ to authenticate the trusted authority. It then compares ID_{TR} with the corre- sponding value stored in memory. Furthermore, the mobile terminal verifies the

identity of the smart home device by checking if $X3 \equiv h(SID||HID||SK_{SHD}||R1||TS1)$;

if this validation fails, the session is terminated. Similarly, to verify the trusted authority, the smart home device checks if $Y2 \equiv h(X2^{*}||SHD)$, terminating the session if this check fails.

Lemma 2. *Anonymity and untraceability are maintained.*

Proof. During the communication process, this system uses temporary session variables and pseudo-identities in place of the devices' true identities. Mes-

sages $MSG1 = \{X2, X1, X3, TS1\}$, $MSG2 = \{X2, X3, TS1, ID_{TR}\}$, $MSG3 =$

$\{X2, Y1, Y2, TS2\}$, and $MSG4 = \{Y1, Y2, TS2\}$ are exchanged, where the

```
(** Authentication procedure (MT) **)
Let MT =
Event begin_MT (IDMT);
in (PCh, (R1IDTA: bitstring, R1A1: bitstring,R1B3: bitstring,
R1T1:bitstring)) ;
new TS2: bistring
let TS2'=TS2-R1TS1 in
if TS2' =TT||TS2' < TT Then
ifIDTA =R1IDTA Then
let PIDSHD=XOR(R1A1,MKMT) in
(*Obtain A2 using PIDSHD from memory*)
Let IDSHD=XOR(A2,h(cn(PIDSHD, MKMT))) in
Let SSHD=h(con(IDSHD, MKMT)) in
Let R1R1=XOR(B1, h(SSHD,TKV)) in
Let B3'=h(con(IDSHS,R1A1,B2,IDTA, R1R1,R1TS1)) in
if B3'=R1B3 Then
new R2: bitsring;
let SKMT=h(con(IDSHD, PIDSHD, SSHD, R1R1,R2,R1TS1,TS2)) in
new PIDSHD': bistring;
let NA1=XOR(PIDSHD', MKMT) in
let NA2=XOR(PIDSHD', MKMT) in
let NR2=Con(R2,NA1) in
let D1=XOR(NR2, h(Con(SSHD,TKV,R1R1))) in
let D2=h(con(NA1, SKMT)) in
out (PCh, (D1,D2,TS2));
(** Substitute A2 with NA2**)
(**Substitte TKV with SKMT**)
event end_MT(IDMT);
0.
```

Fig. 7: Process for portable device verify.

```
RESULT inj-event(end_MT(sid))==>
inj-event (begin_MT(sid) is true.                    (1)
RESULT inj-event(end_SHD(id_1539))==>
inj-event(begin_SHD(id_1539)) is true                (2)
RESULT not attacker (MKMT) is true
RESULT not attacker (sid) is true                    (3)
```

Fig. 8: Validated security features

pseudo-identity HID of the smart home device is included in parameters $X2 = (HID)\rho$ and $Y1 = (R2||HID^*) \oplus h(SHD||SSV||R1)$ rather than its actual identity SID. [Further text of the proof continues...]

Lemma 3. *Attacks aimed at temporarily leaking session-specific information cannot breach this protocol.*

Proof. Assume that an adversary manages to capture the random number $R1$. An attempt is then made to derive the smart home identity SID and the tempo- rary session key variable SSV for the smart home from the intercepted parameter

$X1 = R1 \oplus h(SHD||SSV)$ via public channels. However, the extraction of SSV from $X1$ and SID from $SHD = h(SID||PK_{MT})$ is prevented by the one-way property of the hashing function. Similarly, any attempt to derive SID from

$X3 = h(SID||X2||ID_{TR}||R1||TS1)$ will fail for the same reason. Likewise, the

adversary would have to reverse the hashing function, which is computationally

infeasible, to obtain SK_{SHD} from $X1$.

Lemma 4. *Attacks that take over a session are prevented.*

Proof. The adversary's goal in this attack is to deduce the legitimate session key $SK_{MT} = h(SID||HID||SHD||R1||R2||TS1||TS2)$ in order to deceive the SHD into thinking it is communicating with a valid MT. The adversary would

need to correctly produce the random numbers $R1$ and $R2$, as well as the correct timestamps $TS1$ and $TS2$. This forms a problem that is NP-hard in terms of unpredictability. Additionally, the adversary would need the master key PK_{MT}

to compute the parameter $SHD = h(SID||PK_{MT})$, which is necessary to vali-

date the session key. Since the key is never transmitted over open channels, this

attack is unsuccessful.

Lemma 5. *Backward and forward secrecy of keys is assured by this protocol.*

Proof. The MT uses $SK_{MT} = h(SID||HID||SHD||R1||R2||TS1||TS2)$ to de- rive the session key. Similarly, the SHD derives its session key

$SK_{SHD} = h(SID||HID||SHD||R1||R2||TS1||TS2)$. It is evident that these ses-

sion keys incorporate random numbers ($R1$ and $R2$) and timestamps ($TS1$ and $TS2$). Additionally, to utilize the security parameter $SHD = h(SID||PK_{MT})$, one must know the MT's master key PK_{MT}, and the SHD's real identity SID.

Since these parameters are never communicated over public channels, an adver- sary cannot obtain them. Therefore, even if an attacker manages to compromise the current session key, they cannot deduce the session keys of any past or future sessions.

Lemma 6. *Man-in-the-middle (MITM) attacks are prohibited.*

Proof. A MITM attack aims to intercept and potentially alter the messages being exchanged. However, due to the design of the protocol, where messages $MSG1$, $MSG2$, $MSG3$, and $MSG4$ are exchanged with specific cryptographic parameters, any attempt by an adversary to modify these messages would re- quire knowledge of secret parameters that are not accessible, thus preventing the success of such an attack.

Lemma 7. *Attacks using side channels are prohibited.*

Proof. The smart home device stores parameters SID, $X2$, ID_{TR}, SHD, and SSV in its memory during the initial setup phase, while the mobile terminal stores ID_{TR}, ρ, PK_{MT}, and SSV. However, during the mutual authentication

phase, the MT substitutes SSV with the derived session key SK_{MT} and the SHD replaces SSV with SK_{SHD} after updating $X2^*$ in place of $X2$. Thus, even if an attacker gains access to all memory contents through a side channel attack,

without the random numbers $R1$, $R2$ and timestamps $TS1$, $TS2$, they cannot compute the session keys, rendering the protocol secure against such attacks.

Lemma 8. *Long-term secret key leakage attacks are unlikely to succeed against this protocol.*

Proof. If an adversary captures the mobile terminal's master key PK_{MT}, they aim to decrypt both past and future session keys and the SHD's true iden- tity SID. However, this protocol only includes SID in parameters such as $X3$, SK_{MT}, and SK_{SHD} which are protected by hash functions and never re- vealed in plaintext. Thus, even with PK_{MT}, the attacker cannot compute valid session keys for any sessions, protecting the system against key leakage attacks.

Lemma 9. *This scheme can withstand impersonation attempts.*

Proof. An attacker aiming to impersonate a legitimate party would need to modify the exchanged messages to make them appear as if they come from a trusted source. However, since legitimate messages depend on secret parameters such as SSV, PK_{MT}, and SHD which are not accessible to the adversary, impersonation attempts will fail, securing the system against such attacks.

Lemma 10. *Attacks aimed at denying service are prevented.*

Proof. In centralized authentication architectures, a central authority can be- come a bottleneck during denial of service attacks. However, in the proposed protocol, the Trusted Authority only partakes in lightweight operations such as appending its identity to messages and verifying identities, avoiding engagement in computationally intensive cryptographic processes. Therefore, the protocol mitigates the risk of denial of service attacks targeted at the central authority.

Lemma 11. *This method is resistant to fabrication attempts.*

Proof. Assume an adversary has obtained the smart home device's secret key (SHD) and attempts to derive necessary security tokens to fabricate the message

$MSG4 = \{Y1, Y2, TS2\}$. Given $Y2 = h(X2^*||SK_{MT})$ and $Y1 = (R2||HID^*) \oplus$

$h(SHD||SSV||R1)$, without access to the random numbers $R1$ and $R2$, the updated pseudo-identity HID^*, and the temporary session key variable SSV, the attacker cannot forge the security token $Y1$. Additionally, without the mobile terminal's session key SK_{MT} and the security token $X2^*$, $Y2$ also cannot be

forged. Therefore, the protocol is resistant to fabrication attempts.

Lemma 12. *Attacks using packet replay are thwarted.*

Proof. The protocol includes freshness checks in its design to prevent replay attacks. When the Trusted Authority receives $MSG1$ from the Smart Home De- vice, it appends its identity ID_{TR} and forwards $MSG2$ to the Mobile Terminal, which will verify the message's freshness using timestamps. Similarly, after re- ceiving $MSG3$ from the Mobile Terminal, the Trusted Authority will perform a freshness check before

forwarding to the Smart Home Device. These checks ef- fectively prevent replay attacks by ensuring that only messages with valid, fresh timestamps are accepted, thus terminating sessions where these checks fail.

5 Performance evaluation

In this part, the recommended protocol is compared and evaluated. Overheads in computing, storage, and communication are among the measures utilized in this assessment. The decision-making process is guided by the frequency of these indicators in the authentication protocols evaluation. By the end of this part, a comparison is made between the security features that the proposed protocol has and those that other comparable protocols given.

Table 1: Analyses are constrained by computation.

Organize	Manager(ms)
Damandeep, and Devender	1.3660
Mingxia	1.3660
Shihong	2.6540
Mohammad S	2.6696
Ashok Kumar Das	0.2108
Leila Azouz Saidane	1.4950
Majid Bayat	1.3764
Proposed	0.5004

Computation overheads We utilize a 32-bit, 72 x 106 Cortex M4 microcon- troller to measure the various cryptographic primitives' runtimes. At 3.3V, the non-active mode uses 3.6 × 10-2 A of power and the active mode uses 1.188

× 10-1 A. Based on this hardware implementation, symmetric encryption and decryption (TED) takes 21.5 s, a single one-way hashing operation (TH) takes

5.2 s, and ECC point multiplication (TPM) takes 4.276 x 10-2 s.A single mul- tiplication operation and eight TH operations are performed on the MT side of the suggested protocol. Conversely, on the SHD side, only 6TH operations are performed.

Thus, there is a 4.692 x 10-2 s processing overhead on the MT end. However, the SHD has a calculation overhead of 31.2 s. Consequently, 500.4 s is the entire

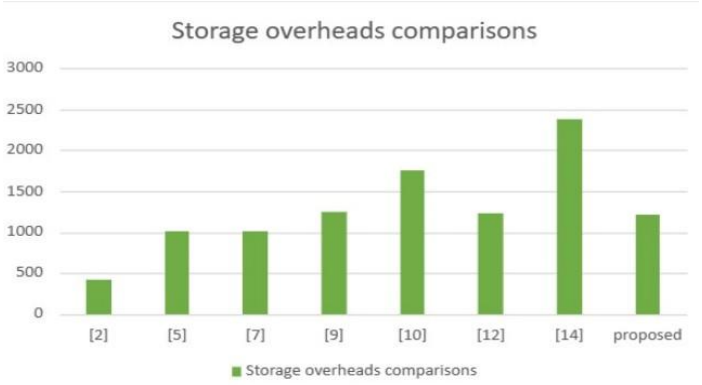

Fig. 9: Computation overheads comparisons

computation overhead at the Mobile Terminal and the SmartHomeDevice. The calculation overheads of various relevant techniques are displayed in Table 2.The protocol in [9] has the most computing overhead, 2.6696 10-3 s, as seen in Fig.

9. The schemes in [7,12,14,2, 5], the suggested protocol, and the scheme in [10] come next, in that order.

Despite having the lowest compute overheads, the protocol in [10] is vulner- able to attacks including transient information leaking and secret key breaches. Furthermore, attacks like forgeries, side-channelling, MITM, and Cookie hijack- ing are not taken into account in its architecture.

5.1 Communication overheads

The cost of communication must be decreased in order to improve communica- tion efficiency. In determining the sizes of the messages that are sent throughout the authentication and key negotiation stages are considered, as well as the com- munication overhead of the proposed protocol. Table 3 lists the various crypto- graphic procedures' output sizes according to the values in [7]. MSG1, MSG2, MSG3, and MSG4 messages are shared during the process of key acquisition and authentication between two parties. The size distribution of these exchanged messages is seen in Table 4. Table 4 makes it evident that the suggested ap- proach has a total communication overhead of 2016 bits. The communication overheads for the other similar systems are shown in Table 5. According to the graphs in Fig. 10, the communication overheads associated with the approach in [14] are the largest. The communications in [7,5,9,10], the suggested proto- col, and the organizes in [2] and [12] come next, in that order. Secret key and transient information leakage attacks can compromise the lowest communication costs of [12] protocol. Furthermore, reciprocal authentication is not provided by it. The lack of consideration for attack types that are untraceable and include MITM, side-channelling, packet replay, denial of service, and fraud is another flaw in its design. However, forgeries, session hijacking, man-in-the-middle, and side- session hijacking attacks are not taken into account in the [2] system.

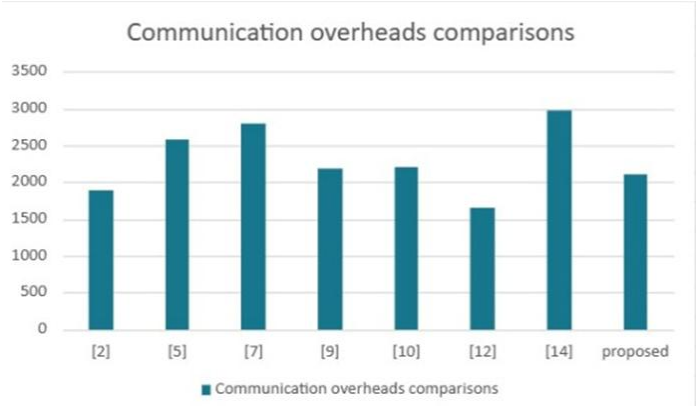

Fig. 10: Comparison with communications expenditures.

Table 2: Cryptographic output sizes.

Cryptographic operation	Size (bits)
ECC point	160
Identity	128
Random number	160
Timestamp	32
Hash value	160
Cipher-text	256
Secret key	160

Table 3: Message size derivations.

Message	Size (bits)
$MSG_1 = \{B_i, X_1, X_2, X_3, TS_1\}$	512
$B_i = X_1 = X_2 = 160; TS_1 = 32$ $B_i = X_1 = X_3 = 160; TS_1 = 32;$ $UE_{ID} = 128$	640
$MSG_2 = \{B_i, Y_1, Y_2, TS_2\}$	512
$B_i = Y_1 = Y_2 = 160; TS_2 = 32$ $MSG_3 = \{Y_1, Y_2, TS_3\}$	352
Total	2,016

5.2 Storage Requirements

In the proposed protocol's registration phase, the mobile terminal saves the parameter set $\{ID_{TR}, \sigma, PK_{MT}, SSV\}$, whereas the smart home device stores

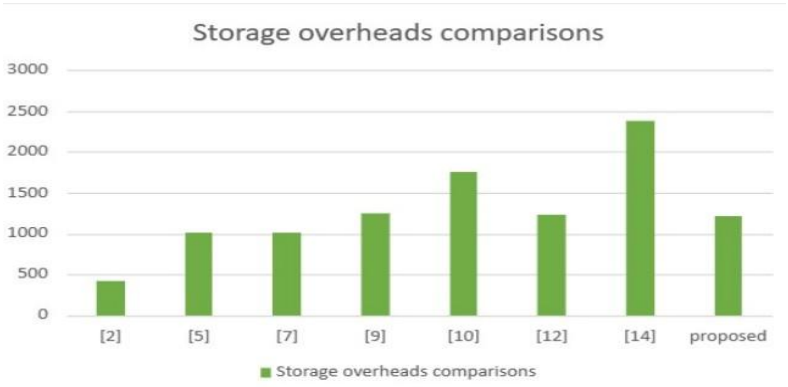

Fig. 11: Comparing Storage overheads.

the parameter set $\{SID, X_2, ID_{TR}, SHD, SSV\}$. Following a successful authen- tication process, the mobile terminal saves $\{ID_{TR}, \sigma, PK_{MT}, SK_{MT}\}$. Simi- larly, following successful mutual authentication, the smart home device saves

$\{SID, X_2, ID_{TR}, SHD, SK_{SHD}\}$. Considering the values in Table 3, ID_{TR} is

equal to 128 bits, and σ, PK_{MT}, and SK_{MT} are equal to 160 bits each. The

mobile terminal, therefore, needs 608 bits of storage. Conversely, X_2, SHD, and SK_{SHD} are each equal to 160 bits, and SID and ID_{TR} are each equal to 128 bits. The smart home device, therefore, needs 736 bits of storage. With n mobile terminal devices and m smart home devices, respectively, the proposed protocol requires $608n + 736m$ bits. Thus, 1344 bits are needed for a single mobile termi- nal and a single smart home device. Table 6 shows the storage requirements for other comparable methods, considering just two peers.

Fig. 11 makes it clear which procedure in [14] has the biggest storage ex- penses. The suggested procedure, the scheme in [5,7], the scheme in [10,12,9], and the scheme in [2] come next. Despite having the protocol with the lowest storage costs in [2] contains many security flaws, as was detailed in Section 5.2 above. The protocol in [5] falls short in providing anonymity and defence against secret key assaults transient information leakage attacks, transient information leakage attacks, and packet replays.

Table 4: Communication overheads

Table 5: Storage overheads.

Scheme	Size (bits)
Damandeep, and Devender	1856
Mingxia	2592
Shihong	2880
Mohammad S	2080
Ashok Kumar Das	2080
Leila Azouz Saidane	1504
Majid Bayat	2944
Proposed	2016

Scheme	Size (bits)
Damandeep, and Devender	384
Mingxia	992
Shihong	992
Mohammad S	1344
Ashok Kumar Das	1856
Leila Azouz Saidane	1376
Majid Bayat	2400
Proposed	1344

Security features comparisons.

	Leila Azouz Saidane. [12]	Shihong. [17]	Majid Bayat. [14]	Damandeep, and Devender [2]	Mohammad S. [9]	Ashok Kumar Das. [10]	Mingxia. [5]	**Proposed**
Security Feature								
Mutual authentication	x	√	√	√	√	√	√	√
Anonymity	x	√	x	√	x	√	x	√
Untraceability	-	-	-	√	-	√	√	√
Backward & forward key secrecy	√	√	x	√	√	√	√	√
Key agreement	√	√	√	√	√	√	√	√
Resilience to Attacks								
Packet replay	-	-	-	√	-	√	x	√
forgery	-	-	-	-	-	-	-	√
impersonation	-	-	-	√	-	√	√	√
Denial of service	-	-	-	√		√	√	√
Secret key leakage	x	√	x	√	√	x	x	√
Side-channeling	-	-	-	-	-	-	-	√
Man-in-the-middle	-	-	-	-	-	√	√	√
Session hijacking	-	-	-	-	-	-	-	√
Temporary information leakage	x	√	x	√	√	x	x	√

Fig. 12: Security Features Comparison

✓ Success, ×*Failure*

Attack types including session hijacking, side-channelling, and forging are not taken into account in its design. Similar to this, the plan in [7] disregards untrace ability and packet security.

5.3 Security Features

This subsection presents a comparison between the security characteristics sup- plied by the proposed protocol and those offered by other relevant systems. These comparisons are shown in Table 7, with the first section addressing security char- acteristics and the second section addressing attack resilience. Fig 13 makes it abundantly evident that the suggested protocol is the only one that provides all the security characteristics and resistance against attacks. The schemes in [2,10,7,9,12] and [14], that follow approach. support the following properties in that order: 10, 9, 6, 5, 2, and 2. Thus, the suggested protocol provides the best security and privacy protection at a little higher computing, storage, and com- munication cost than some of these approaches. For this reason, it is the best option to use in a smart home network

6 Conclusion

Many approaches address the privacy and security issues that come with smart houses in an academic setting. Attack vulnerability, however, draws attention to the continuous search for the fine balance between these two factors. Due to the resource constraints and intrinsic limits of smart home devices, implementing strong

cryptographic techniques is challenging, leading to a complex interaction between security and performance. Our carefully designed protocol was tested extensively, confirming its strong mutual authentication and presenting obsta- cles to adversaries pursuing the session key. Informal evaluations confirmed how well it blocked typical smart home intrusions. Our protocol outperformed other protocols Regarding communicating, storing, and computation efficiency.

References

[1] Hossein Abdi Nasib Far et al. "LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT". In: *Wireless Networks* 27 (2021), pp. 1389–1412.

[2] Bogdan-Cosmin Chifor et al. "A security authorization scheme for smart home Internet of Things devices". In: *Future Generation Com- puter Systems* 86 (2018), pp. 740–749.

[3] Saptarshi Debroy et al. "Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems". In: *IEEE Trans- actions on Network and Service Management* 17.2 (2020), pp. 890– 903.

[4] M. Fakroon et al. "Secure remote anonymous user authentication scheme for smart home environment". In: *Internet of Things* 9 (2020), p. 100158.

[5] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. "Security anal- ysis of emerging smart home applications". In: *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2016, pp. 636–654.

[6] Subramani Jegadeesan et al. "EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area net- works (WBANs)". In: *IEEE Access* 8 (2020), pp. 48576–48586.

[7] Zhe Jiang et al. "PSpSys: A time-predictable mixed-criticality system architecture based on ARM TrustZone". In: *Journal of Systems Archi- tecture* 123 (2022), p. 102368.

[8] Damandeep Kaur and Devender Kumar. "Cryptanalysis and improve- ment of a two-factor user authentication scheme for smart home". In: *Journal of Information Security and Applications* 58 (2021).

[9] Damandeep Kaur et al. "An improved user authentication protocol for wireless sensor networks". In: *Transactions on Emerging Telecommu- nications Technologies* 30.10 (2019), e3745.

[10] Damandeep Kaur et al. "An improved user authentication protocol for wireless sensor networks". In: *Transactions on Emerging Telecommu- nications Technologies* 30.10 (2019), e3745.

[11] Akber Ali Khan et al. "A secure and efficient key agreement framework for critical energy infrastructure using mobile device". In: *Telecommu- nication Systems* 78 (2021), pp. 539–557.

[12] Sekaran, R., Munnangi, A. K., Ramachandran, M., & Gandomi, A. H. (2022). 3D brain slice classification and feature extraction using Deformable Hierarchical Heuristic Model. Computers in Biology and Medicine, 149, 105990-105990.

[13] Ramesh, S. (2017). An efficient secure routing for intermittently connected mobile networks. Wireless Personal Communications, 94, 2705-2718.

[14] Sekaran, R., Al-Turjman, F., Patan, R., & Ramasamy, V. (2023). Tripartite transmitting methodology for intermittently connected mobile network (ICMN). ACM Transactions on Internet Technology, 22(4), 1-18.

[15] Akber Ali Khan et al. "LAKAF: Lightweight authentication and key agreement framework for

smart grid network". In: *Journal of Systems Architecture* 116 (2021), p. 102053.

[16] Minhaj Ahmad Khan and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges". In: *Future Generation Com- puter Systems* 82 (2018), pp. 395–411.

[17] Pardeep Kumar et al. "Lightweight and secure session-key establish- ment scheme in smart home environments". In: *IEEE Sensors Journal* 16.1 (2015), pp. 254–264.

[18] Saru Kumari et al. "Design of a provably secure biometrics-based multi- cloud-server authentication scheme". In: *Future Generation Computer Systems* 68 (2017), pp. 320–330.

[19] Saru Kumari et al. "Questioning key compromise attack on Ostad- Sharif et al.'s authentication and session key generation scheme for healthcare applications". In: *IEEE Access* 7 (2019), pp. 39717–39720.

[20] JiLiang Li et al. "Security analysis and improvement of a mutual au- thentication and key agreement solution for wireless sensor networks using chaotic maps". In: *Transactions on Emerging Telecommunica- tions Technologies* 29.6 (2018), e3295.

[21] JiLiang Li et al. "Security analysis and improvement of a mutual au- thentication and key agreement solution for wireless sensor networks using chaotic maps". In: *Transactions on Emerging Telecommunica- tions Technologies* 29.6 (2018), e3295.

[22] Saravanakumar, S., & Thangaraj, P. (2019). A computer aided diagnosis system for identifying Alzheimer's from MRI scan using improved Adaboost. Journal of medical systems, 43(3), 76.

[23] Kumaresan, T., Saravanakumar, S., & Balamurugan, R. (2019). Visual and textual features based email spam classification using S-Cuckoo search and hybrid kernel support vector machine. Cluster Computing, 22(Suppl 1), 33-46.

[24] Saravanakumar, S., & Saravanan, T. (2023). Secure personal authentication in fog devices via multimodal rank-level fusion. Concurrency and Computation: Practice and Experience, 35(10), e7673.

[25] Thangavel, S., & Selvaraj, S. (2023). Machine Learning Model and Cuckoo Search in a modular system to identify Alzheimer's disease from MRI scan images. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 11(5), 1753-1761.

[26] Saravanakumar, S. (2020). Certain analysis of authentic user behavioral and opinion pattern mining using classification techniques. Solid State Technology, 63(6), 9220-9234.

[27] Xiong Li et al. "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems". In: *IEEE Systems Journal* 14.1 (2019), pp. 39–50.

[28] Sarra Naoui, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. "Lightweight and secure password based smart home authentication protocol: LSP-SHAP". In: *Journal of Network and Systems Manage- ment* 27 (2019), pp. 1020–1042.

[29] K. Nimmy et al. "Lightweight and privacy-preserving remote user au- thentication for smart homes". In: *IEEE Access* 10 (2021), pp. 176– 190.

[30] Vincent Omollo Nyangaresi. "Provably Secure Pseudonyms based Au- thentication Protocol for Wearable Ubiquitous Computing Environ- ment". In: *2022 International Conference on Inventive Computation Technologies (ICICT)*. IEEE. 2022, pp. 1–6.

[31] Vincent Omollo Nyangaresi and Sunday Oyinlola Ogundoyin. "Cer- tificate based authentication

scheme for smart homes". In: *2021 3rd Global Power, Energy and Communication Conference (GPECOM)*. IEEE. 2021, pp. 202–207.

[32] JiHyeon Oh et al. "A secure and lightweight authentication protocol for IoT-based smart homes". In: *Sensors* 21.4 (2021), p. 1488.

[33] Jon Patman et al. "Predictive cyber foraging for visual cloud comput- ing in large-scale IoT systems". In: *IEEE Transactions on Network and Service Management* 17.4 (2020), pp. 2380–2395.

[34] Geong Sen Poh, Prosanta Gope, and Jianting Ning. "PrivHome: Privacy-preserving authenticated communication in smart home en- vironment". In: *IEEE Transactions on Dependable and Secure Computing* 18.3 (2019), pp. 1095–1107.

[35] Richa Sarma, Chandan Kumar, and Ferdous Ahmed Barbhuiya. "MACFI: A multi-authority access control scheme with efficient cipher- text and secret key size for fog-enhanced IoT". In: *Journal of Systems Architecture* 123 (2022), p. 102347.

[36] Mengxia Shuai et al. "Anonymous authentication scheme for smart home environment with provable security". In: *Computers & Security* 86 (2019), pp. 132–146.

[37] Ming Tao et al. "Multi-layer cloud architectural model and ontology- based security service framework for IoT-based smart homes". In: *Fu- ture Generation Computer Systems* 78 (2018), pp. 1040–1051.

[38] Mohammad Wazid et al. "BUAKA-CS: Blockchain-enabled user au- thentication and key agreement scheme for crowdsourcing system". In: *Journal of Systems Architecture* 123 (2022), p. 102370.

[39] Mohammad Wazid et al. "Secure remote user authenticated key estab- lishment protocol for smart home environment". In: *IEEE Transactions on Dependable and Secure Computing* 17.2 (2017), pp. 391–406.

[40] Shihong Zou et al. "A robust two-factor user authentication scheme- based ECC for smart home in IoT". In: *IEEE Systems Journal* 16.3 (2021), pp. 4938–4949.