IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 October 2023, accepted 20 November 2023, date of publication 28 November 2023,
date of current version 13 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336763

RESEARCH ARTICLE

Robust and Lightweight Remote User Authentication Mechanism for Next-Generation IoT-Based Smart Home

ZEESHAN ASHRAF[1], ADNAN SOHAIL[2], ABDUL HAMEED[3], MUHAMMAD FARHAN[4], FAIZ ABDULLAH ALOTAIBI[5], AND MRIM M. ALNFIAI[6]

[1]Department of Computer Science, The University of Chenab, Gujrat 50700, Pakistan
[2]Department of Computing and Technology, IQRA University, Islamabad Campus, Islamabad 44000, Pakistan
[3]Department of Software Engineering, IQRA University, Islamabad Campus, Islamabad 44000, Pakistan
[4]Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan
[5]Department of Information Science, College of Humanities and Social Sciences, King Saud University, Riyadh 11362, Saudi Arabia
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

Corresponding author: Zeeshan Ashraf (zeeshan.np@gmail.com)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project under Grant RSPD2023R838.

ABSTRACT The IPv4 address architecture has been declared ended finally due to the fast growth of the Internet of Things (IoT). IPv6 is becoming a next-generation communication protocol and provides all the requirements that the industry needs. A smart home is an emerging technological revolution in which IoT-enabled smart physical objects such as smart TVs, smart refrigerators, smart locks, etc. are linked to the Internet to make human life more comfortable. There are several resource-constrained smart devices interconnecting with 6LoWPAN to control the smart home remotely. The communication channels used by cellular communication are vulnerable and increase security threats especially related to authentication. A reliable and portable remote authentication method is critical for ensuring safe communication in the next-generation smart home environment. Recently, many authentication schemes have been proposed but adopt complex mathematical techniques or protocols that are viewed as heavyweights in the context of computation and communication costs. This research proposes a lightweight and reliable remote authentication mechanism for the next generation of IoT-based smart homes. Informal and formal security assessments through the AVISPA tool determine the robustness of our proposed scheme. Moreover, we implemented our authentication scheme on a Linux-based client-server network model by using Android programming. In addition, we compared our proposed scheme with existing schemes based on computation and communication costs. Results show that our proposed mechanism reduced computation costs by up to 54.03 % and reduced communication costs by up to 25.28 % related to existing schemes. So, our proposed scheme is better, more secure, and most suitable for smart home ecosystems.

INDEX TERMS Authentication, IoT security, key exchange, NGN, security analysis, smart home.

I. INTRODUCTION

DUE to the fast growth of the Internet of Things (IoT) and fast development in emerging technologies, the Internet is moving towards Next-Generation Networks (NGNs). A next-generation IoT is a packetized and digitized network that transports different types of traffic such as voice, video, or data at a very high speed [1]. The billions of new smart devices have ended the IPv4 address architecture. The IPv6 address architecture satisfies all the requirements of NGN [2]. Internet Services Providers (ISPs) are moving towards IPv6 with the help of emerging technologies [3]. The improvement of 5G and 6G cellular technology has performed an essential role in the popularity of smart homes

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

or smart cities concept [4]. IoT introduces a home automation concept called smart home where physical objects called things such as smart TVs, smart security cameras, smart lights, smart ACs, smart locks, etc. have built-in sensors, limited processing ability, and short memory are connected to the Wireless Personal Area Network (WPAN) [5]. The Low-Power Wireless Personal Area Network (6LoWPAN) is an IEEE 802.15.4 protocol standard to support IPv6 packets to be transmitted on top of low-power wireless networks [6]. The major theory behind the invention of 6LoWPAN is providing a platform independent of the internet even on low-power devices that have inadequate processing resources and have to be capable to contribute in the IoT [7]. Next-generation mobile communication networks, IPv6 address architecture, and IoT-enabled smart devices are crucial for smart city infrastructure [8].

A smart city concept is a modern urban area that is based on technology. In smart cities, different types of electronic smart devices such as IoT-based sensors are used to collect specific data and transfer the data to central systems. The data are collected from different citizens, devices, buildings, and assets. The data are used to analyze & monitor the traffic, manage transportation systems, monitor power plants, manage water supply networks, criminal investigations, weather stations, pollution monitors, vehicle networks, home automation systems, and other community services [9]. The data helps to improve the operations across the city.

IoT-based smart home appliances are increasing the volume of the internet day by day. Based on Moore's law, it has been predicted that by the end of 2025, the number of IoT devices long go beyond 100 billion worldwide and distribute an average of more than 10 devices per person [10]. These smart devices are controlled by users remotely through smartphones with the help of the internet. The user can turn on or off smart lights, open or close smart doors, increase or decrease the temperature, and check surveillance remotely by accessing the smart devices through 5G or 6G-enabled IPv6 portable devices. The communication channels between remote users and smart home devices are vulnerable [11]. It increases security threats especially related to authentication. If an attacker finds the secret data, the adversary will misuse it for his purposes. Therefore, security and privacy are necessary for the smart home environment. Moreover, data should be exchanged between two parties confidential and without any change [12].

Although, the IPv6 address architecture provides a built-in security feature with the support of the extension header [13]. Despite these improvements in IPv6, some malicious attempts such as man-in-the-middle (MITM) attacks, replay attacks, impersonation attacks, and denial-of-service (DoS) attacks affect both IPv4 and IPv6 architectures and do not discriminate by appearance [14]. In an MITM attack, the adversary is involved between two communication parties secretly [15]. The authentication between two communication parties is compromised due to the MITM attack. Authentication is a technique of verifying the identification of someone or device [16]. Authentication is the top priority service in IoT-based sensor networks while other security services such as data confidentiality, and data integrity are also important in smart cities [17]. There are several authentication types such as Kerbrose, password-based authentication, biometric authentication, hash-based authentication, digital certificates, multi-factor authentication, and token-based authentication to perform verification [18], [19], [20], [21]. Smart cities or smart homes use IoT-enabled smart devices and sensors. Smart devices have short processing power and short memory. Therefore, smart devices demand lightweight and secure authentication protocols.

A. CONTRIBUTION

The foremost contributions of the studies have a look at are concise as follows:

1) We introduce a lightweight authentication scheme by the usage of a hash-based method with a pre-shared session key to recognize the legitimacy of remote users in smart homes.
2) We also propose a secure and lightweight key exchange algorithm for resource-constrained smart devices.
3) We show the robustness of our proposed authentication scheme via informal and formal security analysis by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool.
4) We implement our authentication scheme on Linux-based Ubuntu operating systems in client-server networks by using Android programming.
5) Finally, We compare the performance of our recommended authentication scheme with other existing schemes based on communication overhead, computation cost, and security properties.

B. PAPER ORGANIZATION

The remainder of the research paper structured as: Section II describes associated works and compares this study with present research. Section III describes the IoT-based smart home network model and adversary model. Section IV presents a lightweight remote user authentication scheme for a smart home environment. Section V provides a formal and informal security analysis of the proposed scheme. Section VI compares the proposed scheme with the existing authentication schemes. Finally, section VII concludes the paper.

II. RELATED WORKS

A variety of available proposed mutual authentication schemes for IoT-based smart home environments are classified into asymmetric-key-based and symmetric-key-based groups.

A. ASYMMETRIC-KEY-BASED AUTHENTICATION SCHEMES

In asymmetric-key-based authentication schemes, keys are generated through asymmetric algorithms such as Elliptic Curve Cryptography (ECC) and Rivest Shamir Adleman

(RSA). The ECC and RSA are heavyweight in terms of computation and communication costs [22]. So, ECC and RSA are not suitable for smart devices while smart devices demand lightweight due to low computation and communication powers [23].

B. SYMMETRIC-KEY-BASED AUTHENTICATION SCHEMES

In symmetric-key-based authentication schemes, keys are exchanged through symmetric algorithms such as Diffie-Hellman (DH) and Elliptic Curve Diffie Hellman (EC-DH). EC-DH is an advanced version of DH with extra functions in terms of small key length. Both DH and EC-DH are non-authenticated. Hence, DH and EC-DH are exposed to MITM attacks [24]. In some research studies, researchers introduced their own key exchange methods.

In [25], researchers proposed an authentication model for smart homes. The proposed authentication model uses a DH key exchange algorithm between two parties. The researchers have evaluated the security strength of the proposed authentication model by using the AVISPA analyzer tool. However, the proposed model fails to provide security against MITM attacks because the DH protocol itself is a non-authentic protocol, fails to ensure message freshness, and may not withstand a known-key attack. The time complexity behavior of the DH key exchange algorithm is polynomial. Therefore, it increases computation time and communication overhead. So, this scheme is not recommended for resource-constrained smart devices.

In [26], authors proposed a lightweight authentication model for IoT-based smart homes. The scheme provides mutual authentication and identity assurance by using the concepts of temporary identity, keyed-hash chain mechanism, and fog computing. In this research study, the authors claimed that their scheme is secured against several known attacks. Unfortunately, the scheme may fail to provide complete confidentiality and protection against known key attacks. So, this scheme is not suitable for smart homes.

In [27], researchers proposed a privacy-preserving two-factor authentication scheme for IoT devices. The scheme uses Physically Unclonable Functions (PUF) authentication methodology to protect IoT devices against physical and cloning assaults. The authors said that their method resists impersonation, achieves untraced ability, and exhibits security traits including resistance to physical attacks and mutual authentication. Because of the extensive usage of hash operations, their system requires high computation. As a result, IoT-based applications may not be appropriate for the proposed strategy.

In [28], researchers extended the research work of other researchers and presented an upgraded authentication scheme for next-generation IoT-based infrastructure. According to this research study, the scheme is safe against conventional IoT-based smart home attacks such as impersonation attacks, offline/online password guessing attacks, replay attacks, DoS attacks, and MITM attacks. However, the proposed scheme has not been evaluated by any formal security analysis tool. Furthermore, the proposed scheme has become more complex, and its computation cost is very high. The proposed scheme is not suitable for the smart home environment.

Similarly, in [29], [30], [31], [32], and [33], researchers proposed authentication schemes for IoT-based smart home environments. The proposed schemes adopt very complex procedures for key exchange and authentication processes. Multiple times XOR, concatenation, and hashing functions are used to perform authentication. The proposed schemes increase computation time and communication overhead. In these schemes, heavy-size messages are exchanged during key exchange and authentication. The communication overhead increases delays.

Although, there are several proposed authentication schemes for IoT-based smart home environments. Most of the proposed schemes use heavyweight key exchange algorithms while some proposed schemes use complex mathematical operations. In contrast with existing studies, we introduce and implement a simple, robust, and lightweight remote user authentication mechanism for the next-generation IoT-based smart homes by using a pre-shared symmetric session key.

III. IOT-BASED SMART HOME ENVIRONMENT

The idea of a smart home has gained enormous popularity throughout the world because of the rapid growth of information and communication technologies (ICT) and the Internet of Everything (IoE). In a smart home automation system, IoT-enabled smart devices such as smart TVs, smart security cameras, smart lights, smart ACs, smart locks, etc. are connected through wireless technology. A variety of wireless technologies are available for connecting smart home devices but 6LoWPAN is the most suitable protocol for IPv6 to enable IPv6 packets to be carried on top of low-power wireless networks [34]. Users utilize different services by accessing these smart devices either inside the network or outside the network. Users can control smart devices with an application, check the status of smart devices, and perform on or off services on various smart devices through smartphones. Users can control smart devices easily and remotely within a smart home by connecting to the smart home network.

A. SYSTEM MODEL

Mobile users, smart gadgets, a home gateway, and a registration authority are the typical components of a smart home automation system. Smart devices have limited resources, including low bandwidth, short memory, and short processing power. The home gateway or server facilitates communication between smart gadgets. The wireless access point serves as a bridge between the smart devices and a home gateway or server. Figure 1 depicts the system model of a smart home.

According to our suggested system paradigm, the gateway or server serves as a connection point between smart devices and remote users. It offers an interface for preserving connections. By connecting to a gateway or server using internet-capable mobile phones or tablets, mobile users

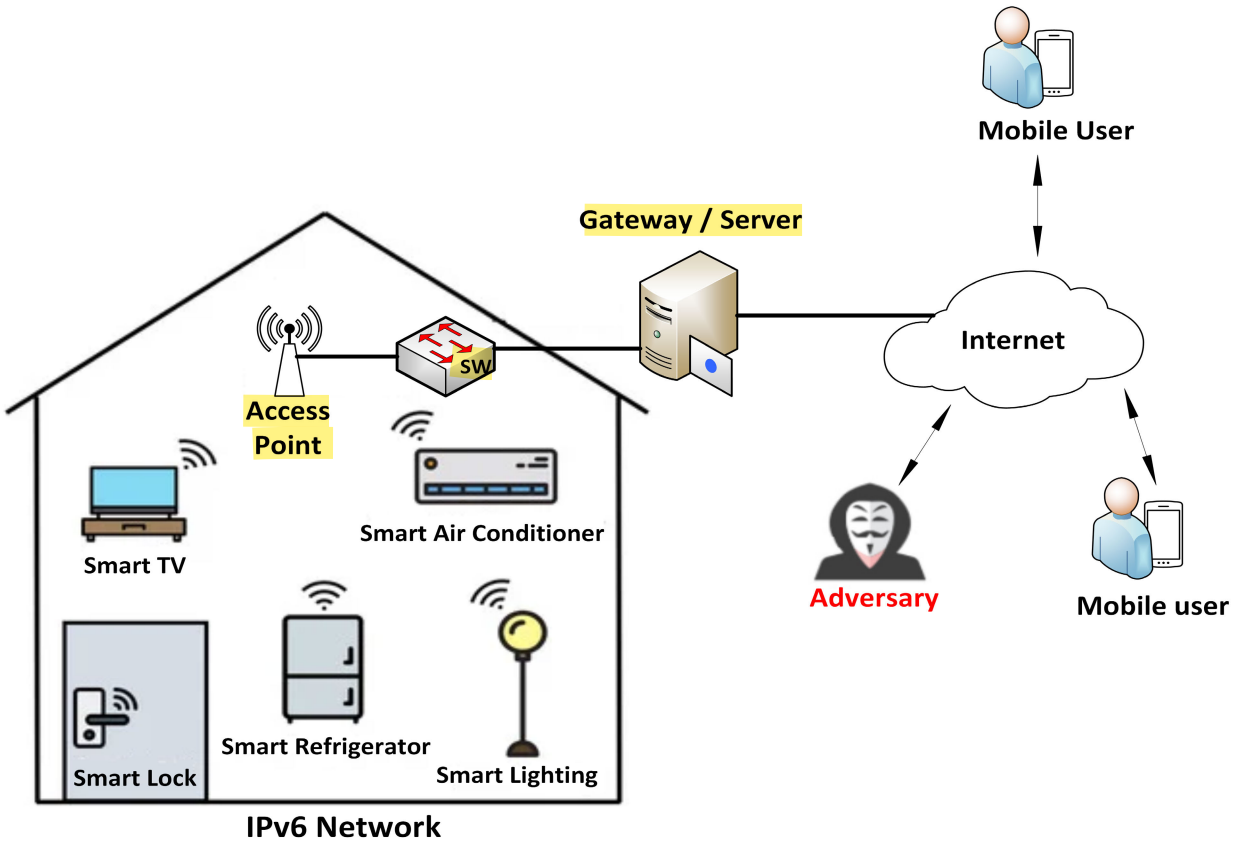

FIGURE 1. Smart Home Environment.

operate smart devices remotely at any time and from any location [35]. The proposed IoT-based smart system is composed of mobile users (MUs), smart devices (SDs), an access point (AP), and a home gateway (HGW). The home gateway performs multiple roles such as a registration authority (RA), server, virtual router, and virtual firewall. The server is responsible for initializing the system, providing an interface, registering MUs and SDs, and other communication services. MU, SD, and HGW are needed to register at RA. RA stores the information of each entity in its database. Additionally, RA keeps all the data necessary for the MU, SD, and HGW in the database. Before using the services of the smart home automation system, MU and HGW exchange symmetric session keys for mutual authentication procedures. The notation of this paper is described in Table 1.

B. ADVERSARY MODEL

To assess the effectiveness and security of the suggested protocol, we consider the Dolev-Yao (DY) threat model [36]. These are some examples of an adversary's capabilities.

1) Using a public channel, the adversary may listen in on, intercept, replay, inject, and change transmitted communications. The adversary can then launch MITM, replay, and impersonation attacks.
2) By the use of a power analysis attack, the adversary can get the right of entry to a legitimate consumer's cellular or a smart device and get better any mystery credentials that are kept inside the memory.

TABLE 1. Notations and Descriptions.

Notation	Description
RA	Registration Authority
T_{ED}	Time for Encryption or Decryption
T_{Exp}	Time for ECC point Multiplication
T_{Fe}	Time for Fuzzy Extractor
T_{hmac}	Time for HMAC
SD	Smart Devices
HGW	Home Gateway
ID_{SD}	Identification of Smart Devices
ID_U	User's Identity
HID_U	Hash-based User's Identity
PSW_U	Password of User
$HPSW_U$	Has-based Password of User
N_1, N_2	Two secret random numbers
N_S, N_U	Randomly generated numbers by Server and User
FR_S, FR_U	Final results sent by Server and User
K_S	Secret key
$\oplus$	XOR
Mod	Modulus
$\|\|$	Concatenation
$Hash(.)$	Hash function
$HMAC_S$	Hash value generated by Server
$HMAC_U$	Hash value generated by User
$E_K(.)$	Encryption by using symmetric key

3) The opponent has access to the session states, long-term keys, and short-term keys of each side.
4) The attacker can steal the information that is exchanged across network components.
5) The adversary can perform active and passive assaults.

In addition, we developed a presumption for our scheme. Since the home gateway contains a secure database, the attacker cannot extract the data kept there.

IV. PROPOSED SCHEMEL

This section describes the proposed scheme. The scheme consists of the registration phase, login phase, key exchange phase, and authentication phase.

A. SMART DEVICE REGISTRATION PHASE

First, every smart device in the smart home system should be registered. At the registration phase, RA is assigned a unique ID_{SD} to every smart device. The ID_{SD} of the smart device and the status of the smart device are stored in the server's database.

B. USER REGISTRATION PHASE

All authorized users must be registered at RA. The user selects a unique username as an ID_U, and password PSW_U respectively. The user generates hash-based identity HID_U and hash-based password $HPSW_U$ by using a hash function as described in Eq. (1) and Eq. (2).

$$HID_U = hash\,(ID_U) \tag{1}$$

$$HPSW_U = hash\,(ID_U \parallel PSW_U) \tag{2}$$

The user's secret information is saved to the server's database secretly along with the user's email address and mobile number.

C. LOGIN PHASE

Remote user R_U sends hash-based identity HID_U along with hash-based password $HPSW_U$ to the server for verification. For security reasons, the identity and password are not sent in clear text. The server locates the HID_U and $HPSW_U$ from databases and verifies them. If any of the given login information is incorrect, then the server immediately terminates the connection. In case of multiple failed login attempts which were mentioned then, the server blocks that identity temporarily to save time and bandwidth. If both HID_U and $HPSW_U$ are matched with data saved in the server's database, then it verifies that the user is a registered user. The server picks two larger randomly generated numbers N_1 and N_2 respectively and sends them to the user for a specific period through an alternative channel. For security reasons, an alternative channel such as a registered mobile number of the user is adopted. These two larger random numbers are used to exchange the symmetric session key between the server and the remote user. If the remote user does not receive these two numbers N_1 and N_2 then the user sends a request for new numbers.

D. SESSION KEY EXCHANGE PHASE

After successful login, the symmetric session key exchange process starts by using our proposed symmetric session key exchange Algorithm 1. The remote user generates a larger random number of N_U. The size of the random number should be 128 bits. The user multiplies the number N_U with the N_1 number, adds the number N_1, and computes Res_U as shown in Eq. (3).

$$Res_U = (N_U \times N_1) + N_1 \tag{3}$$

The user multiplies the result Res_U with the second number N_2, adds both numbers N_1, N_2, and calculates the final result FR_U as shown in Eq. (4).

$$FR_U = (Res_U \times N_2) + N_1 + N_2 \tag{4}$$

The user finally sends the final result FR_U to the server. The result FR_U is not a key and if the intruder captures it then he can't retrieve the actual key until he knows both secret numbers N_1 and N_2 respectively. When the server receives the result FR_U by the remote user then the server extracts the number N_U by using both numbers N_1 and N_2 respectively. The server subtracts the values of N_1 and N_2 and gets Res_S as depicted in Eq. (5).

$$Res_S = FR_U - (N_1 + N_2) \tag{5}$$

The server first multiplies N_1 and N_2, divides Res_S, subtracts one, and finally gets N_U as presented in Eq. (6).

$$N_U = (Res_S \,/\, (N_1 \times N_2)) - 1 \tag{6}$$

Similarly, the server generates a larger random number of N_S and sends the result of FR_S to the user by following the same procedure as shown in Eq. (3) and Eq. (4).

At last, the server and the user compute bitwise XOR of N_U with N_S which were received on both sides, calculate mod with M, and get the final session key K_S on both sides secretly as shown in Eq. (7). M is a variable that determines the size of the key. Initially, it stores the larger value of size 128 bits. It limits the size of the key to 128 bits. The larger size of the key minimizes the threats of brute-force attacks [24].

$$K_S = (N_U \oplus N_S)\ mod\ M \tag{7}$$

The same key K_S has been exchanged between the server and the recognized remote user. On every newly established connection between the remote user and the server, the session key will be changed. The session key is used for authentication.

E. AUTHENTICATION PHASE

The primary goal of our proposed scheme is to authenticate the remote users over an IPv6 IoT-based smart home network so that the MITM's interception will fail. Authentication is the process of verifying the identity of a person, device, or service [37]. Our proposed authentication scheme uses a Hash-based Message Authentication Code (HMAC) for the authentication process. The HMAC is a specific type of

Algorithm 1 Proposed Key Exchange Algorithm

Require: M is a variable that stores the value of size 128 bits. Server saved the hash-based identity and hash-based password of the clients HID_C *and* $HPSW_C$

Client Sends HID_C *and* $HPSW_C$ *to Server* : $(HID_C, HPSW_C) \rightarrow$ *Server*
if $HID_C = HID_C$ AND $HPSW_C = HPSW_C$ **then**
  Server generates N_1, N_2 and sends to client on mobile number: N_1 *and* $N_2 \rightarrow$ *Client*
  Client generates a larger random number as N_C : $N_C \leftarrow rand()$
  if $N_C = 0$ **then**
    Goto Step 4
  end if
  Set $C = (N_C \times N_1) + N_1$
  Set $R_C = (C \times N_2) + N_1 + N_2$
  Client Sends R_C *to Server* : $R_C \rightarrow$ *Server*
  Set $r_C = R_C - (N_1 + N_2)$
  Set $N_C = (r_C \ / \ (N_1 \times N_2)) - 1$
  Server generates a larger random number as N_S : $N_S \leftarrow rand()$
  if $N_S = 0$ **then**
    Goto Step 13
  end if
  Set $S = (N_S \times N_1) + N_1$
  Set $R_S = (S \times N_2) + N_1 + N_2$
  Server Sends R_S *to client* : $R_S \rightarrow$ *Client*
  [Client performs the same process from 11 to 12]
  /* Client and Server compute the same Key as */
  Set $K_S = (N_C \oplus N_S)$ *mod* M
  if $K_S = 0$ **then**
    Goto Step 4
  end if
else
  Connection Terminate
end if

fixed-length message authentication code that is generated by a hashing algorithm and a secret key [38]. The size of the HMAC depends upon the hashing algorithm [39]. SHA-1 generates a 160-bit (20-byte) long hash value and it consists of 40 digits long hexadecimal numbers [40]. SHA-256 generates a fixed-size code of 256 bits long. In our proposed scheme, the IPv6 address of the host concatenates with a randomly generated number by the host, and the session key is used to generate a hash value through the SHA-256 algorithm as depicted in Eq. (8) and Eq. (9).

$$HMAC_U = SHA - 256\ (IP\ Address_U \parallel N_U, K_S) \quad (8)$$

$$HMAC_S = SHA - 256\ (IP\ Address_S \parallel N_S, K_S) \quad (9)$$

The HMAC calculated values sent to each other on both sides. HMAC values are re-calculated on both sides for cross-checking and verification with the received value. If the calculated HMAC and received HMAC are verified, then the authentication process is completed on both sides. After a successful authentication, the remote user grants access and control to smart devices. If the authentication process fails on any side, then the connection is terminated immediately on both sides and declared an adversary attack. The login, key exchange, and authentication processes are described in Fig. 2.

1) SIMPLE PRACTICAL EXAMPLE

A simple practical example of 8-bit key exchange and authentication is represented as follows for simplification.

1) Suppose M = 256.
2) Suppose the server generates two larger random numbers $N_1 = 11$, $N_2 = 13$, and sends them to the remote user after login verification.
3) The remote user generates a larger random number $N_U = 180$. The user calculates $FR_U = ((((180 \times 11) + 11) \times 13) + 11 + 13) = 25907$ and sends final results $FR_U = 25907$ to the server.
4) The server generates a larger random number of $N_S = 240$. Server calculates $FR_S = ((((240 \times 11) + 11) \times 13) + 11 + 13) = 34487$ and sends final results $FR_S = 34487$ to the remote user.
5) The server and the user extract N_S and N_U from FR_S and FR_U respectively. The symmetric session key K_S is shared on both sides as $K_S = (180 \oplus 240) \bmod 256$. The symmetric key value $K_S = 68$ has been shared between the server and the remote user. The binary value of 68 is "1000100".
6) The remote user calculates $HMAC_U$ by using the SHA-256 hash function with its IPv6 address = 2001:0:1::1, randomly generated number $N_U = 180$, and session key $K_S = 68$ as SHA-256 (2001:0:1::1 ‖ 180, 68) = "9f7a878074e73a2f4e96067609ba8e23bb0b05f af37f21a20eed9fd24dc67c3e", and sends it to the server for verification.
7) Similarly, the server calculates $HMAC_S$ by using the SHA-256 hash function with its IPv6 address = 2001:0:10::10, randomly generated number $N_S = 240$, and session key $K_S = 68$ as SHA-256 (2001:0:10::10 ‖ 240, 68) = "ba2dc7db02d732e6e19b1bb39478f35900d1 ce48ee8fc1efd9c8416f992b79dc", and sends it to the remote user for verification.
8) The server and the remote user generate HMAC values by using each other IPv6 addresses, random numbers, and K_S for cross-checking.
9) Both sides compare calculated results with the values received by each other.
10) After verification, the server grants access to remote users. If the verification fails, the connection with the remote user is cut off immediately.

V. SECURITY ANALYSIS

In this section, we prove the robustness of our proposed scheme against different types of known attacks through formal and informal security analysis.

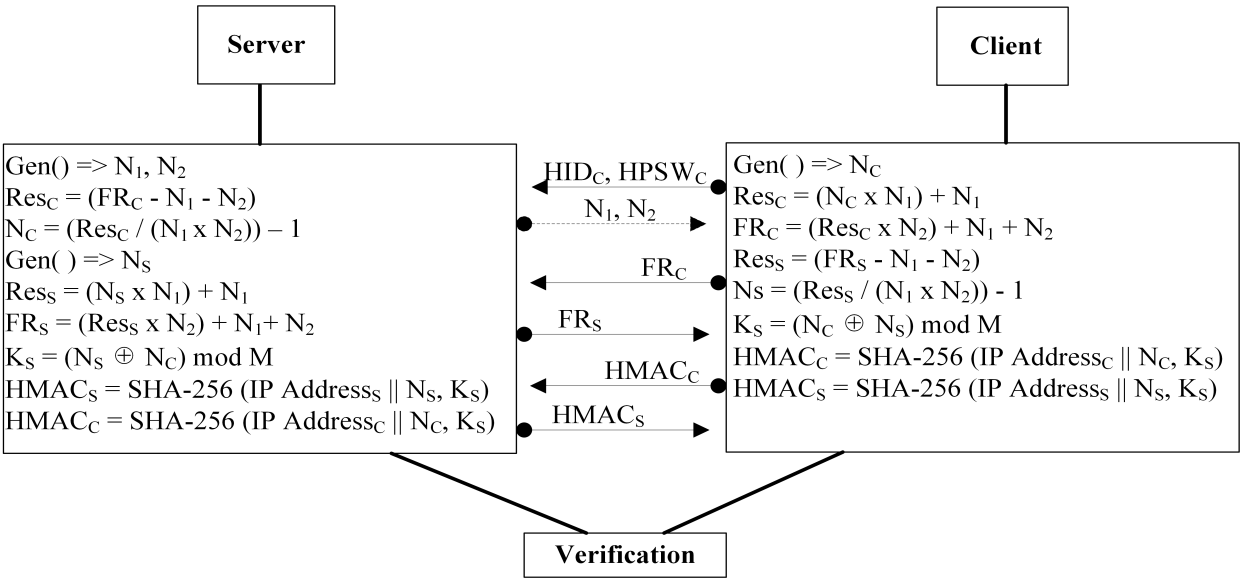

FIGURE 2. Key Exchange and Authentication Process.

A. INFORMAL SECURITY ANALYSIS

The strength of our proposed scheme with respect to the required security features is presented in [23]. Informal security analysis shows how our proposed scheme meets security requirements against multiple attacks such as password guessing attacks, brute-force attacks, impersonate attacks, replay attacks, forgery attacks, denial of service attacks, MITM attacks, perfect forward secrecy, etc.

B. FORMAL SECURITY ANALYSIS THROUGH AVISPA

To test the proposed scheme's strength, we employed the AVISPA tool. When evaluating the security of various protocols and schemes that require messages to be sent between two or more entities, AVISPA is a trustworthy open-source tool. AVISPA uses High-Level Protocol Specification Language (HLPSL) scripting language. At the backend of the AVISPA, on-the-fly model checker (OFMC) compiles the results. The fact that communication between the entities takes place across a compromised channel (dy) is also noted. This means that the channel is open to all the assaults described in the Dolev-Yao (DY) adversary model III-B. A Security Protocol Animator (SPAN) tool is used for AVISPA [41].

The symmetric key sharing and authentication operations are programmed in HLPSL and tested on AVISPA to gauge the robustness of our suggested authentication strategy against well-known vulnerabilities like replay and MITM attacks. The essential tasks of nodes (Server and Client) include agent roles (S and C), crypto-operations, and local declarations. AVISPA code and simulation results are available on GitHub [42].

1) RESULTS THROUGH OFMC AND ATSE

The robustness of our proposed scheme against replay attacks and MITM attacks is verified by using the OFMC and CL-AtSe at the backend and is reported safe as shown in Fig. 3.

TABLE 2. Devices and their Description.

Device	Description
Router	GNS3-based CISCO 3700 Series, IOS v.12.4(15)T10, C3725-adventerprisek9-mz.124-15.T10 Total = 3
PCs	Linux-based Ubuntu 18.04 LTS Total = 2

VI. IMPLEMENTATION AND PERFORMANCE ANALYSIS

We implemented our proposed scheme on Linux-based virtual machines (Ubuntu 18.04.2 LTS) in a client-server IPv6 network model by using Android socket programming. The virtual machines installed on Oracle VM Virtual Box integrated to the GNS3 v2.1.16 simulator with system specifications as Intel(R) Core, TM *i*3-M390 2.67 GHz processor, 6 GB DDR3 RAM, 3 MB cache memory with 64-bit Windows 10 Professional operating system. The experimental setup is described in Fig. 4. Table 2 displays the description of the devices.

In our next-generation IPv6 experimental setup, both virtual machines (client and server) are connected to different IPv6 networks. The server's IPv6 address is 2001:0:10::10/64 while the client's IPv6 address is 2001:0:1::1/64. An intruder is also connected to the network having full control over the network. The connectivity between the client and the server is shown in Fig. 5.

A. COMPUTATION COSTS COMPARISON

We compare the anticipated computing costs of our proposed scheme to those of current schemes in the computation cost comparison. In Table 3, we specified the expected unit time costs of several activities that were completed during a

```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/myScheme.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.12s
  visitedNodes: 108 nodes
  depth: 4 plies
```

```
%AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/myScheme.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 15 states
  Reachable  : 7 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

FIGURE 3. Results through OFMC and AtSe.

TABLE 3. Estimated Simulation Time of Various Operations.

Notation	Description	Simulation Time (ms)
$T_{E/D}$	Time for Encryption/Decryption	0.0215
T_{exp}	Time for ECC point Multiplication	0.4276
T_{FE}	Time for Fuzzy Extractor	0.4276
T_{HMAC}	Time for HMAC	0.0052
$T_{\oplus}$	Time for XOR Operation	0.0004
$T_{\|\|}$	Time for Concatenation Operation	0.0004
T_{ran}	Time for Generate Random Number	0.0052
T_H	Time for one-way Hash function	0.0052
T_M	Time for Mathematical Operation	0.0004

TABLE 4. Computation Cost Comparison.

Ref.	Total Computation Cost	Estimated Time (ms)
[5]	$18T_H + 9T_{\oplus} + 56T_{\|\|} + 3T_{ran}$	0.1352
[22]	$16T_H + 21T_{\oplus} + 70T_{\|\|} + 4T_{ran} + 4T_{exp}$	1.4232
[26]	$22T_H + 18T_{\oplus} + 47T_{\|\|} + 1T_{ran}$	0.1456
[28]	$42T_H + 25T_{\oplus} + 105T_{\|\|} + 3T_{ran}$	0.2860
[29]	$20T_H + 29T_{\oplus} + 27T_{\|\|} + 3T_{ran} + 3T_{E/D}$	0.2065
[30]	$24T_H + 16T_{\oplus} + 73T_{\|\|} + 4T_{ran}$	0.1812
[32]	$10T_H + 12T_{\oplus} + 47T_{\|\|} + 3T_{ran}$	0.0912
[33]	$29T_H + 17T_{\oplus} + 97T_{\|\|} + 4T_{ran}$	0.2172
Our	$2T_H + 2T_{\oplus} + 3T_{\|\|} + 4T_{ran} + 22T_M + 2T_{HMAC}$	0.0524

simulation on an Intel(R) Core, TM *i*7-4710 HQ 2.50 GHz computer with 8 GB of memory and the 64-bit Windows 8 operating system [22].

TABLE 5. Communication Cost Comparison.

Ref.	Total Communication Cost (bits)	Message Exchanged
[5]	(608 + 640 + 352 + 352) = 1952	4
[22]	(768 + 320 + 320 + 320) = 1728	4
[26]	(1056 + 640 + 384 + 544) = 2624	4
[28]	(800 + 640 + 640 + 448 + 448 + 320) = 3296	6
[29]	(640 + 640 + 320 + 320 + 160) = 2080	5
[30]	(544 + 320 + 448 + 576) = 1888	4
[32]	(800 + 416 + 416 + 672) = 2304	4
[33]	(608 + 320 + 320 + 320) = 1568	4
Our	(320 + 256 + 160 + 160 + 160 + 160) = 1216	6

Table 4 and Fig. 6 shows the assessment outcomes of computational costs among our proposed scheme and other related schemes. The results show that our proposed scheme including the key exchange process consumed less estimated computational time as compared to other existing schemes. Our proposed scheme reduced computation costs by up to 54.03 % compared to [32].

B. COMMUNICATION OVERHEAD COMPARISONS

When comparing the anticipated communication overhead of our proposed scheme with other relevant schemes, we call this comparison the communication cost comparison. The amount of data transmitted through the communication lines in packets and its size in bits per second are calculated as communication costs. An ECC point is assumed to be 320 bits in size, a hash digest to be 160 bits (assuming the

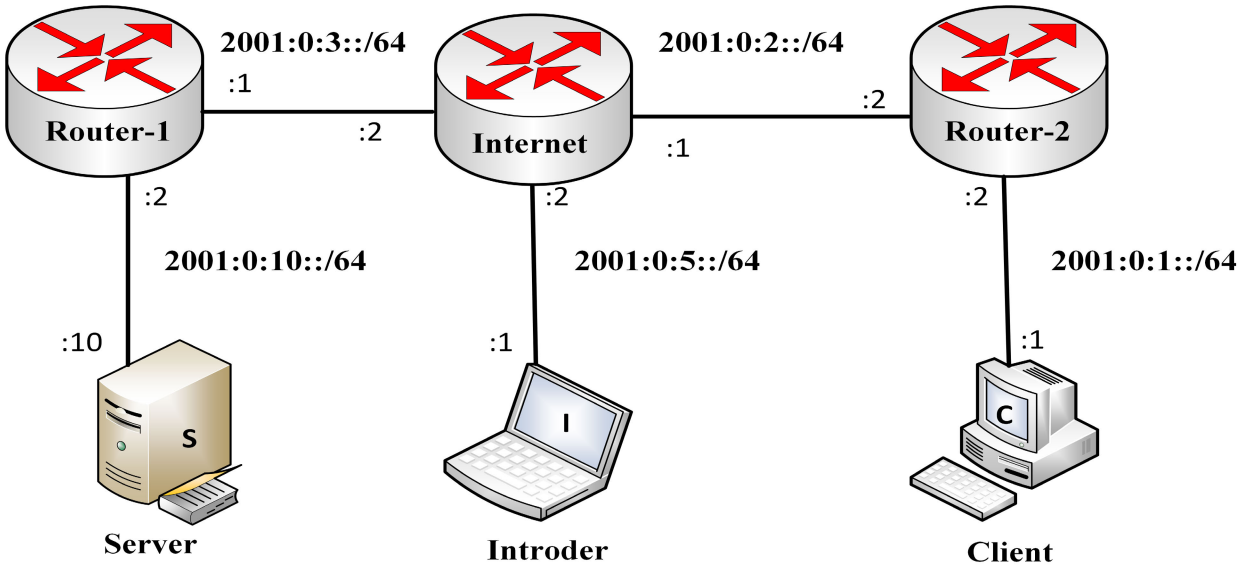

FIGURE 4. Experimental Setup.

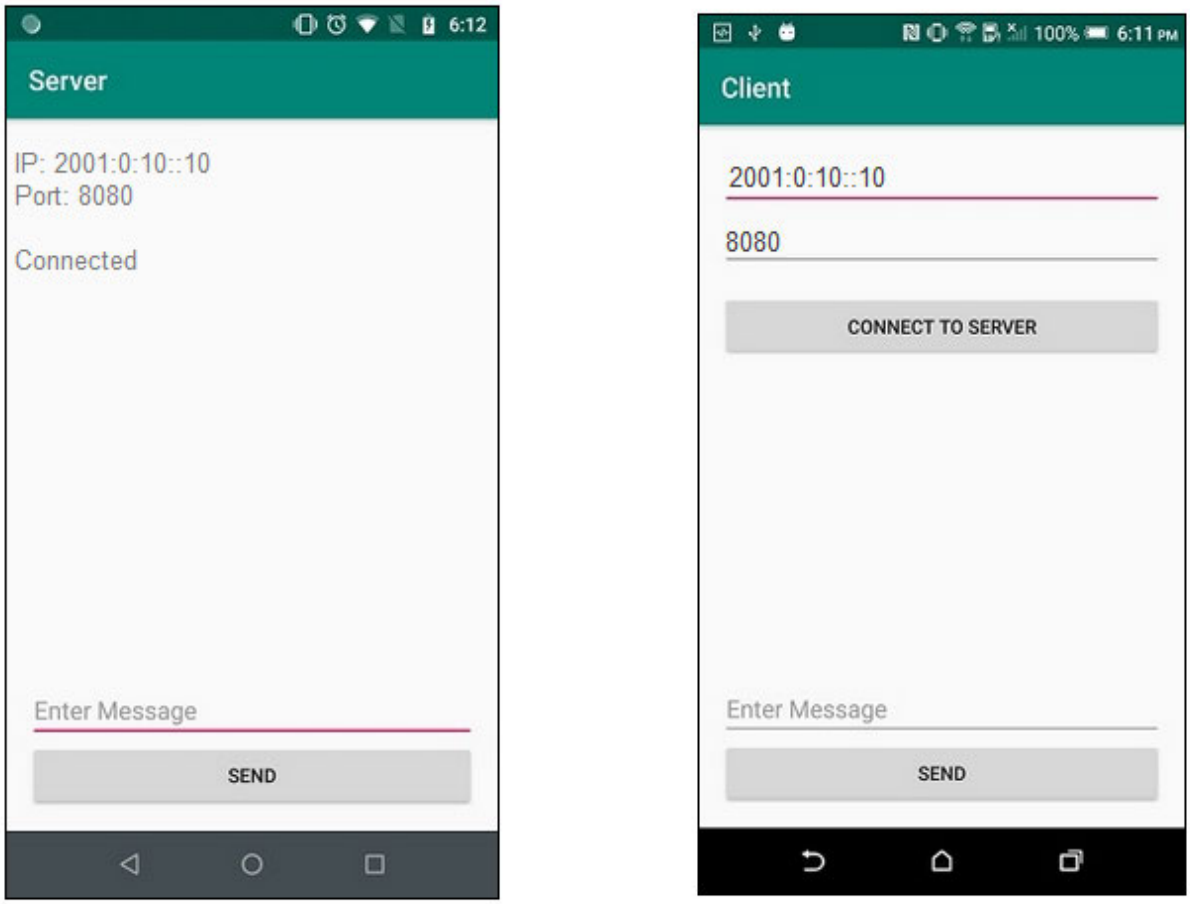

FIGURE 5. Connectivity between Client and Server.

SHA-1 hashing technique is used for all schemes), 128 bits for random numbers, 512 bits for encryption and decryption, 32 bits for timestamp, and 128 bits for identification to compare communication costs. Our suggested scheme

TABLE 6. Security Features Comparison.

Security Features	[5]	[22]	[26]	[28]	[29]	[30]	[32]	[33]	Our
Impersonate Attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password Guessing Attacks	x	✓	✓	✓	✓	✓	✓	✓	✓
Replay Attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Forgery Attacks	✓	✓	✓	x	✓	✓	x	x	✓
MITM Attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Forward Secrecy	x	✓	✓	x	✓	x	✓	✓	✓
Data Integrity and Privacy	✓	✓	✓	✓	✓	✓	✓	✓	✓

Acronyms: ✓ Protected against attacks
x Vulnerable against attacks

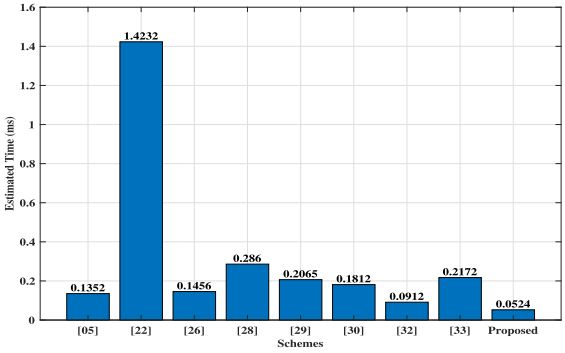

FIGURE 6. Computation Cost Comparisons.

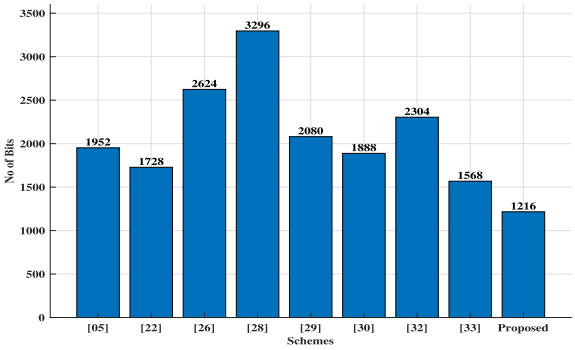

FIGURE 7. Communication Cost Comparisons.

computes the communication overhead of 6 messages as $320 + 256 + 160 + 160 + 160 + 160 = 1216$ bits that were passed during key exchange and authentication processes.

Table 5 and Fig. 7 displays the assessment effects of envisioned communication costs between our proposed scheme and different related schemes. Outcomes display that our suggested scheme including the key exchange process consumed less estimated communication cost as compared to other existing schemes. Our proposed scheme reduced communication costs by up to 25.28 % compared to [33].

C. SECURITY PROPERTIES COMPARISONS

In Table 6, the comparisons of the security properties of the proposed scheme and other similar existing schemes are highlighted.

VII. CONCLUSION

Although, IPv6 has built-in security. However, some attacks such as MITM attacks, replay attacks, and impersonation attacks affect IPv6 architecture. Authentication is compromised due to an MITM attack. Researchers introduced authentication schemes for remote users to provide security against MITM attacks and impersonate attacks. The available authentication schemes adopted complex mathematical operations and exchanged heavy-size messages. The available schemes increase computation and communication costs for smart devices. We proposed a robust and lightweight authentication scheme by using a pre-shared symmetric session key for the next-generation of IoT-based smart homes. In addition, the robustness of the proposed scheme has been proven through informal security analysis as well as through formal security analysis using the AVISPA tool. Moreover, we implemented our authentication scheme on a Linux-based IPv6 client-server network model with Android socket programming. Our proposed scheme is lightweight in terms of computation and communication costs. According to the performance comparison with other comparable existing schemes our proposed scheme reduced computation costs by up to 54.03 % and reduced communication costs by up to 25.28 % compared to the existing schemes in the literature. So, we conclude that our proposed scheme is most suitable for resource-constrained IoT-based smart home environments. Our proposed lightweight and secure communication protocol addressed the key requirements for secure IoT deployments in smart cities and contributed towards making cities more connected, sustainable, and livable. The limitation of this research work is that it did not focus on energy efficiency.

DECLARATION OF COMPETING INTEREST

We do not have any conflict of interest.

ACKNOWLEDGMENT

The authors would like to thank the Editor-in-Chief, an Editor, and a Reviewers for their valuable reviews.

REFERENCES

[1] Y. B. Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-generation Internet of Things (IoT): Opportunities, challenges, and solutions," *Sensors*, vol. 21, no. 4, p. 1174, Feb. 2021.

[2] D. S. E. Deering and B. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, document RFC 8200, Jul. 2017. [Online]. Available: https://www.rfc-editor.org/info/rfc8200

[3] B. R. Dawadi, D. B. Rawat, S. R. Joshi, P. Manzoni, and M. M. Keitsch, "Migration cost optimization for service provider legacy network migration to software-defined IPv6 network," *Int. J. Netw. Manage.*, vol. 31, no. 4, Jul. 2021, Art. no. e2145.

[4] H. Han, W. Zhai, and J. Zhao, "Smart city enabled by 5G/6G networks: An intelligent hybrid random access scheme," 2021, *arXiv:2101.06421*.

[5] L. C. Thungon, N. Ahmed, S. C. Sahana, and M. I. Hussain, "A lightweight authentication and key exchange mechanism for IPv6 over low-power wireless personal area networks-based Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 5, May 2021, Art. no. e4033.

[6] E. Kim, D. Kaspar, and J. Vasseur, *Design and Application Spaces for IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs)*, document RFC 6568, Apr. 2012. [Online]. Available: https://www.rfc-editor.org/info/rfc6568

[7] B. R. Al-Kaseem, Y. Al-Dunainawi, and H. S. Al-Raweshidy, "End-to-end delay enhancement in 6LoWPAN testbed using programmable network concepts," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3070–3086, Apr. 2019.

[8] Z. Yan, Z. Sun, R. Shi, and M. Zhao, "Smart city and green development: Empirical evidence from the perspective of green technological innovation," *Technolog. Forecasting Social Change*, vol. 191, Jun. 2023, Art. no. 122507.

[9] J. S. Gracias, G. S. Parnell, E. Specking, E. A. Pohl, and R. Buchanan, "Smart cities—A structured literature review," *Smart Cities*, vol. 6, no. 4, pp. 1719–1743, Jul. 2023.

[10] R. Taylor, D. Baron, and D. Schmidt, "The world in 2025–predictions for the next ten years," in *Proc. 10th Int. Microsyst., Packag., Assem. Circuits Technol. Conf. (IMPACT)*, Oct. 2015, pp. 192–195.

[11] S. U. Jan, I. A. Abbasi, and M. A. Alqarni, "LMAS-SHS: A lightweight mutual authentication scheme for smart home surveillance," *IEEE Access*, vol. 10, pp. 52791–52803, 2022.

[12] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: Challenges, issues and solutions at different IoT layers," *J. Supercomput.*, vol. 77, no. 12, pp. 14053–14089, Dec. 2021.

[13] B. E. Carpenter and S. Jiang, *Transmission and Processing of IPv6 Extension Headers*, document RFC 7045, Dec. 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc7045

[14] Z. Ashraf, A. Sohail, S. Latif, A. Hameed, and M. Yousaf, "Challenges and mitigation strategies for transition from IPv4 network to virtualized next-generation IPv6 network," *Int. Arab J. Inf. Technol.*, vol. 20, no. 1, pp. 78–91, 2023.

[15] S. A. Abdullah and A. A. Al Ashoor, "IPv6 security issues: A systematic review following PRISMA guidelines," *Baghdad Sci. J.*, vol. 19, no. 6, p. 1430, Dec. 2022.

[16] R. Sharma and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 11, Nov. 2023, Art. no. e4571.

[17] S. Saini, A. Chauhan, G. Thakur, and L. Sapra, "Challenges and opportunities in secure smart cities for enhancing the security and privacy," in *Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities*. Springer, 2023, pp. 1–27.

[18] M. Tabassum, A. H. Sarower, A. Esha, and M. M. Hassan, "An enhancement of kerberos using biometric template and steganography," in *Proc. Int. Conf. Cyber Secur. Comput. Sci.*, Dhaka, Bangladesh, Feb. 2020, pp. 116–127.

[19] Y. Chen, H. Wen, H. Song, S. Chen, F. Xie, Q. Yang, and L. Hu, "Lightweight one-time password authentication scheme based on radio-frequency fingerprinting," *IET Commun.*, vol. 12, no. 12, pp. 1477–1484, Jul. 2018.

[20] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for Internet of Things," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100160.

[21] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102787.

[22] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Comput. Secur.*, vol. 86, pp. 132–146, Sep. 2019.

[23] Z. Ashraf, A. Sohail, and M. Yousaf, "Lightweight and authentic symmetric session key cryptosystem for client–server mobile communication," *J. Supercomput.*, vol. 79, no. 14, pp. 16181–16205, Sep. 2023.

[24] Z. Ashraf, A. Sohail, and M. Yousaf, "Robust and lightweight symmetric key exchange algorithm for next-generation IoE," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100703.

[25] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," *IEEE Sensors Lett.*, vol. 3, no. 4, pp. 1–4, Apr. 2019.

[26] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," *J. Inf. Secur. Appl.*, vol. 45, pp. 156–175, Apr. 2019.

[27] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[28] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood, S. A. Chaudhry, and Y. B. Zikria, "A secure and lightweight authentication scheme for next generation IoT infrastructure," *Comput. Commun.*, vol. 165, pp. 85–96, Jan. 2021.

[29] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes," *Sensors*, vol. 21, no. 4, p. 1488, Feb. 2021.

[30] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, and Y. Park, "An efficient, anonymous and robust authentication scheme for smart home environments," *Sensors*, vol. 20, no. 4, p. 1215, Feb. 2020.

[31] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "An IoT-based smart home automation system," *Sensors*, vol. 21, no. 11, p. 3784, May 2021.

[32] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100158.

[33] B. A. Alzahrani, A. Barnawi, A. Albarakati, A. Irshad, M. A. Khan, and S. A. Chaudhry, "SKIA-SH: A symmetric key-based improved lightweight authentication scheme for smart homes," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Feb. 2022.

[34] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "LAKE-6SH: Lightweight user authenticated key exchange for 6LoWPAN-based smart homes," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2578–2591, Feb. 2022.

[35] O. Taiwo and A. E. Ezugwu, "Internet of Things-based intelligent smart home control system," *Secur. Commun. Netw.*, vol. 2021, pp. 1–17, Sep. 2021.

[36] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[37] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102468.

[38] T. Lawrence, F. Li, I. Ali, M. Y. Kpiebaareh, C. R. Haruna, and T. Christopher, "An HMAC-based authentication scheme for network coding with support for error correction and rogue node identification," *J. Syst. Archit.*, vol. 116, Jun. 2021, Art. no. 102051.

[39] S. Frankel and S. G. Kelly, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 With IPsec*, document RFC 4868, May 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc4868

[40] G. Kaur, K. Singh, and H. S. Gill, "Chaos-based joint speech encryption scheme using SHA-1," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 10927–10947, Mar. 2021.

[41] *Span: Security Protocol Animator for AVISPA*. Thomas Genet. Accessed: May 30, 2023. [Online]. Available: http://people.irisa.fr/Thomas.Genet/span/

[42] *AVISPA Code and Simulation Results*. GitHub. Accessed: Nov. 20, 2023. [Online]. Available: http://https://github.com/zashraf-sudo/researchpaper-5-code

ZEESHAN ASHRAF received the MSCS degree with a specialization in computer networks from UMT, Lahore, Pakistan. He is currently pursuing the Ph.D. degree in computer science with IQRA University, Islamabad Campus, Islamabad, Pakistan.

He is also a Permanent Faculty Member with the Computer Science Department, The University of Chenab, Gujrat, Pakistan. He has more than 15 years of experience in the IT field. He is CISCO CCNP (R&S) certified. He is the author of several books. His several research articles have been published in well-reputed international journals having good impact factors and conferences. His research interests include next-generation virtualized internet architecture, IPv6 routing, the IoT, performance modeling, optimization techniques, and security services in different networks. He is a reviewer of several journals.

ADNAN SOHAIL received the master's degree in computer science from Bahria University, Islamabad, Pakistan, and the Ph.D. degree in electrical engineering and information technology from the Institute of Telecommunications, Vienna University of Technology, Vienna, Austria.

During the Ph.D. studies, his research focus was on performance modeling and evaluation of network access nodes. He is currently an Associate Professor with the Computing and Technology Department, IQRA University, Islamabad Campus, Islamabad. He is also an Assistant Professor with CUI and IIUI, Pakistan. His research interests include performance modeling and analysis of communication networks, optimization techniques, and quality of service of communication networks.

ABDUL HAMEED received the Ph.D. degree in video quality assessment from North Dakota State University, USA.

He is currently an Associate Professor with the Software Engineering Department, IQRA University, Islamabad Campus, Islamabad, Pakistan. He completed many research projects. His research interests include video quality assessment, quality of experience, quality of service, encoding and decoding of the video bitstream, algorithm design and development, data mining, machine learning, and software development.

MUHAMMAD FARHAN received the BSCS degree from the Virtual University of Pakistan (VU), in 2007, the MSCS degree from the University of Management and Technology (UMT), Pakistan, in 2010, and the Ph.D. degree in computer science from the Department of Computer Sciences and Engineering, University of Engineering and Technology (UET), Pakistan, in 2017.

He was an Instructor of computer science with VU, for about five years. He was a Lecturer with the Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Pakistan, where he is currently an Assistant Professor. He has published a good number of SCI-indexed impact factor journal articles, which are published by the *Journal of Real-Time Image Processing* (Springer), *Multimedia Tools and Applications* (Springer), *International Journal of Distributed Sensor Networks* (SAGE Journals), *EURASIA Journal of Mathematics, Science and Technology Education* (Modestum), and *Life Science journal* (Marshland Press), and in various renowned journals of IEEE, Springer, Elsevier, and Hindawi. His research interests include data science, machine and deep learning, and the Internet of Things.

FAIZ ABDULLAH ALOTAIBI is currently an Assistant Professor with the Department of Information science, College of Humanities and Social Sciences, King Saud University, Saudi Arabia. He has been the Head of the Saudi Library and Information Society, since 2022. His research interests include information system management and technology, organization and classification of information, electronic archiving, and artificial intelligence.

MRIM M. ALNFIAI is currently an Associate Professor of information technology with Taif University, Saudi Arabia. She publishes several papers at assistive technology, HCI, and accessibility conferences, including ASSETS, ANT, *FNC*, CIST, *JAIHC*, and ICCA. She has published several papers related to accessibility and authentication mechanisms for visually impaired users. She has also published papers related to using NFC technology and machine learning to enhance the healthcare system. Her research interests include assistive technology, human–computer interaction, accessibility, usable security, machine learning, and designing accessible tools for visually impaired people, including people with no or low vision. She has conducted several studies and experiences to understand visually impaired abilities and behaviors and design accessible systems that help them interact easily with technology.