cryptography

MDPI

Article

Light Weight Authentication Scheme for Smart Home IoT Devices

Vipin Kumar [1], Navneet Malik [1], Jimmy Singla [1], N. Z. Jhanjhi [2,*], Fathi Amsaad [3] and Abdul Razaque [4]

[1] Department of Computer Science and Engineering, Lovely Professional University, Phagwara 144001, India; vipin.17730@lpu.co.in (V.K.); subhash.14335@lpu.co.in (N.M.); jimmy.21733@lpu.co.in (J.S.)
[2] School of Computer Science, Taylor's University, Subang Jaya 47500, Malaysia
[3] Department of Computer Science and Engineering, Wright State University, 3640 Colonel Glenn Hwy, Dayton, OH 45435-0001, USA; fathi.amsaad@wright.edu
[4] Department of Computer Engineering, International Information Technology University, Almaty 050000, Kazakhstan; a.razaque@edu.iitu.kz
* Correspondence: noorzaman.jhanjhi@taylors.edu.my

Abstract: In today's world, the use of computer networks is everywhere, and to access the home network we use the Internet. IoT networks are the new range of these networks in which we try to connect different home appliances and try to give commands from a remote place. Access to any device over an insecure network invites various types of attacks. User authentication can be performed using some password or biometric technique. However, when it comes to authenticating a device, it becomes challenging to maintain data security over a secure network such as the Internet. Many encryptions and decryption algorithms assert confidentiality, and hash code or message authentication code MAC is used for authentication. Traditional cryptographic security methods are expensive in terms of computational resources such as memory, processing capacity, and power consumption. They are incompatible with the Internet of Things devices that have limited resources. Although automatic Device-to-Device communication enables new potential applications, the limited resources of the networks' machines and devices impose various constraints. This paper proposes a home device authentication scheme when these are accessed from a remote place. An authentication device is used for the home network and controller device to control home appliances. Our scheme can prevent various attacks such as replay attacks, server spoofing, and man-in-the-middle attack. The proposed scheme maintains the confidentiality and authenticity of the user and devices in the network. At the same time, we check the system in a simulated environment, and the results show that the network's performance does not degrade much in terms of delay, throughput, and energy consumed.

Keywords: authentication; confidentiality; internet of things; cryptography; security

Citation: Kumar, V.; Malik, N.; Singla, J.; Jhanjhi, N.Z.; Amsaad, F.; Razaque, A. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography* **2022**, *6*, 37. https://doi.org/10.3390/cryptography6030037

Academic Editors: Cheng-Chi Lee, Mehdi Gheisari, Mohammad Javad Shayegan, Milad Taleby Ahvanooey and Yang Liu

Received: 26 May 2022
Accepted: 8 July 2022
Published: 20 July 2022

1. Introduction

In today's world, the use of the Internet is everywhere. It has become an integral part of our lives. A computer network is the basis of digital communication. There are many problems related to network security and cyber security. Whereas network security concerns the protection of essential network software and hardware, cyber security's primary concern is the security of websites and servers and data transfer between communicating parties. Two predominant concerns are confidentiality and authenticity. Confidentiality makes sure that data traveling between the devices over the network is not disclosed and seen by untrusted parties. Authenticity verifies the origin of the data. In today's computer network communication, authenticating the users is very important, as different types of attacks are on the user's privacy, such as security concerns. Using network services is also essential, as some paid services require proper authentication of the user [1]. There are many cryptographic techniques to achieve confidentiality and authenticity in computer

network and website security. Message digests, encryption, and decryption are used for these purposes [2]. In the cyber world, there are different types of communication between clients and servers, and authentication is the process of verifying two communication parties. There are different types of communication, such as client to server or peer to peer [3].

It is vital to protect the physical and logical barriers between the data, software, services, and the rest of the world. This is one of the parts of a multi-layered data protection technique known as defense-in-depth [4]. The Internet has altered our reality by becoming a global means of communication; it has transformed communication to the point where we now use it as our primary way of communication. The Internet of Things (IoT) has forced new research to secure these IoT devices and to use conventional classical cryptography to protect data exchanges by applying mathematical approaches to minimize assaults, such as eavesdropper attacks [5].

Machine authentication is beneficial since it confirms that the device connecting to the network is a simple corporate device. In today's society, it is likely to be a laptop connected to a wireless or wired network. Person authentication is the process of a user authenticating themselves to the network. Authentication, such as machine authentication, may be performedvia certificates or credentials. The user certificate is usually downloaded to the computer when a user registers for the first time.

On the other hand, machine authentication falls short when users share computers [6]. You cannot apply multiple privileges, such as VLANs, based on who is using the computer since only the machine is authenticated, not the user. Here is a terrible example: a student at a school logs onto a teacher's computer. Because the device is shared, students and teachers might share the same network. If a teacher previously used the computer, the student now has access to the instructor's network, which is rarely good [7].

1.1. Attacks on IoT and Computer Networks

In some networks, authentication servers are installed and perform multi-factor authentication by checking some questions, such as who you are, what you have, who you know, where you are, and what you do? A third-party authentication server can be expensive or inexpensive. However, some vulnerabilities exist in the system, and the following are the common attacks on computer networks [8].

1. Distributed Denial of Service (DDoS) attacks. This attack is fired by an attacker by sending bulk requests to busy the server so that it is not available to legitimate users. Attackers send fake bulk requests from different computers, so the server is busy processing that and real users are not allowed to use the services. The attack is due to user authentication and can be prevented by challenging users, such as captcha [9].
2. Man-in-the-Middle attacks. An attacker intercepts the communication and transmits an altered message to the receiver in this attack. The attacker receives the receiver's message and sends a modified message to the sender in a man-in-the-middle attack. Both the sender and the recipient believe they are communicating with one another. In this case, either eavesdropping or mimicking one of the participants creates the illusion of a continuous flow of information.
3. Code and SQL injection attacks. SQL injection, often known as SQLI, is a frequent attack vector in which malicious SQL code alters backend databases and gains information that should not be displayed. A user can gain access to illegal data by sharing facial information. A SQL server provides all results if the condition is proper. A user can build an always-true query condition and choose unpermitted data. This information might range from sensitive corporation information to usage lists to private customer information.
4. Privilege escalation. A privilege escalation assault occurs when a person acquires illegal access to greater levels of rights or privileges than they are supposed to have. This attack's perpetrators might be an external threat actor or an insider. A critical

stage in the cyberattack chain is to exploit a privilege escalation vulnerability, such as a system flaw, misconfiguration, or insufficient access controls [10].

5. Insider threats. An insider threat is a risky insider attack on a company that comes from within the organization. Examples include employees, former employees, contractors, or business partners who have inside knowledge of the company's security procedures, information, and computer systems. An insider attack poses a greater threat than an external attack. Anyone who has the right to access system resources is vulnerable to attacks. For instance, a person might harbor animosity toward a former employer or a dishonest worker who gives away trade secrets to a rival. In comparison to other attackers, turn cloaks have an advantage because they are knowledgeable about a company's security policies, procedures, and weaknesses. Inside intruders can exploit the access provided because they are more knowledgeable about the system.
6. Wireless security: It becomes very difficult to secure a wireless network as the medium is the air, and data are transferred using a low-frequency radio channel. Anybody can attach to the access point using an appropriate device as access points are sending signals in every direction. Managing the access of these devices must be carefully designed, and admins have to authenticate every user accessing the network. Wireless security authentication can be local authentication if a third-party server is not used due to privacy or the admin does not believe a third-party device.
7. Unauthorized access. A security breach occurs when an attacker gains access to a network without obtaining authorization. A physical attack may be on a network where a person compromises the node and accesses all the data, such as key and key generation functions stored on the node. Some of the attacks on the networks are eavesdropping, privilege escalation attack, and brute-force attack.

1.2. Authentication Techniques and Protocol for Networks

1. RADIUS: Remote Authentication Dial-in Service is a centralized authentication for users on different networking devices and server authentication Remote VPN access 802.1X network access. This service provider also authenticates machines. Machine-to-machine authentication is very venerable as some external software can be set in the device. The service is available on almost any operating server. By activating this service, a network administrator authenticates users on the devices that are connected to the system [11].
2. TACAC + S: Terminal access controller access control system is a networking authentication scheme that provides user authentication for devices with centralized authentication and permission management. This system is a scheme for new users from remote-place connections with any UNIX server. Allow/deny methods with authentication keys that match users' and TACACS users' passwords. A new version of TACACS, TACACS+, released in 1993, is an authentication method for network devices.
3. LDAP (lightweight directory access protocol): It contains information about user devices. It uses the active Windows directory or Apple directory. The lightweight directory access protocol (LDAP) is an open-source standard application protocol that allows users to access and manage dispersed directory information services through an Internet Protocol network. Because LDAP is a protocol, it does not affect how directory applications work [12]. This protocol stores user information and grants access to just those users who have registered with the system. Instead, it is a type of language that enables consumers to discover the information they require. Because LDAP is vendor-neutral, it may be utilized with many directory applications. A directory usually contains the following types of information. Descriptive; an asset is defined by several factors, including its name and location. Static; the data does not change frequently, and the changes are minor. It is valuable; data in the directory are crucial to fundamental business processes and are often accessed. LDAP is sometimes

used in conjunction with other systems throughout the workday. Employees may use LDAP to connect to printers or check credentials [13].

4. Network authentication protocol (Kerberos): Kerberos is the authentication protocol for internal networks. In this protocol, there are two servers used. One is the authentication server, AS, and one is the ticket granted server, TGT. A user that wants access to any service in the network should authenticate itself to AS and generate a ticket to access the services. This protocol prevents on-path or replay attacks. This is integrated on Window 2000 and some other operating systems [14].
5. SSO with Kerberos: Used to authenticate cloud services as well. When it comes to implementing security in a wireless network, key distribution is one of the most common issues [15]. If every node has the same key and one of them is compromised or evil, the key for the whole network will be exposed. If each node has a separate key, it will be exceedingly difficult to maintain all of the keys due to the many devices. In the case of the pool key distribution, if each node has a limited number of keys, the network connection will suffer. If each node is given a more significant number of keys, network resiliency will suffer. The benefit of public-key cryptography is that it generally has many resources in demand. The multi-path random essential pre-distribution approach cannot fully protect the system. The Kerberos network can authenticate LDAP.
6. IEEE 802.1x: Based on hardware port network access control protocol. It works as a physical layer and a data link layer. This protocol standard is used in conjunction with an access database portal. It is also used in VPNs as the constrictor can talk to the RADIUS server. This authentication scheme makes the access of systems standardized, and any CISCO device can support it with tacacs+.
7. EAP: extensible authentication protocol integrated with IEEE 802.1x. To prevent access to a network from authenticating access, this protocol is used. This protocol is very strong and uses DES. The newer version of it uses the AES. It also uses MD5 and SHA-1 for authentication. It also includes the IEEE802.1 standard protocol. It is used in LAN device authentication. IEEE 802.1X describes the extensible authentication protocol (EAP) encapsulation over IEEE 802.11, sometimes known as "EAP over LAN" or EAPOL. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

1.3. Security Challenges in IoT

Implementing Internet of Things-based solutions is challenging because of a lack of standard security and privacy protections, expensive sensor costs, and short battery life. Although Internet of Things-based solutions are being adopted at a low rate, further research is needed to understand why IoT solutions are being used in limited numbers in other industries. There are many difficulties related to the Internet of Things, which are as follows.

1. Privacy and Security: Privacy is the leading cause of concern and difficulty for any technological development in today's society, which is especially true for social media. When there is a public website thathas many connected users, it is very necessary to maintain privacy. To attack the system, a variety of techniques are possible. These include restricting network availability, providing misleading information to networks, and obtaining personal information. It is impossible to enforce a proper privacy and security system using the now available technologies. Because the Internet of Things uses a variety of item identification technologies, such as RFID and 2D barcodes, it must offer adequate privacy protections and prevent unwanted access [16].
2. Data Storage and Intelligence: Cleaning, analyzing, and understanding the massive amounts of data collected by sensors is another difficulty in developing IoT applications. To create smart IoT applications, the data gathered by IoT devices must be appropriately maintained and utilized. To accomplish automated decision-making, IoT can be used for data collection and analysis. Wireless Sensor Networks are being

investigated as a method for data analysis. These networks exchange data between sensor nodes, which are then sent to a distributed system to analyze the sensory data collected [17].

3. Quality of Service: Throughput and bandwidth are the two most important factors that influence the quality of service (QoS) of IoT applications. Data generated by the Internet of Things (IoT) ranges from sensors linked to machine components or environmental monitors to the words we shout at our smart speakers in enormous numbers. Because of restrictions in resource allocation and management capabilities in shared wireless media, the devices will need a specific frequency in order to transmit data across the wireless medium. Another major research subject in cloud computing is quality of service, which will become more essential as the data and tools required for the Internet of Things become more readily available on the cloud [18].
4. Interoperability and Standardization: There is a lack of interoperability, platform fragmentation, and widely accepted technological standards in the IoT networks. While developing apps that will work consistently across diverse technical ecosystems, it is critical to consider the broad range of Internet of Things devices accessible, both in hardware variances and changes in the software that runs on them. Given the fact that there will be a plethora of device makers in the future, technologies and services that are accessible for one device may become unavailable for other devices within the same period of time. Consequently, the standardization of all network objects and sensor devices is essential to improve interoperability [19].
5. Object's safety and security: It is difficult and potentially dangerous for attackers to access the Internet of Things due to the enormous number of perceptual objects spread across a vast deployment area. The things may be rendered unusable or physically damaged if the attackers get access to the goods.

1.4. Research Contributions

The following is the most significant contribution made by this study:

- Introduction of a generalized authentication method for low-power IoT devices to improve security in remote access scenarios.
- We investigate the most common authentication methods for low-power devices and discover the drawbacks of the available authentication methods.
- The proposed scheme explains the detailed working of the proposed authentication scheme for low-power devices and analyzes the performance.

1.5. Organization of the Paper

After the relevant research introduction in the area of IoT device authentication, Section 2 discusses the existing device authentication schemes available for IoT networks. Section 3 contains an explanation of our proposed system, and in Section 4, we give the security analysis and performance of the suggested scheme. Finally, in Section 5, we bring this paper to a close by providing a conclusion as well as future research opportunities.

2. Related Work

For the low-energy device, it is very difficult to implement security. All the access to the device or the network is through the Internet, so it is necessary to authenticate the user and maintain confidentiality. Different types of encryption-decryption algorithms are used in cryptography. Secret keys are used in these encryption-decryption algorithms. These secret keys are only shared between communication parties. The process of distributing and maintaining these keys is known as key management. It is difficult to create a single key scheme that can be used for networks with varying topologies. Many key sensor network management techniques that meet the majority of the requirements have been developed. In addition to other security concerns, key management should consider the sensor node's limited energy and processing. As a result, any approach should be as light in terms of storage and processing as feasible. It should not concentrate all of its efforts on

the first setup. In [20], the SPINS protocol, suggested by the author. was one of the first protocols for low-energy devices' security. In this approach, the base station serves as the key distribution center, or KDC, and two nodes can use the KDC to create a pairwise key.

The scheme discussed in [21] works in a client–server way. When the device wants to connect to the server, it requests and sends a challenge the device has to solve and send to the server. Another technique for server authentication given in [22] is a space-time authentication technique and a location-based technique that employs a GPS to determine the position. The second approach uses IQRF, unique communication technology for position determination.

In [23], the author proposed a technique based on data analysis, and this scheme takes the advantages of opportunistically leveraging physical layer characteristics and applying intelligence to authentication; new authentication systems based on machine learning algorithms provide more efficient security provisioning. There are other machine learning paradigms available for use with parametric and non-parametric learning algorithms, as well as supervised, unsupervised, and reinforcement learning algorithms.

In 2018, another algorithm was provided in [24], and a secure and efficient multi-factor device authentication scheme was proposed. The proposed concept uses digital signatures and device capabilities to authenticate a device. In the presented technique, a machine will be allowed into the network only if multi-factor authentication has been successfully established; otherwise, the authentication process will fail, and the entire authentication procedure will be redone.

Another technique is given in [25] based on human biometrics. A per-packet authentication is a research approach in which security mechanisms should be established to ensure the authentication of a specific network flow. User biometrics are used for authentication and fall under the category of "something you have." The author applies biometric techniques to apply per-packet authentication rules in highly dynamic contexts.

In [26], a mutual authentication technique for low-energy devices was given, in which each node in a WSN is assigned a Medium Access Control (MAC) address in order to register with the nearest cluster head (CH) or base station module. Offline registration is used to validate the legitimacy of both lawful nodes and base stations in a live network. The suggested technique eliminates the black-hole attack problem since an invader node must register with both the gateway and its neighbors, which is impossible. To increase the acquired authenticity, confidentiality, and integrity data, a hybrid data encryption strategy, elliptic curve integrated encryption standard (ECIES), and an elliptic curve Diffie–Hellman problem (ECDDHP) are utilized [27].

By studying the different strategies for IoT network security, we discovered that the schemes mostly concentrate on security rather than network performance [28]. The Internet of Things (IoT) is employed in a range of applications, including smart cities, traffic management, ambulance communication, and at home. These gadgets also raise a plethora of security concerns. This is because the industry is young, and manufacturers and sellers are more concerned with features; making devices have a more promising future and a speedier market debut. However, for hackers, this may result in million-dollar breaches [29]. At the moment of conception, security is not a priority. If a hacker compromises a tiny IoT device, the hacker has access to the whole infrastructure, including the sensitivity date. Therefore, there is a need for a lightweight authentication scheme for these low-power devices that also have the same performance level [30].

3. Proposed Scheme

In this section, we explain the proposed scheme and the implementation of the scheme. IoT device manufacturers consider connectivity and performance, but they are unconcerned about the device's security, making the device vulnerable to various attacks. Before accepting any instruction, this technique performs the appropriate authentication of users and provides access control; as a result, it is capable of preventing a significant number of assaults on IoT networks. The proposed scheme has to preserve data transfer security and

provide user authentication. A user can control the home device from anywhere using a mobile or laptop and an Internet connection. A central controller or authentication device is used to control the communication between the user and the device. The controller is the main source that has processing capability for data and transmission. The notations used in the work are shown in Table 1.

Table 1. Notations.

Symbol	Meaning
AD	Authentication Device
CD	Controlling Device
UD	User device
HA	Home Appliances
SK	Session Key
Kp	Private Kay
Ku	Pubic Key
En(K,M)	Message M encrypted with Key K
TS	Time Stamp

Network Model and Adversarial Model: The network model is given in Figure 1. A user wants to operate the home device from a remote location. The user uses the Internet to send a command to the home appliances. The Internet channel may be insecure, and an attacker may impersonate themself as an authenticated user and try to access the home devices.

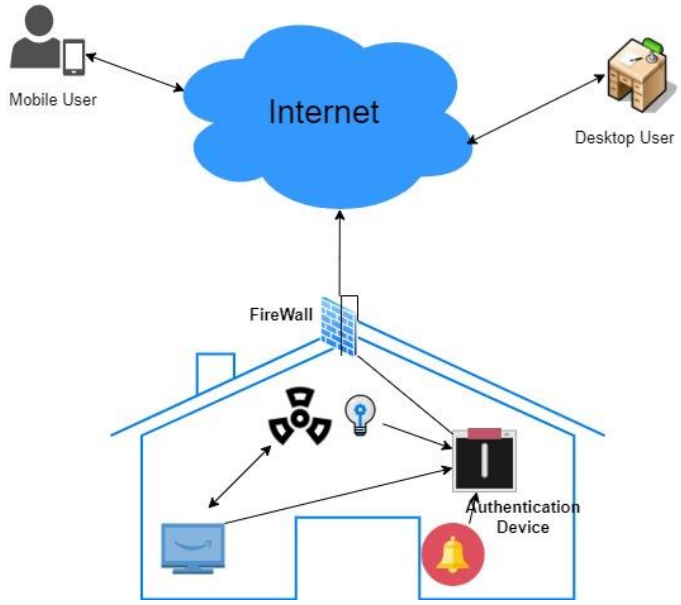
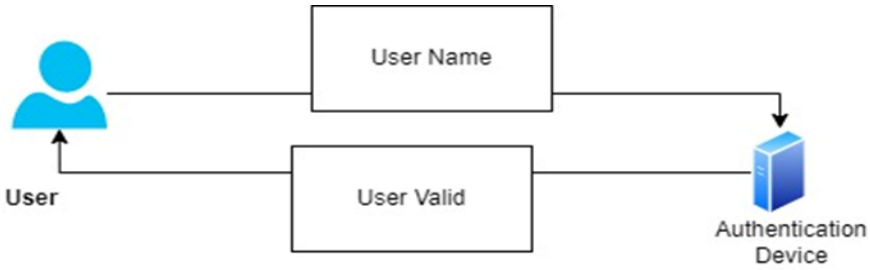


Figure 1. Home IoT Network.

User Registration: The algorithm to authenticate home devices requires that the user device must first have some small software that has a public-private key pair with the authentication device. This step (Scheme 1) is offline and may be considered as the user registration with the authentication device (AD).

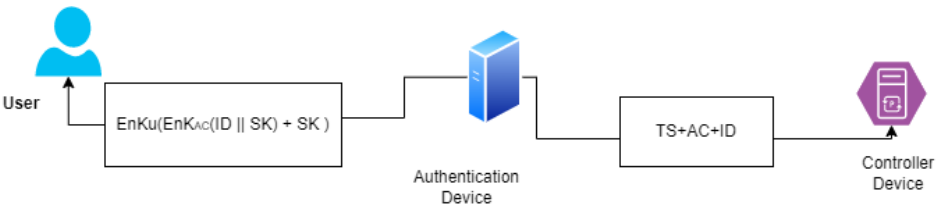


Scheme 1. User Sends the Request to the AD.

The user wants to access appliances in the home. Appliances can be anything, such as a bulb, tube light, fan, AC, fridge, or geyser. A home appliance is represented by HA. There are three parties involved in the communication; theauthentication device, AD; the controller, CD; and the user. Before creating the connection over the Internet, it the user device uses an algorithm to generate the public key with the help of the user's password that can be used by an authentication server as a Public-Key Infrastructure (PKI).

1. The user sends the request to an authenticated device for login. This authentication request is sent using a secure public-key encryption algorithm, such as RSA, and the AD authenticates the user by the public/private key pair shared offline at the time of user registration. It gives the same level of security provided by publickey cryptography.
2. The authenticator device generates a session key and performs the following;
    a. Alice identity and Session Key are encrypted by a symmetric shared key with a controller device called the Authentication Coupon (AC).
    b. The Authentication Device sends the Session key and encrypted AC with the User public key to the user.
    c. The Authentication Device sends the Timestamp, Authentication Coupon, and user Identity to the Controller Device.

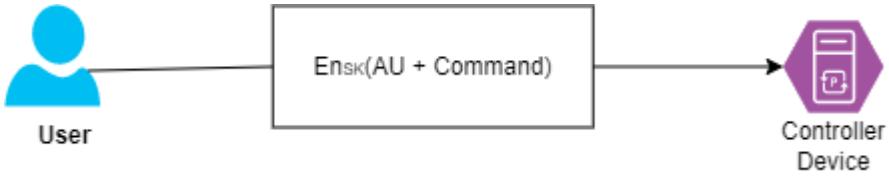
Above mentioned steps are shown in Scheme 2.



Scheme 2. The AD sends the coupon to the user.

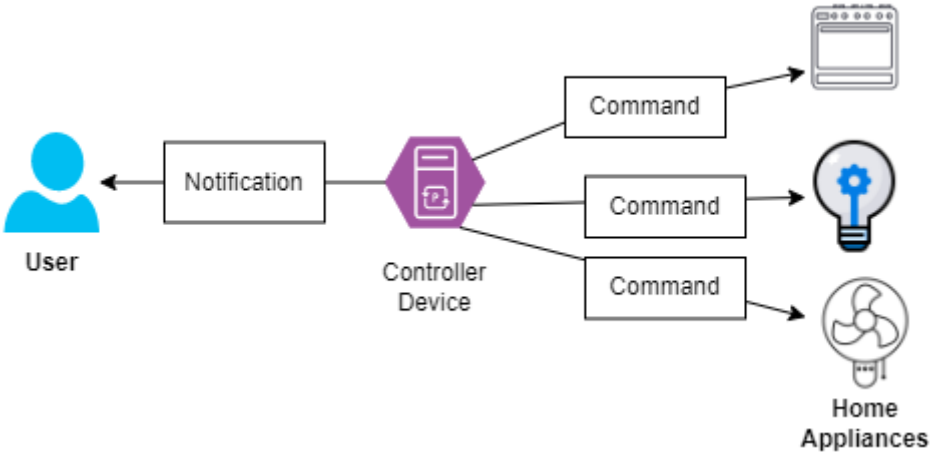
3. The user device requests the controller device to access HA with an Authentication Coupon AC. The controlling device performs the following;
    a. Decrypt the coupon with the shared key of AD and finds the identity of the user.
    b. The Controlling Device already has the AC, user identity, and time of request.
    c. The Controlling Device checks and authenticates the user and sends the command to HA.
    d. The Controller Device adds the entry in the log list record.

Above mentioned steps are shown in Scheme 3.



Scheme 3. User sends the AU and command to the CD.

4. The controller authenticates the user and asks for the command to give to the HA.
5. The user sends the command to the controller.
6. The controller sends the command to the device and sends a notification to the user. All these steps are shown below in Scheme 4.



Scheme 4. CD sends the command to HA.

4. Security and Performance Analysis

The security protocol must have strong user authentication and confidentiality of transmitted data. A security protocol may ensure very strong security in the network, but sometimes, it degrades the network's performance. A security protocol must be attack resistant and should be able to stop and prevent various attacks by an adversary. We analyze the scheme on three different types of parameters [31]. First, it has to have an efficient level of security to effectively offer protection and meet all of the standards for safety. Second, it must prevent all known attacks on the system and should not leave any vulnerability in the system. Third, at the same time, it should not degrade the system's performance. We check that the protocol provides sufficient security, prevents all types of attacks, and gives good performance. The authentication message transitions are shown in Figure 2.

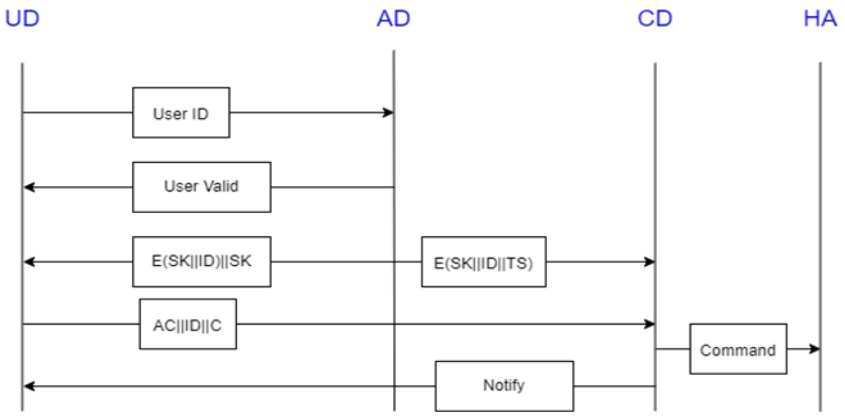


Figure 2. Authentication Message Transitions.

4.1. Security Efficiency and Verification

The security of the scheme only depends on encryption algorithms that are very secure, such as RSA and triple DES. All of the communication is secured between the user and the authenticating server and between the user and the controlling device [32]. We usethe security protocol animator for AVISPA for protocol verification. We implement user authentication to AD and transmissions between the AD and the controller CD. The results are satisfactory, and some of the statics are given in Table 2.

Table 2. Verification Statistics.

Parameter	Output
Parse Time	0.05 s
Search Time	1.2 s
Depth	12
Translation	222 States
Computation	0.45 s
Reachable	234 States

Authentication: Authentication is provided by the method of a public key shared between the authenticating device and the user device. This process must be completed offline, and a secure public key for authentication can be setup between the authentication device and the user's device [27]. For this purpose, no authority certificate is required, as this public key or certificate is never going over any Internet or insecure channel.

Authentication between the user and controlling device is provided by an authentication coupon generated by the authentication device. The information is also sent to the appliance device with a time stamp that stops any replay attack.

Confidentiality: A session key is generated by the authentication device, and all the communication between users or AS and the user and controlling device is secured by this session key. This confidentiality technique uses AES or DES. It is as secure as these algorithms. The encryption algorithm is very secure, and the only problem is sharing the key or the authentication of the public key. All the shared keys are encrypted by the public key, and the public key is authenticated offline and never revealed without physically challenging the authentication device. Therefore, it is as secure as the physical security of the authentication device [33].

4.2. Attacks Resistance

The scheme provides resistance from various known attacks and prevents any adversary from taking advantage of venerability. We analyze the scheme against various attacks and give logical explanations of different attacks. The verification results are shown in Figure 3.

Replay Attack: When an appliance device is accessed by the authenticated user, the controller also stores the information and access used and maintains the log and backup for future use. A request coming to the controller to access the device can only come through the authentication device. The same information is also sent by the authentication device with a time stamp. This time stamp sharing between the AD and CD is used to stop replay attacks. We can use a backup log to analyze the different activities of the user, or Machine Learning can be used to analyze the behavior of the user.

Man-in-the-Middle attack: A man-in-the-middle attack is a form of active wiretapping in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. This process for authentication is started by a key being shared by devices. A password is used to authenticate the user, but we have to also authenticate the devices. Therefore, this communication is started by the user and the used device [34]. The communication between the user and AD on an insecure channel is encrypted by the public key shared between the user and AD. This process is completely offline, so there is no chance of this

key compromization or an authentication problem. All the subsequent keys are encrypted by this public key, and the authentication process is completed, which stops this type of attack.

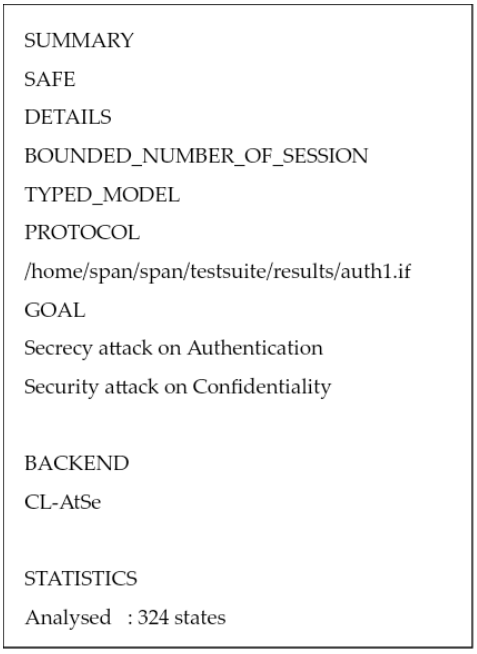


Figure 3. Verification Results.

Masquerade: An attacker may reveal the identity of a legitimate user and claim that I am the person who can access the device. To stop this type of attack, authentication is required, and the whole process is about authentication. The authentication techniques are provided by RSA or MD5 algorithms [35]. Therefore, if the first part of the communication is secure and a public key is securely exchanged and authenticated, it all depends on the algorithm's strangeness.

Server Spoofing: An attacker may divert the traffic from the user to a fake server by server spoofing and getting user information or credentials. Any spoofed server does not know the keys used by the AD, and the scheme is as secure as the physical security of the authentication device. All the data coming from the user is encrypted by the public key of the server and only the AD can decrypt it with the private key.

Offline Password Guessing: The instruction of strong passwords is given by various security agencies, and if a user chooses a strong password, it is difficult to guess. Moreover, it is recommended to change the password at regular intervals. In the proposed scheme, the password is set offline initially at the time of registration and may be extended by choosing another online method of password changing, such as email or OTP verification.

User impersonation: A user is a person who wants to give the commands to the home device, and an attacker may impersonate the user and claim to be an authenticated user. A user can communicate with the AD only if the password is offline resisted by the AD. Therefore, it is not possible for anyone to obtain the user's password, and when it is transferred over the Internet, it is protected by the private–public key of the user's device and the authentication device.

4.3. Simulation and Performance Analysis

The performance of the network depends on various parameters; delay, jitter, bandwidth, and packet drops. After implementing security in any network, the performance of the network may slow down. The security technique must be strong enough to stop the various types of attacks and must not degrade the performance of the networks.

Computation Overhead: The proposed scheme is implemented in NS3 with different cryptographic methods and calculatesthe computation overhead for various communicating devices. A simulation is set up with a User, Authentication Device, and Controlling Device. The user uses a high-energy device, such as a laptop or desktop, so there are no energy and computation limitations for the user. The AD and CD are implemented within 10,000 square meters with a transmission range Tx Range 20DB and initial energy of 1 mJ. Message sizes of 100 to 300 Bytes are sent between entities. We use different encryption methods (AES-128 bit, SHA-1) for different security strengths. The computation overheadsfor different entities are given in Table 3.

Table 3. Computation Overhead.

Cryptographic Scheme	AES	SHA-1
User	0.001975 ms	0.001135 ms
AD	0.003945 ms	0.002135 ms
CD	0.004155 ms	0.002511 ms

Delay in different encryption: Figure 4 depicts the delay in various encryption schemes and key sizes. The proposed scheme is implemented in NS3 with the above parameters to test the delay and packet drop rate. RSA has a high delay and provides high security according to the computation time required for different encryption methods. We found that the network's performance was slowed, but this is insignificant compared to providing security.

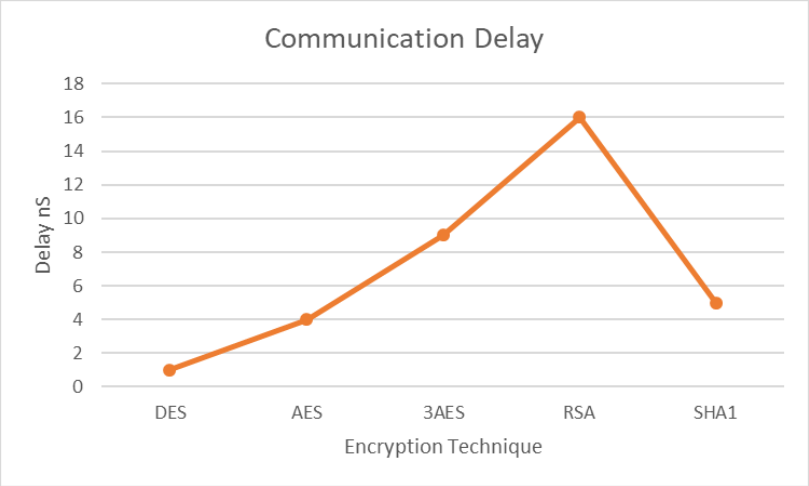


Figure 4. Delay in the Communication.

Storage Overhead and Energy Efficiency: Storage and energy requirements for the scheme are given in the Table 4, and check that less storage is required compared to other existing schemes. The energy requirements for the scheme may be slightly high, but the security provided is high. We run the simulation in various scenarios and check the energy spent with security and without security. A maximum of 1 Mb of memory is required to store the keys, and some is computation required, as shown in the previous table. We separately analyze our proposed scheme on the plate against security attacks and find it robust against various attacks. We check our scheme in the NS3 simulator and calculate and compare storage cost and computation cost. We also check the communication cost.

Table 4. Storage and Energy Requirements.

Device	Message Storage (Bits)	Energy (mJ)
UD	525	0.196
AD	235	0.31
CD	235	0.247
HA	95	0.2116

We implement the scheme and measure energy expenditure for different devices, as shown in Figure 5. The graph in Figure 5 shows the energy consumption with and without security for individual devices. With 1 mJ initial energy maximum energy expenditure in the authentication device, the energy consumption of this scheme is calculated via the average remaining energy in a device and the energy required for encryption and decryption. Insecure methods, a device sends a message after encryption, which consumes more energy than an insecure scheme.

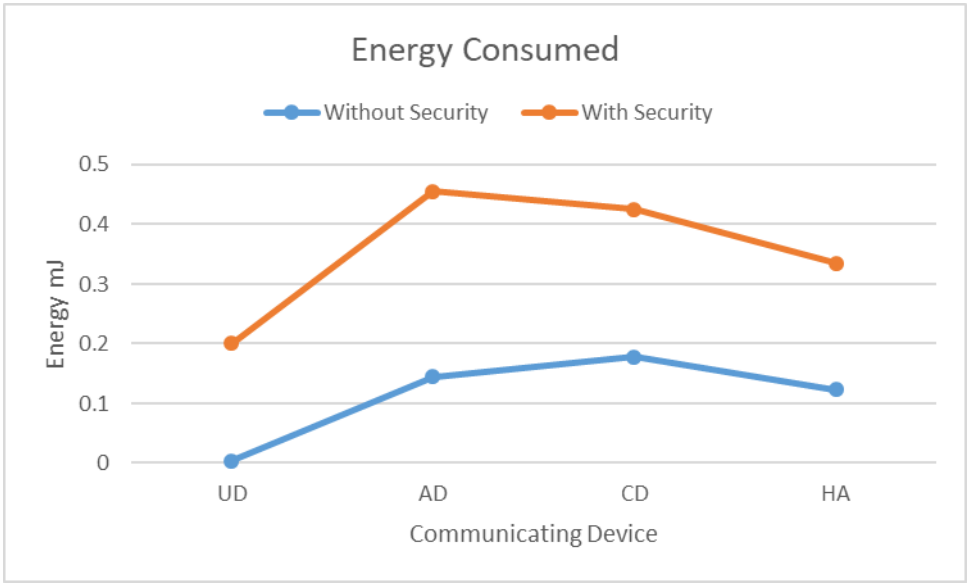


Figure 5. Energy Consumption in Proposed Scheme.

5. Conclusions

Use of the Internet, Wi-Fi, or 5G technology to access different personal devices or cloud storage is very common nowadays [36]. We use the Internet to access our personal devices, office networks, office mail servers, or laptops. Authenticating users is very important to prevent data from getting into the wrong hands. Therefore, various authentication techniques are used to authenticate the user. We develop the authentication technique that mainly relies on asymmetric key cryptography. The scheme is checked against various attacks and gives good results. This scheme can be implemented with IoT networks and works well in a diluted network. We proposed a scheme for home device authentication using public-key cryptography. The scheme is used to send commands to home devices securely. The results show that the proposed scheme is secure, and it prevents many attacks. The authenticating device and controlling device check every step and scheme and also prevents the server spoofing scheme. Biometric authentication enhances authentication, although it necessitates the purchase of additional gear. Authentication technology is continually changing, and as technology advances, companies must consider authentication and passwords to improve the user experience. Because of enhanced authentication procedures and technology, attackers will be unable to exploit passwords, and security may be improved.

Author Contributions: Conceptualization, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Data curation, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Formal analysis, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Funding acquisition, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Investigation, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Methodology, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Resources, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Software, N.M., J.S., N.Z.J. and F.A.; Supervision, N.M. and N.Z.J.; Validation, V.K. and F.A.; Visualization, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Writing—original draft, V.K., N.M., J.S., N.Z.J., F.A. and A.R.; Writing—review & editing, V.K., J.S., N.Z.J., F.A. and A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is available on demand on request through first author.

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

References

1. Zhang, Y.; Xiao, Y.; Ghaboosi, K.; Zhang, J.; Deng, H. A survey of cyber crimesYanping. *Secur. Commun. Netw.* **2012**, *5*, 422–437. [CrossRef]
2. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, pp. 648–651.
3. Wazid, M.; Das, A.K.; Hussain, R.; Succi, G.; Rodrigues, J.J. Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *J. Syst. Arch.* **2019**, *97*, 185–196. [CrossRef]
4. Kizza, J.M. *Guide to Computer Network Security*, 5th ed.; Springer: Berlin/Heidelberg, Germany, 2017; Chapters 2 and 3.
5. Mamun, Q.; Islam, R.; Kaosar, M. Secured Communication Key Establishment for Cluster-Based Wireless Sensor Networks. *Int. J. Wirel. Netw. Broadband Technol.* **2015**, *4*, 29–44. [CrossRef]
6. Schmitt, C.; Noack, M.; Stiller, B. TinyTO: Two-way authentication for constrained devices in the Internet of Things. In *Internet of Things*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 239–258.
7. Anthi, E.; Williams, L.; Slowinska, M.; Theodorakopoulos, G.; Burnap, P. A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 9042–9053. [CrossRef]
8. Zhu, W.T.; Zhou, J.; Deng, R.H.; Bao, F. Detecting node replication attacks in wireless sensor networks: A survey. *J. Netw. Comput. Appl.* **2012**, *35*, 1022–1034. [CrossRef]
9. Ye, J.; Cheng, X.; Zhu, J.; Feng, L.; Song, L. A DDoS Attack Detection Method Based on SVM in Software Defined Network. *Secur. Commun. Netw.* **2018**, *2018*, 9804061. [CrossRef]
10. Hema, B.R.K.; Sangeetha, S.; Bora, R.K.; Rao, K.S. Preference analysis of game theory for network security in WSN. *J. Crit. Rev. Synth. Adv. Sci. Res.* **2020**, *7*, 2637–2642.
11. Smith, R.E. *Authentication: From Passwords to Public Keys*; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 2001.
12. Vithanage, N.N.N.; Thanthrige, S.S.H.; Kapuge, M.C.K.P.; Malwenna, T.H.; Liyanapathirana, C.; Wijekoon, J.L. A Secure Corroboration Protocol for Internet of Things (IoT) Devices Using MQTT Version 5 and LDAP. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 837–841.
13. Cristescu, G.-C.; Croitoru, V. Spoofed Packet Injection Attack-Resistant AAA-RADIUS Solution Based on LDAP and EAP. In Proceedings of the 2021 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 15–16 July 2021; pp. 1–4.
14. Motero, C.D.; Higuera, J.R.B.; Higuera, J.B.; Montalvo, J.A.S.; Gomez, N.G. On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. *IEEE Access* **2021**, *9*, 109289–109319. [CrossRef]
15. Takieldeen, A.; Elkhalik, S.A.; Samra, A.; Mohamed, M.; Khalifa, F. A Robust and Hybrid Cryptosystem for Identity Authentication. *Information* **2021**, *12*, 104. [CrossRef]
16. Porkodi, R.; Bhuvaneswari, V. The internet of things (IOT) applications and communication enabling technology standards: An overview. In Proceedings of the 2014 International Conference on Intelligent Computing Applications, Coimbatore, India, 6–7 March 2014; pp. 324–329.
17. Hong-Tan, L.I.; Cui-hua, K.; Muthu, B.; Sivaparthipan, C.B. Big data and ambient intelligence in IoT-based wireless student health monitoring system. *Aggress. Violent Behav.* **2021**, 101601. [CrossRef]
18. Sodhro, A.H.; Obaidat, M.S.; Abbasi, Q.H.; Pace, P.; Pirbhulal, S.; Fortino, G.; Qaraqe, M. Quality of service optimization in an IoT-driven intelligent transportation system. *IEEE Wirel. Commun.* **2019**, *26*, 10–17. [CrossRef]
19. Hazra, A.; Adhikari, M.; Amgoth, T.; Srirama, S.N. A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions. *ACM Comput. Surv.* **2021**, *55*, 1–35. [CrossRef]
20. Seshadri, A.; Luk, M.; Perrig, A.; van Doorn, L.; Khosla, P. *Using Fire & Ice for Detecting and Recovering Compromised Nodes in Sensor Networks*; School of Computer Science, Carnegie Mellon University: Pittsburgh, PA, USA, 2004.
21. Falk, R.; Fries, S. Advanced Device Authentication Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things. In Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems, Venice, Italy, 9–13 October 2016; pp. 69–74.

22. Jaros, D.; Kuchta, R. New location-based authentication techniques in the access management. In Proceedings of the 2010 6th International Conference on Wireless and Mobile Communications, Chengdu, China, 23–25 September 2010; pp. 426–430.
23. Fang, H.; Wang, X.; Tomasin, S. Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks. *IEEE Wirel. Commun.* **2019**, *26*, 55–61. [CrossRef]
24. Alizai, Z.A.; Tareen, N.F.; Jadoon, I. Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. In Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 4–5 September 2018; pp. 115–119. [CrossRef]
25. Nakouri, I.; Hamdi, M.; Kim, T.-H. Biometric-based Per-Packet Authentication Techniques in Communication Networks. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 273–278.
26. Adil, M.; Khan, R.; Almaiah, M.A.; Al-Zahrani, M.; Zakarya, M.; Amjad, M.S.; Ahmed, R. MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks. *IEEE Access* **2020**, *8*, 44459–44469. [CrossRef]
27. Costello, C. B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, Korea, 6–10 December 2020; pp. 440–463.
28. Tewari, A.; Gupta, B.B. Secure Timestamp-Based Mutual Authentication Protocol for IoT Devices Using RFID Tags. *Int. J. Semantic Web Inf. Syst.* **2020**, *16*, 20–34. [CrossRef]
29. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
30. Aboubakar, M.; Kellil, M.; Roux, P. A review of IoT network management: Current status and perspectives. *J. King Saud Univ. Inf. Sci.* **2021**, *34*, 4163–4176. [CrossRef]
31. Hayashi, V.T.; Arakaki, R.; Ruggiero, W.V. OKIoT: Trade off analysis of smart speaker architecture on open knowledge IoT project. *Internet Things* **2020**, *12*, 100310. [CrossRef]
32. Yin, J.; Zhu, H.; Fei, Y. Formal analysis and automated validation of privacy-preserving AICE protocol in mobile edge computing. *Mob. Networks Appl.* **2021**, *26*, 2258–2271. [CrossRef]
33. Kampova, K.; Lovecek, T.; Rehak, D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *Int. J. Crit. Infrastruct. Prot.* **2020**, *30*, 100376. [CrossRef]
34. Mallik, A. Man-in-the-middle-attack: Understanding in simple words. *Cybersp. J. Pendidik. Teknol. Inf.* **2019**, *2*, 109–134.
35. Jo, H.J.; Kim, J.H.; Choi, H.-Y.; Choi, W.; Lee, D.H.; Lee, I. MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Networks. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2204–2218. [CrossRef]
36. Sathyadevan, S.; Achuthan, K.; Doss, R.; Pan, L. Protean Authentication Scheme—A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments. *IEEE Access* **2019**, *7*, 92419–92435. [CrossRef]