An Enhanced Secure User Authentication and Authorized Scheme for Smart Home Management

Md. Razu Ahmed, Mohammad Osiur Rahman
Dept. of Computer Science & Engineering, University of Chittagong, Chittagong-4331, Bangladesh

***Abstract*—Due to rapid and advanced technology, home automation has gained popularity, making daily life easier. Digitalization and automation have encompassed a wide range of activities and industries. IoT will make home automation more affordable and appealing. With IoT-enabled remote appliance control, smart home automation should improve living standards. A home gateway configures smart, multimedia, and home networks for IoT devices. Safety of life and property is essential to human fulfilment. Automating homes and using related apps have increased the ease, comfort, security, and safety of living in one. Home automation systems have motion detection capabilities and surveillance features to enhance home security. The logic of avoiding excessive or fraudulent notifications remains difficult. Using intelligent response and monitoring mechanisms improves the efficiency of smart home automation. This study introduces a smart home automation system designed to control household devices, monitor environmental conditions, and identify unauthorized entry inside the smart home network and its immediate surrounding area. A smart home network design and configuration that enables secure IoT services with an Access Control List (ACL) for home networks. The research aims to design a robust authentication scheme for guaranteed secure communication in a smart home environment. Implementing a Next Generation Access Control (NGAC) technique serves with Telnet, SSH, IPSec and VPN to detect unauthorized access and mitigate security issues. The efficacy of the suggested design and configuration is validated using a simulation, demonstrating a notable performance in the context of enhanced security measures.**

Keywords—Smart home automation; Internet of Things; security and privacy; ACL; IPSec; VPN

I. Introduction

The fast expansion of the IoT has made us increasingly vulnerable to attacks that exploit vulnerabilities in IoT resources such as data and actuators. The implementation of access control, which delineates the authorization of individuals to access objects under specific conditions, has been acknowledged as a viable approach to tackle this concern. The incidence of home-based criminal activities, such as theft and burglary, has shown an upward trend yearly. Several South African homes were assaulted and robbed despite the lockdown and stay-at-home order [1]. Smart homes are appealing targets for hackers due to user technical ignorance, unsecured IoT devices, insufficient settings, poor control implementation, and high digital asset values. The IoT sector is predicted to reach 48 billion linked devices by 2023 after exponential growth [2]. Every day, hacks exploit these vulnerabilities with substantial potential impact. Gaining unauthorized access to particular gadgets could overhear private conversations within a house [3]. In addition, malicious users get unauthorized access to the control unit of a smart home network to cause serious accidents [4]. Access control, which specifies explicitly or implicitly who (i.e., subjects) can access what resources (i.e., objects) and under what conditions, has been identified as an effective method for preventing unauthorized access [5]. Consequently, our research concentrates on the issue of access control in the IoT. Fig. 1 depicts a sample smart home that uses several services connected via the IoT.

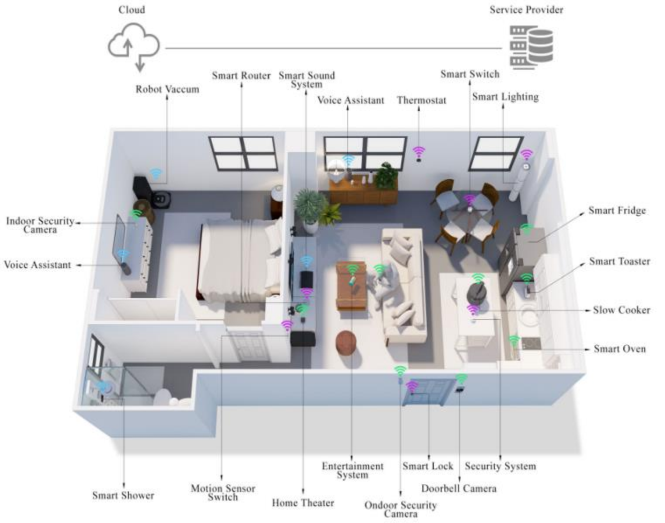


Fig. 1. An overview of a conventional smart home.

The challenges associated with the requirements and limitations of interconnected "things" encompass various aspects. These include the challenge of establishing connectivity for a vast number of devices to communicate with each other effectively. According to a Gartner report, 20% of organizations have experienced at least one IoT attack in the last three years [6]. It is imperative to safeguard these networks from external aggression and being manipulated and utilized as tools for launching attacks, as the Mirai botnet exemplifies [7,8]. Controlling smart devices has become a significant concern as the smart home ecosystem grows. Access control technology in the IoT ensures safe administrative operations over smart home devices to address this issue. It is becoming clear that smart homes should have access control. Smart home terminals and users interact, creating complicated access control system needs that must be carefully considered. According to [9 – 11], smart home systems are usually intended for only a few users and sometimes lack primary access management. According to study [12], Samsung SmartThings offers one permission level for all users and no access control restrictions. Thus, access control needs careful consideration of a complicated design space rather than just designing an interconnected system. Considering user perceptions while solving access control challenges is especially important for a smart home system. This research aims to examine the design of an access control system for IoT Smart Home Systems through the utilization of a user survey.

The main contribution of this research is a proposed and verified Next Generation Access Control (NGAC) list-based smart home security system architecture. Decentralized access control and multi-agent systems underpin the approach.

Create a web-server-based smart home automation system to manage and monitor household appliances and environmental factors.

Implements the proposed system in a simulated secure smart home and assesses its viability in providing specified functionality and features.

The rest of this paper is organized as follows: The problem statements are presented in Section II. Section III discusses the main research background. Section IV discusses the primary security concerns in IoT and the security challenges at each layer of the IoT architecture while Section V provides the proposed system. Section VI provides an implementation of the proposed network design and configuration. Finally, Section VII analyses the research results, and Section VIII concludes with future work on the findings.

II. Problem Statements

Implementing the traditional access control concept in smart homes may need to be more practical. Children should get greater control over IoT devices as they become older. This variety of authority is challenging in access networks, which limit permissions by role and must renegotiate kid roles. Some models assume a single user, whereas the system is used in homes with many family members [13]. In a typical household, parents and children may demand complete gadget control. When guests arrive, wireless routers and TVs must be accessible. Overall, house sharing requires flexible user access management. In such circumstances, distinct user groups need access privileges based on time, location, and other criteria. Therefore, a new access control method must accommodate multi-user, multi-device SHS and changing usage situations [14 – 16].

Another major problem is that SHS apps scarcely imply a fine-grained access control mechanism for end users. The "fine-grained" means the access control system must modify the policy to describe numerous situations. In smart homes, access control rules may be role-based, time-based, location-based, per person, and device [17].

Thus, present access control mechanisms scarcely hint at an end-user-tested system. This project will employ a user study to create an IoT SHS access control system.

III. Research Background

The smart home automation research field has seen remarkable development, creativity, experimentation, and application of its findings. As a result, smart home automation systems can now provide additional services in addition to the standard home management and environmental monitoring functions with technological advancements. Security specialists have conducted substantial studies on the IoT in smart homes, specifically identifying security and privacy issues. In addition, scholars have worked on analyses of IoT frameworks to evaluate the security risks and associated design concerns. Access control is widely recognized as a crucial security feature within the IoT and has garnered substantial attention in academic research [18 – 20].

The utmost priority is ensuring safety and security within residential and commercial premises. Incorporating security and access control systems into a building automation framework offers optimal security measures, enhancing user comfort and lifestyle. Intelligent solutions enable the remote management and control of alarm systems, access control mechanisms, lighting systems, and surveillance cameras through the utilization of mobile devices such as smartphones facilitated by dedicated applications. The proliferation of smart technology is attributed to the need to mitigate the growing threat of burglary and accidents. The demand for remote monitoring and management of home status has emerged as a significant concern due to the prevalent busy lifestyles of individuals [21, 22].

The integration of technology and the level of complexity involved in their respective setups differ, as do the advantages and disadvantages related to intricacy, expenses, performance, and other factors. The IoT is crucial in integrating security mechanisms inside intelligent infrastructures. Traditional security systems typically consist of an activated alarm mechanism that emits a loud sound in response to an unauthorized intrusion. A sophisticated security system serves a broader range of functions beyond its primary purpose. It can promptly notify the owners through an SMS alert on their mobile devices [23].

Additionally, the owners can remotely activate and deactivate the alarm system using a smartphone application. With time, a multitude of technologies have been employed in the development of intelligent security systems. One illustrative instance pertains to Bluetooth-based automation, which exhibits affordability, expeditiousness, and ease of installation [24]. However, it is important to note that this technology is constrained by its restricted range, primarily suitable for short distances. Zigbee is a wireless mesh network standard that has been specifically developed to cater to the needs of low-cost and energy-efficient wireless control and monitoring applications, particularly those involving battery-powered devices. Nevertheless, the technology in question exhibits suboptimal data speed, transmission capacity, and network reliability while incurring a significant maintenance expense [25].

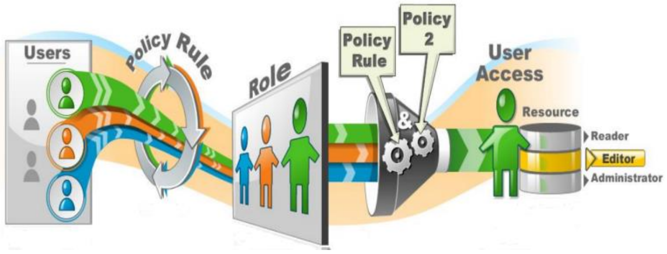


Fig. 2. Access control architecture.

Implementing access control is paramount in facilitating access privileges to both users and devices in the context of network connectivity, including IoT devices. The access control process often encompasses many functions, including authentication, access control, audit, policy management, and administration, as seen in Fig. 2. The authentication function serves the purpose of verifying the identification of a user, process, or device. The access control function is responsible for authorizing or denying particular requests made by a person, process, or device to get access to resources. Access control policies are comprehensive guidelines outlining access management's fundamental criteria and determining authorized individuals who may get information contingent upon certain conditions. The access control process encompasses an administrative function that involves creating, provisioning, and efficient management of various users, groups, roles, devices, and policies. The audit function serves the purpose of conducting an impartial evaluation and analysis of records and activities to evaluate the effectiveness of access control measures and verify adherence to defined policies and operational processes. The process of authorization occurs after the completion of authentication. Authorization is intrinsically linked with authorization policies to ascertain the accessibility of resources or services for a user or device [3, 5, 15, 20, 26].

The IoT technology enables the interconnection and remote monitoring of equipment through the Internet. IoT has become employed in smart homes, telemedicine, industrial settings, and more. IoT-integrated wireless sensor network technologies connect smart devices with sophisticated functions globally. Intelligent home technology relies on a wireless home automation network comprising networked sensors and actuators that share resources. A significant advantage is monitoring and operating home automation systems from various devices—smartwatches, smartphones, tablets, computers, and voice assistants. Home automation systems have many benefits, such as making the house more secure through automated door locks and lighting controls, more awareness through security cameras, and more convenience through the ability to adjust the temperature, saving time, empowering users, and reducing costs. Still, only some people using a home network think about the necessity of proper security measures. To prevent unwanted access to their home gateway, many users still utilize the bare minimum of home network security measures, such as establishing a password that is easy to guess. Developing suitable authorization and authentication systems is crucial in addressing privacy and security concerns in IoT devices with limited resources [27].

TABLE I. EXISTING RESEARCH ON ACCESS CONTROL LIST (ACL)-BASED SMART HOME SECURITY SYSTEMS

Ref.	Key Focus	Methodology	Findings
3	Analyzes various access control models for smart homes, including ACLs, RBAC, and ABAC.	Literature review and analysis	Highlights limitations of ACLs for dynamic and personalized access control in smart homes.
5	Proposes a multi-agent reinforcement learning approach for dynamic access control in smart homes using ACLs.	Simulation and experiments	Demonstrates improved security and scalability compared to static ACLs.
8	Investigates context-aware ACLs for adaptive access control in smart homes based on user behavior and environmental factors.	Prototype development and evaluation	Shows increased security and user convenience with context-aware ACLs.
18	Explores homomorphic encryption to enable secure and privacy-preserving access control in smart homes with ACLs.	Theoretical analysis and prototype demonstration	Offers privacy protection for user and device data while enforcing access control through ACLs.
20	Utilizes federated learning to improve anomaly detection and access control accuracy in smart homes, using ACLs for access enforcement.	Simulation and practical testing	Demonstrates enhanced security and anomaly detection accuracy through federated learning with ACLs.

There is a higher demand for information network confidentiality from small and medium-sized enterprises (SMEs) due to the high cost of professional information security technology and equipment provided by network protection companies. However, by using Access Control lists (ACL) technology as an independent security technology of network security management requirements in terms of design, focus on the router using ACL technology to protect sensitive data. The implementation process involves establishing a central command and determining the specific testing network's requirements. This should lead to a more intuitive and efficient implementation of ACL network protection in SMEs [28 – 31].

We aim to present a robust, unified smart home automation framework utilizing an Access Control List (ACL) setup. Our network setup enables all home network segments to access external networks with our configuration. However, only approved IoT clients can contact the IoT server from the home network or other networks. Simultaneously, the remaining components of the home network, excluding the IoT devices, are systematically safeguarded against both internal and external accessibility.

IV. KEY ISSUES IN SMART HOME SECURITY AND PRIVACY

Authentication is the process of confirming the integrity of data and establishing its origin from the stated sender. Non-repudiation, which refers to the prevention of a sender denying the act of sending a message, is occasionally regarded as a distinct concept. However, we incorporate it within the scope of authentication. Access enables only authorized users to access data, communications infrastructure, and computer resources and does not prevent them. According to the most recent study by the UK Department for Business conducted in 2015, there has been an increase in security breaches. In 2015, 90% of major enterprises and 74% of small firms had cyber intrusions, compared to 81% and an unspecified percentage in 2014. This indicates a year-on-year growth rate of 14%. At the same time as cybersecurity is improving, cybercrime is growing in scope, severity, and sophistication [30, 31]. Automated methods that are both trustworthy and easy to use are essential for smart home network administration so that homeowners may safely control their systems. The risks to privacy and security posed by the Smart Home would certainly exceed its benefits without such technologies.

A. Threats

While the Smart Home presents a unique setting, the general characteristics of security risks are comparable to those seen in other domains. Confidentiality risks refer to situations where sensitive information is unintentionally disclosed. As one illustration, confidentiality breaches in-home monitoring systems can result in the inadvertent disclosure of sensitive medical data. Even seemingly harmless information, like the inside temperature and details about the air conditioning system, might be utilized to ascertain if a residence is now occupied or vacant, leading to a theft. The compromise of confidentiality in items such as keys and passwords will result in the emergence of unauthorized system access risks [4].

Authentication attacks can compromise sensing or control data. Unauthenticated system status signals may trick a house controller into opening doors and windows for an emergency evacuation when they enable unlawful entrance. Later, automatic software upgrades might cause issues if not authorized [5].

The most substantial dangers are those related to access to the system. Unauthorized administrator access to a system controller renders the whole system vulnerable. Using incorrect passwords, crucial management, or unapproved equipment might cause this. Even without oversight, an illegal network connection might steal bandwidth or deny access to legitimate users. Many Smart Home gadgets are battery-operated and wirelessly networked with a limited operational duty cycle; thus, flooding a network with requests may cause energy depletion attacks—denial of service [6].

B. Vulnerabilities

The accessibility of networked systems is a significant risk of vulnerability. Due to their Internet connectivity, current Smart Home systems are susceptible to remote assaults, which may occur by direct access to networked control interfaces or installing malware. The question of physical accessibility to the system is also a concern. Wireless and power-line carrier technologies provide physical access to the networks from outside the home, even if the house is securely closed [11].

The vulnerability at hand pertains to the limitation of system resources. Resource constraints are the following vulnerability. Small 8-bit microcontrollers with low computing and storage capabilities have constrained device controllers' capacity to implement advanced security methods. Various manufacturers' devices have different networking and software update protocols. Devices require more excellent software, operating systems, and security documentation [12].

Another problem is updated firmware. Very few smart home equipment provides frequent software updates to address security flaws. One assumes that there needs to be more motivation to constantly modify software to keep ahead of security risks for low-cost devices. Slow standardization is a weakness. While specific proprietary systems, such as a health monitoring subsystem, may have well-designed standards-compliant security, most existing Smart Home gadgets use few security measures [13]. The most serious risk is a need for more specialized security personnel capable of managing the intricacies of a Smart Home network. Most homeowners need help to afford continuous professional support for managing their home network. Instead, novice homeowners must be able to self-manage their systems safely and securely.

C. Smart Home Elements

The smart home components, sometimes referred to as nodes, are categorized into the following three groups [14]:

Physical nodes include entities or objects capable of interacting with the environment and supplying resources. Examples include sensors, actuators, smart fridges, microwave ovens, light bulbs, cameras, and doorbells.

Application nodes refer to the resources given by physical nodes used to provide consumer services.

Intermediate or intermediary nodes are situated between physical and application nodes. They establish connections across many distinct networks and facilitate data routing, functioning similarly to a bridge or gateway.

As shown in Fig. 3, the application layer consists of application nodes that provide end-user services. The middleware layer consists of intermediate nodes to maintain connectivity and interoperability within the smart home system. The network layer provides communication and data transfer between nodes. Finally, the physical layer consists of smart devices.

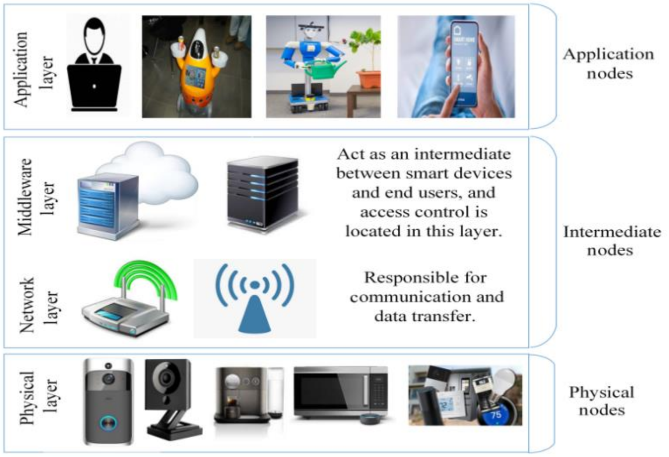

Application layer
Application nodes
Middleware layer
Act as an intermediate between smart devices and end users, and access control is located in this layer.
Intermediate nodes
Network layer
Responsible for communication and data transfer.
Physical layer
Physical nodes

Fig. 3. Architectural model and smart home elements.

V. Proposed System Scheme

This section provides an overview of the specific smart house model that is the main focus of this research work. It also presents a comprehensive explanation of all possible situations that may be encountered in this smart home system (SHS). This SH model is constructed using situations outlined in the literature research. This model exemplifies a smart home system incorporating various users and gadgets, as indicated by individuals in prior research.

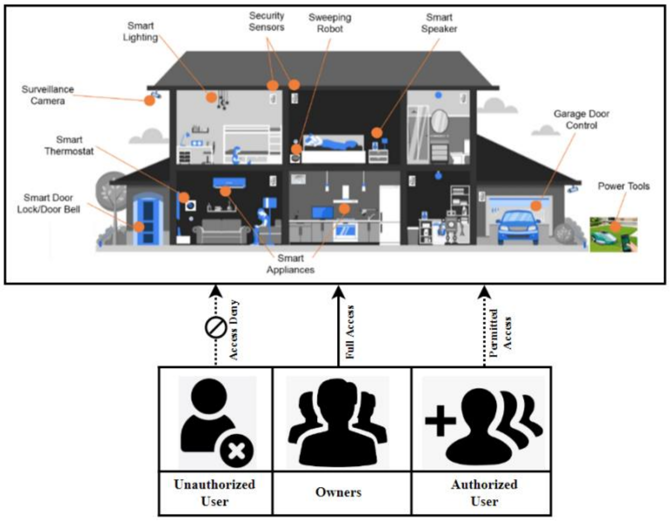


Fig. 4. Proposed model.

Fig. 4 illustrates a prototype of a multi-user smart house fitted with various gadgets. In a multi-user, multi-device smart home system situation, it is often observed that there are typically several users and devices present. Devices located in multiple home regions are assigned distinct degrees of significance. For instance, the living room and guest room are seen to be more easily accessible. Therefore, they possess a comparatively diminished degree of importance compared to those in the bedroom.

There is no universally standardized categorization system for various categories of consumers. This research first examines the individual responsible for overseeing the whole SHS. A genuine social support network encompasses a collective of individuals, including parents, spouses, and partners. The regular user’s category consists of those authorized to use SHS, including roommates, friends, and classmates. Under extraordinary circumstances, some chronic users possess complete mastery of specific technologies.

An illustrative instance is when a child can operate a smart light but is prohibited from using a smart kettle. Based on the user study conducted in an SHS, all participants are considered valid users who need interaction with smart gadgets. Additionally, those who are uninvited or unauthorized are prohibited from accessing the devices.

Attentive users may have noticed that the owner, as described in this research, refers to a collective entity assuming full authority over the SHS. Nevertheless, a joint characterization of an intelligent homeowner in contemporary platforms, particularly in some single-owner systems, is an individual with smart gadgets. Consequently, the presence of a single owner with exclusive administrative control over devices could be more practical within the context of a smart home setting. One of the interview outcomes suggests that some consumers anticipate the presence of numerous owners in smart homes. Therefore, this research considers "owners" to include all intelligent householders. Additional reasons will be shown while implementing user roles in this project. Thus, in the subsequent chapters, the term "the owner" denotes explicitly those who have authority over the SHS rather than the devices themselves. It is essential to mention that the questioned users are all smart homeowners. When referring to interviewed consumers in the following parts, it pertains only to intelligent householders.

Guests must have access to specific household equipment and services. Nevertheless, as per the feedback from the questioned consumers, this access is often transient. Interviews reveal that the duration of smart device use by visitors might vary from a few minutes to several hours or even extend to multiple days. For instance, equipment installers may need a substantial amount of time to get approval for debugging. Another instance may be acquaintances requiring many hours of consent to access entertainment devices and several days of approval to manage utilities, such as lights, in the guest room. The provision of temporary access necessitates the implementation of a time constraint, as recommended by the users interviewed.

Consequently, consumers may be categorized as short-term or temporary users and long-term users, depending on the duration of their use lies in their possession of administrative privileges.

Access to some features of devices in other rooms, such as smart door locks, is restricted to specified individuals only with the owner's permission. Users have also identified geography as a limiting factor. A secondary school is anticipated to limit access depending on the user's location. Non-family members are restricted from accessing devices located outside the home. They can only interact with equipment inside the Smart Home System (SHS) connected to the same Wireless Local Area Network (WLAN).

In conclusion, the owner should possess unrestricted access, while others may have permanent or temporary access. Regarding location restrictions, it is recommended that the owner has both remote and local access. At the same time, other individuals are only able to use the devices while they are physically present in the SHS [7]. Regarding their degree of authorization, it differs across users:

The owner has unequivocal authority over all devices inside this SHS.

Users control just some of the fundamental operations of some appliances, such as the switching functionality. The distinction between users and owners.

In addition, a police officer may sometimes seek temporary authorization to access a smart house's exterior security cameras or door locks. Also, those who are temporarily departing from the city or nation may want remote connectivity to their smart home.

VI. Network Design and Configuration

The proposed framework and configuration with operation are shown in Fig. 5. We aim to create and set up a next-generation access control-based home network framework that is accessible and more secure. In this model, we implement the Telnet and SSH technique with extended ACL for authorized remote access. Also, configure IPSec and VPN secure technique for encrypted data transmitted from server to smart home user. The main focus is on improving security and performance for multimedia applications.

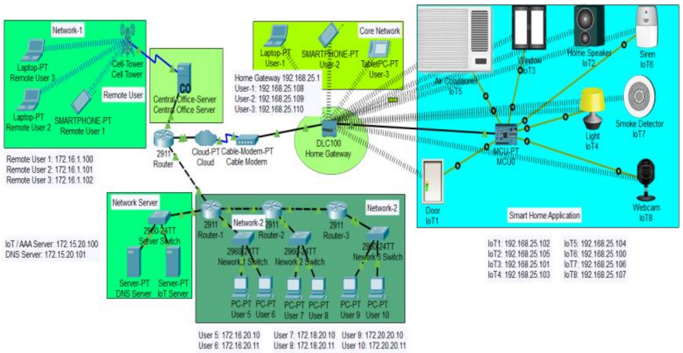


Fig. 5. Experimental setup of the smart home network.

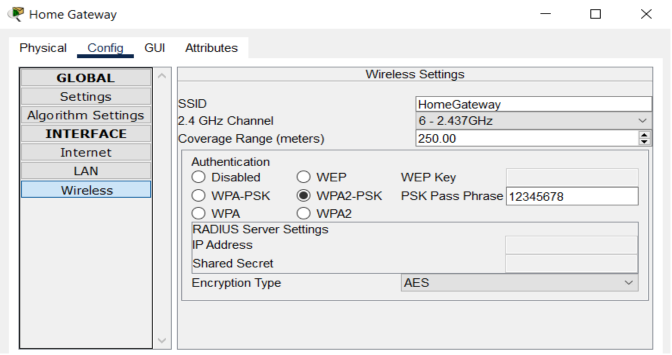
We explain our setup objectives for the given network architecture as follows:

Enables all devices connected to the home network to establish outgoing connections to the Internet.

Enables approved hosts on the Internet to have inbound access to the IoT server.

It prohibits any external hosts from accessing other hosts inside the home network.

The IoT server is restricted from accessing other hosts inside the inner subnet, except for necessary hosts like the IoT devices or the DNS server.



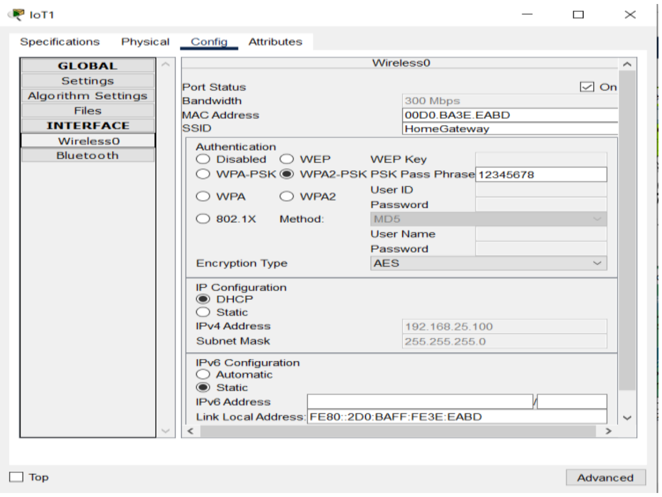
Wireless Settings

SSID: HomeGateway
2.4 GHz Channel: 6 - 2.437GHz
Coverage Range (meters): 250.00

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase 12345678
○ WPA ○ WPA2
RADIUS Server Settings
IP Address
Shared Secret
Encryption Type: AES

Fig. 6. Home gateway setup.

First, we set the home gateway router at a 2.4 GHz wireless channel with a 250-meter range, shown in Fig. 6. Also, set the WPA2-PSK authentication key with AES encryption for secure data transmission. Then, wirelessly connect all IoT-enabled smart devices with the home gateway router and wire through the MCU controller. IoT devices are connected wirelessly using a WPA2-PSK authentication key with a dynamically assigned IP address, shown in Fig. 7. All connected IoT devices with the core home gateway network are shown in Fig. 8. Fig. 9 shows the conditions of IoT devices for automation.



Wireless0

Port Status ☑ On
Bandwidth: 300 Mbps
MAC Address: 00D0.BA3E.EABD
SSID: HomeGateway

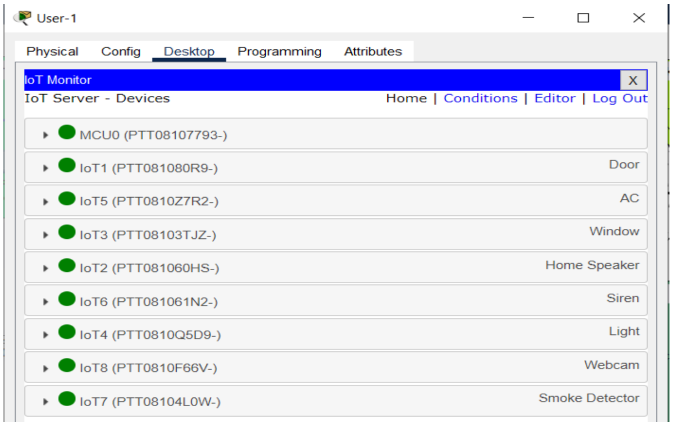
Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase 12345678
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type: AES

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.25.100
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address
Link Local Address: FE80::2D0:BAFF:FE3E:EABD

□ Top

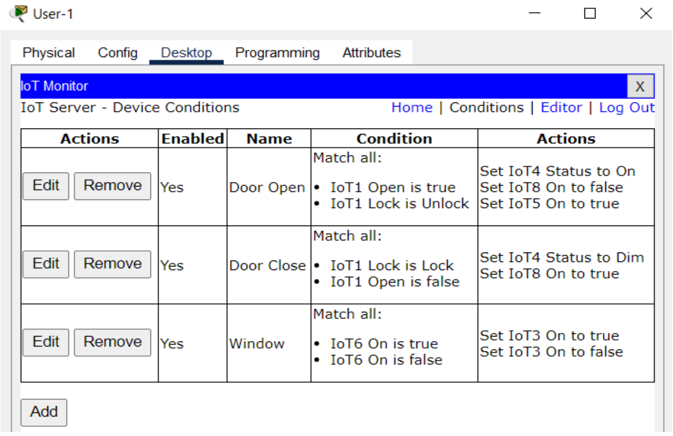
Fig. 7. Assigned IP address.



IoT Server - Devices

MCU0 (PTT08107793-)	
IoT1 (PTT081080R9-)	Door
IoT5 (PTT0810Z7R2-)	AC
IoT3 (PTT08103TJZ-)	Window
IoT2 (PTT081060HS-)	Home Speaker
IoT6 (PTT081061N2-)	Siren
IoT4 (PTT0810Q5D9-)	Light
IoT8 (PTT0810F66V-)	Webcam
IoT7 (PTT08104L0W-)	Smoke Detector

Fig. 8. IoT device wireless connection.



IoT Server - Device Conditions

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Door Open	Match all: • IoT1 Open is true • IoT1 Lock is Unlock	Set IoT4 Status to On Set IoT8 On to false Set IoT5 On to true
Edit Remove	Yes	Door Close	Match all: • IoT1 Lock is Lock • IoT1 Open is false	Set IoT4 Status to Dim Set IoT8 On to true
Edit Remove	Yes	Window	Match all: • IoT6 On is true • IoT6 On is false	Set IoT3 On to true Set IoT3 On to false

Fig. 9. IoT device condition for automation.

A. Configuration

Our proposed network model enables telnet and SSH techniques for remotely accessing the core client-server smart home network. Telnet is a text-oriented network communication protocol that uses a virtual terminal connection and provides clients with a dual peer-to-peer interaction system. Over the Transmission Control Protocol (TCP), client data is interpolated in-band with telnet control information remotely. SSH is a commonly used network protocol for remote access and management of devices. It is the leading web protocol for accessing network hardware and servers. It makes networked computer logins simpler and allows remote command execution. SSH transmission is encrypted, preventing hacking of passwords, trafficking, and snooping.

Internet Protocol Security (IPsec) allows secure communications between devices via IP networks, primarily on the public internet. This network protocol suite provides packet encryption and source authentication. IPsec VPN solutions utilize IPsec to build VPN connections because it protects IP network traffic. IPsec is a security standard that uses strong ciphers, algorithms, TLS authentication, MitM protection, and Perfect Forward Secrecy to secure private network communications, protect web traffic, and ensure IP packet integrity. The IPsec protocols are:

1) Authenticating Headers (AH): It verifies packet origin and integrity, not encrypts. The Authentication Header encapsulates and checks packet integrity using MD5/SHAxxxx before sending data to the destination router. After arrival, the router decapsulates and verifies integrity.

2) Encapsulating Security Protocol (ESP): Packing Security ESPIPsec protocol component ESP maintains payload data integrity and encryption, like the Security Authentication Header. The IP header of the ESP packet is neither encrypted nor protected. Therefore, it may be changed during transit, enabling NAT bypass. Tunnelling is typical ESP.

3) Security Association (SA): The Internet Security Association AND Key Management Protocol ISAKMP formed Security Associations. Two stages are involved.

The initial phase constructs the IKE SA two-way key exchange tunnel. Step 2 creates IPSEC SA channels for secure data transmission after the conversation. Both hosts pre-agreed on this one-way IPsec VPN tunnel's encryption, method, and key.

Phase 2 IPsec VPN tunnels need two IPSEC SAs—IN and OUT. Most ISAKMP settings are manual (PSK, IKEv1, IKEv2) or dynamic (IKEv2).

Based on the provided network architecture, our configuration criterions are outlined below:

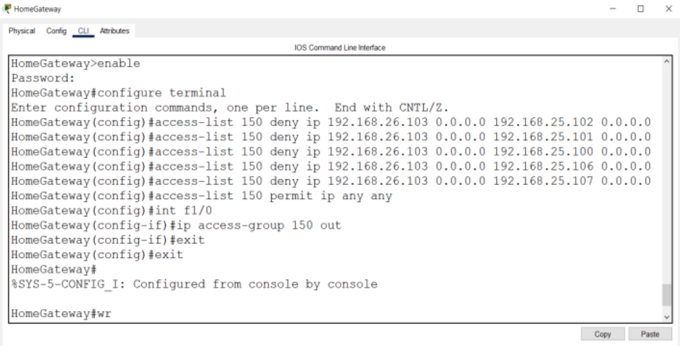
Criterion 1: Allow all in-house all users access to the smart home network, and user 3 allows for partial control of some home devices except users 1 and 2.

Criterion 2: Only authorized users can access the smart home network and IoT server through Telnet and SSH with extended inbound access control.

Criterion 3: Configure IPsec and VPN to secure data with an encrypted connection between the user and the smart home device over a public network.

VII. Result

We have implemented an extended ACL policy to the home gateway router internal interface FastEthernet 1/0 to manage internal network access as per criterion 1. The ACL configuration policy is presented in Fig. 10.

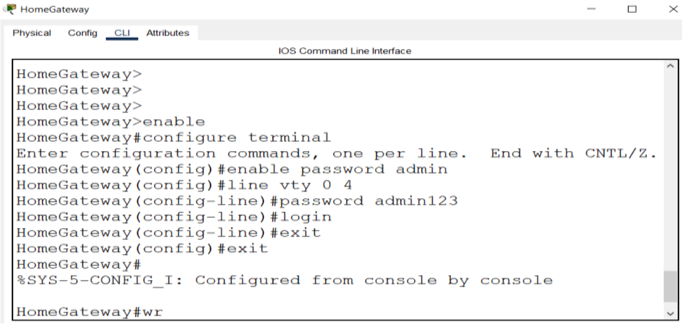


```
HomeGateway>enable
Password:
HomeGateway#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HomeGateway(config)#access-list 150 deny ip 192.168.26.103 0.0.0.0 192.168.25.102 0.0.0.0
HomeGateway(config)#access-list 150 deny ip 192.168.26.103 0.0.0.0 192.168.25.101 0.0.0.0
HomeGateway(config)#access-list 150 deny ip 192.168.26.103 0.0.0.0 192.168.25.100 0.0.0.0
HomeGateway(config)#access-list 150 deny ip 192.168.26.103 0.0.0.0 192.168.25.106 0.0.0.0
HomeGateway(config)#access-list 150 deny ip 192.168.26.103 0.0.0.0 192.168.25.107 0.0.0.0
HomeGateway(config)#access-list 150 permit ip any any
HomeGateway(config)#int f1/0
HomeGateway(config-if)#ip access-group 150 out
HomeGateway(config-if)#exit
HomeGateway(config)#exit
HomeGateway#
%SYS-5-CONFIG_I: Configured from console by console

HomeGateway#wr
```

Fig. 10. Extended ACL policy for criterion 1.

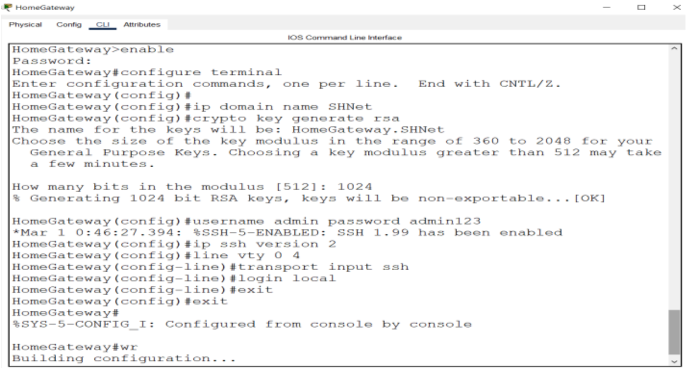
Furthermore, by implementing this policy on the external interface of the home gateway router, we successfully fulfil our objective of effectively managing outgoing traffic while maintaining control.

Now, we configure Telnet and SSH on the home gateway router so the user can access and manage it remotely using an SSH client on the user's device show in Fig. 11 and Fig. 12. Using the 'crypto key generate RSA' command, a crypto key is generated to maintain a secure SSH connection.



```
HomeGateway>
HomeGateway>
HomeGateway>
HomeGateway>enable
HomeGateway#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HomeGateway(config)#enable password admin
HomeGateway(config)#line vty 0 4
HomeGateway(config-line)#password admin123
HomeGateway(config-line)#login
HomeGateway(config-line)#exit
HomeGateway(config)#exit
HomeGateway#
%SYS-5-CONFIG_I: Configured from console by console

HomeGateway#wr
```

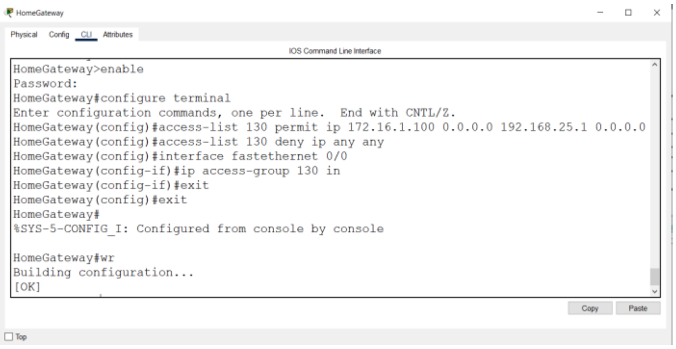
Fig. 11. Telnet activation on home gateway router.



```
HomeGateway>enable
Password:
HomeGateway#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HomeGateway(config)#
HomeGateway(config)#ip domain name SHNet
HomeGateway(config)#crypto key generate rsa
The name for the keys will be: HomeGateway.SHNet
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

HomeGateway(config)#username admin password admin123
*Mar 1 0:46:27.394: %SSH-5-ENABLED: SSH 1.99 has been enabled
HomeGateway(config)#ip ssh version 2
HomeGateway(config)#line vty 0 4
HomeGateway(config-line)#transport input ssh
HomeGateway(config-line)#login local
HomeGateway(config-line)#exit
HomeGateway(config)#exit
HomeGateway#
%SYS-5-CONFIG_I: Configured from console by console

HomeGateway#wr
Building configuration...
```

Fig. 12. SSH activation on home gateway router.

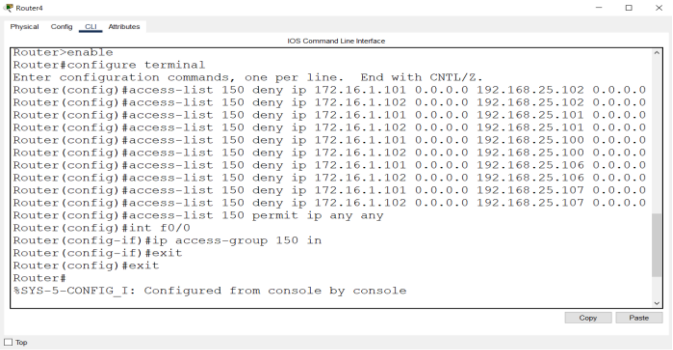
Only Remote Host 1 can access the Home-Gateway network by Telnet and SSH. Remote Hosts 2 and 3 cannot access the smart home network remotely. We implement and configure extended inbound ACL at the home gateway router interface FastEthernet 0/0 to manage external user network access as per criterion 2, shown in the Fig. 13.



```
HomeGateway>enable
Password:
HomeGateway#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HomeGateway(config)#access-list 130 permit ip 172.16.1.100 0.0.0.0 192.168.25.1 0.0.0.0
HomeGateway(config)#access-list 130 deny ip any any
HomeGateway(config)#interface fastethernet 0/0
HomeGateway(config-if)#ip access-group 130 in
HomeGateway(config-if)#exit
HomeGateway(config)#exit
HomeGateway#
%SYS-5-CONFIG_I: Configured from console by console

HomeGateway#wr
Building configuration...
[OK]
```

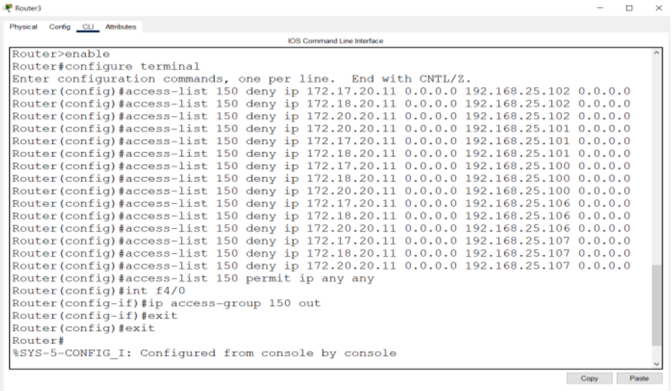
Fig. 13. Configure ACL for remote user access by telnet and SSH.

Remote Host 1, User 1, 2, 4, 6, & 8 can control all IoT devices of the smart home, and another user cannot control all IoT devices except IoT-2, 4, and 5. We configured extended ACL policy to the 3 & 4 router's interface FastEthernet 1/0 and 4/0 to manage internal IoT device access as required shown in Fig. 14 and Fig. 15. We successfully fulfil our objective of effectively managing incoming traffic while maintaining control.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 150 deny ip 172.16.1.101 0.0.0.0 192.168.25.102 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.102 0.0.0.0 192.168.25.102 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.101 0.0.0.0 192.168.25.101 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.102 0.0.0.0 192.168.25.101 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.101 0.0.0.0 192.168.25.100 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.102 0.0.0.0 192.168.25.100 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.101 0.0.0.0 192.168.25.106 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.102 0.0.0.0 192.168.25.106 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.101 0.0.0.0 192.168.25.107 0.0.0.0
Router(config)#access-list 150 deny ip 172.16.1.102 0.0.0.0 192.168.25.107 0.0.0.0
Router(config)#access-list 150 permit ip any any
Router(config)#int f0/0
Router(config-if)#ip access-group 150 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

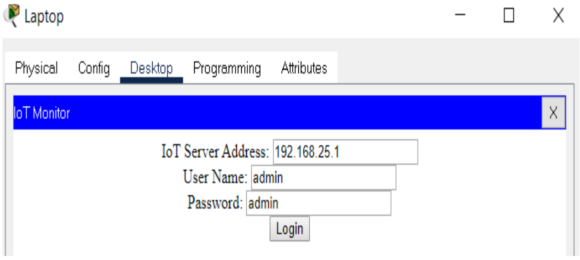
Fig. 14. Configure ACL for remote user control IoT devices.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 150 deny ip 172.17.20.11 0.0.0.0 192.168.25.102 0.0.0.0
Router(config)#access-list 150 deny ip 172.18.20.11 0.0.0.0 192.168.25.102 0.0.0.0
Router(config)#access-list 150 deny ip 172.20.20.11 0.0.0.0 192.168.25.102 0.0.0.0
Router(config)#access-list 150 deny ip 172.20.20.11 0.0.0.0 192.168.25.101 0.0.0.0
Router(config)#access-list 150 deny ip 172.17.20.11 0.0.0.0 192.168.25.101 0.0.0.0
Router(config)#access-list 150 deny ip 172.18.20.11 0.0.0.0 192.168.25.101 0.0.0.0
Router(config)#access-list 150 deny ip 172.17.20.11 0.0.0.0 192.168.25.100 0.0.0.0
Router(config)#access-list 150 deny ip 172.18.20.11 0.0.0.0 192.168.25.100 0.0.0.0
Router(config)#access-list 150 deny ip 172.20.20.11 0.0.0.0 192.168.25.100 0.0.0.0
Router(config)#access-list 150 deny ip 172.17.20.11 0.0.0.0 192.168.25.106 0.0.0.0
Router(config)#access-list 150 deny ip 172.18.20.11 0.0.0.0 192.168.25.106 0.0.0.0
Router(config)#access-list 150 deny ip 172.20.20.11 0.0.0.0 192.168.25.106 0.0.0.0
Router(config)#access-list 150 deny ip 172.17.20.11 0.0.0.0 192.168.25.107 0.0.0.0
Router(config)#access-list 150 deny ip 172.18.20.11 0.0.0.0 192.168.25.107 0.0.0.0
Router(config)#access-list 150 deny ip 172.20.20.11 0.0.0.0 192.168.25.107 0.0.0.0
Router(config)#access-list 150 permit ip any any
Router(config)#int f4/0
Router(config-if)#ip access-group 150 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Fig. 15. Configure ACL for user control IoT devices.

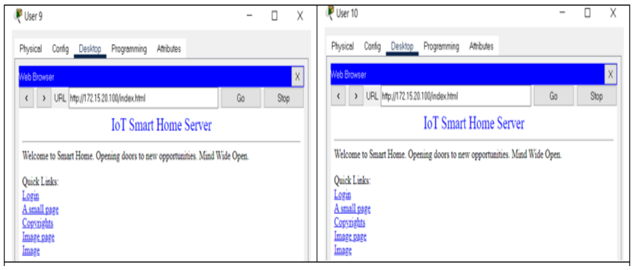
To establish the first connection with the IoT Server (192.168.25.1) and monitor the linked home application (IoT Devices), the home user computer and device will submit an HTTP request to the IoT server and verify the receipt of an HTTP response. The browser displays the home page of the IoT server, which requires the user to log in as an administrator using their admin name and Password. This procedure is effectively completed, as seen in Fig. 16.



IoT Server Address: 192.168.25.1
User Name: admin
Password: admin

Fig. 16. IoT server login.

Verified the following requirements: remote Host 1, User 1, 2, 4, 6, and 8 can control all IoT devices of the smart home, and another user cannot control all IoT devices except IoT-2, 4, and 5 are shown in Fig. 17 and Fig. 18.



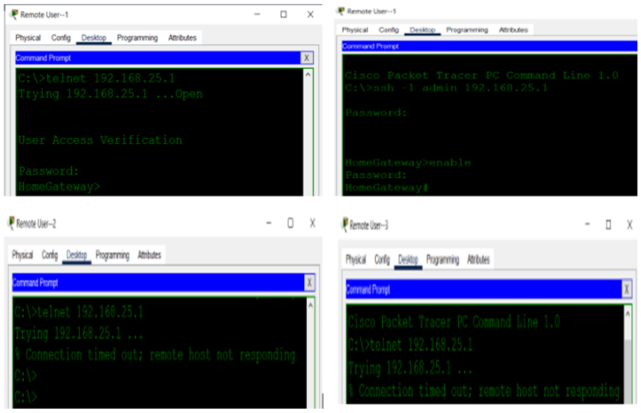
URL http://172.15.20.100/index.html

IoT Smart Home Server

Welcome to Smart Home. Opening doors to new opportunities. Mind Wide Open.

Quick Links:

Fig. 17. User access the IoT server.



```
C:\>telnet 192.168.25.1
Trying 192.168.25.1 ...Open


User Access Verification

Password:
HomeGateway>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.25.1

Password:



HomeGateway>enable
Password:
HomeGateway#
```

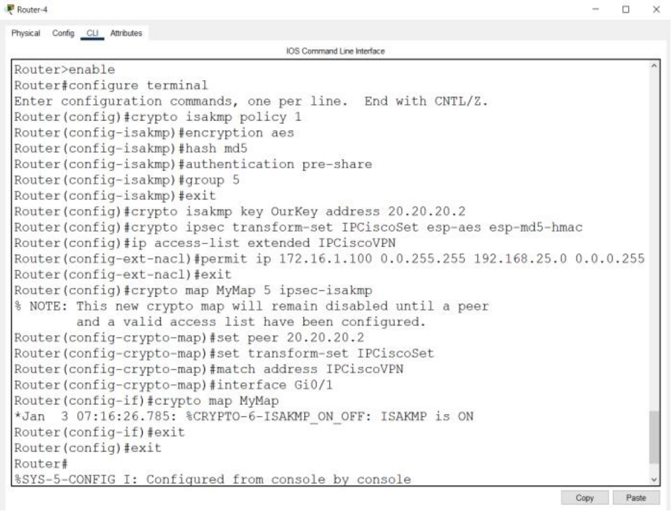
```
C:\>telnet 192.168.25.1
Trying 192.168.25.1 ...
% Connection timed out; remote host not responding
C:\>
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.25.1
Trying 192.168.25.1 ...
% Connection timed out; remote host not responding
```

Fig. 18. Remote user access the network by telnet and SSH.

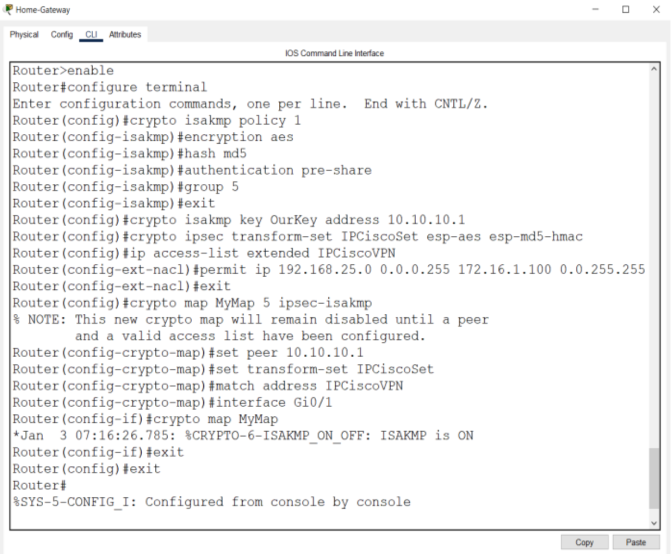
The IPSec for VPN Configuration involves configuring the ISAKMP Policy. We make this arrangement to facilitate Phase 1 discussions. To do this, we will use the "crypto isakmp policy" command with a priority value of 1. The priority number identifies the policy and indicates its degree of priority. A lower numerical priority corresponds to a greater level of importance. According to this policy, we shall establish the specific protocols for encryption, hashing, authentication, and group procedures. Our encryption technology is AES. We can also use DES, 3DES, AES-192, and AES-256 encryption algorithms. The hashing algorithm we use is MD5. Another alternative might be the use of SHA hashing. We used a pre-shared authentication mechanism.

Additionally, we may use the rsa-sig and crack techniques. We used group 10 as the crypto isakmp policy group. Additional Diffie-Hellman groups are accessible at this location. We will establish a pre-shared key to authenticate communication between two peers. We will verify the pre-shared key by associating it with the IP address of the remote tunnel endpoint. Router4 will use this pre-shared key to authenticate when establishing a VPN Tunnel with the home gateway Router. The pre-shared key must be exact at the other end. The pre-shared key we are using is "OurKey", and the IP address of the remote tunnel is 20.20.20.2 and 10.10.10.2. We will establish the method for safeguarding the communication using the "crypto ipsec transform-set" command, specifying the name of the transform set shown in Fig. 19 and Fig. 20. In this context, we shall use AES as an encryption algorithm and MD5 as a hashing algorithm.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key OurKey address 20.20.20.2
Router(config)#crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
Router(config)#ip access-list extended IPCiscoVPN
Router(config-ext-nacl)#permit ip 172.16.1.100 0.0.255.255 192.168.25.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map MyMap 5 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 20.20.20.2
Router(config-crypto-map)#set transform-set IPCiscoSet
Router(config-crypto-map)#match address IPCiscoVPN
Router(config-crypto-map)#interface Gi0/1
Router(config-if)#crypto map MyMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

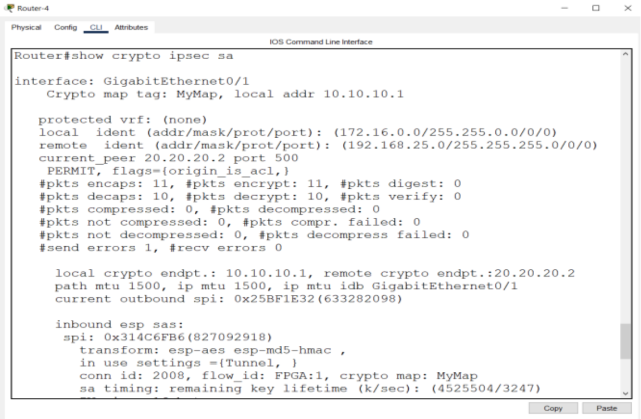
Fig. 19. Configure IPSec and VPN in outer router 4.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key OurKey address 10.10.10.1
Router(config)#crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
Router(config)#ip access-list extended IPCiscoVPN
Router(config-ext-nacl)#permit ip 192.168.25.0 0.0.0.255 172.16.1.100 0.0.255.255
Router(config-ext-nacl)#exit
Router(config)#crypto map MyMap 5 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 10.10.10.1
Router(config-crypto-map)#set transform-set IPCiscoSet
Router(config-crypto-map)#match address IPCiscoVPN
Router(config-crypto-map)#interface Gi0/1
Router(config-if)#crypto map MyMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

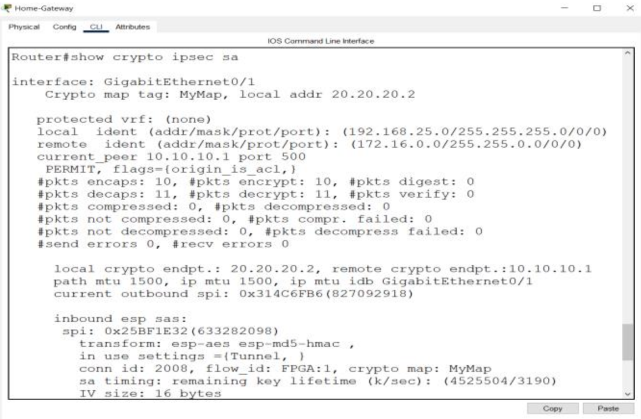
Fig. 20. Configure IPSec and VPN in core home gateway router.

Identification and validity of IPSec VPN devices and data packets are verified via authentication are shown in Fig. 21 and Fig. 22.



```
Router#show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: MyMap, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.25.0/255.255.255.0/0/0)
   current_peer 20.20.20.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.:20.20.20.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x25BF1E32(633282098)

     inbound esp sas:
      spi: 0x314C6FB6(827092918)
        transform: esp-aes esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: MyMap
        sa timing: remaining key lifetime (k/sec): (4525504/3247)
```

Fig. 21. Verified IPSec and VPN in outer router 4.



```
Router#show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: MyMap, local addr 20.20.20.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.25.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
   current_peer 10.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
   #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 20.20.20.2, remote crypto endpt.:10.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x314C6FB6(827092918)

     inbound esp sas:
      spi: 0x25BF1E32(633282098)
        transform: esp-aes esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: MyMap
        sa timing: remaining key lifetime (k/sec): (4525504/3190)
        IV size: 16 bytes
```

Fig. 22. Verified IPSec and VPN in core home gateway router.

VIII. CONCLUSION

The smart home automation system, which has a secure network architecture and thorough authentication, significantly improves security. This technology efficiently safeguards smart homes against unwanted access and other security vulnerabilities. The suggested system can regulate domestic appliances, oversee environmental conditions, and detect unwanted access. The system employs a secure network architecture with an Access Control List (ACL) and robust authentication mechanisms to safeguard against illegal entry. The Next Generation Access Control (NGAC) approach, which works with Telnet, SSH, IPSec, and VPN to detect unauthorized access and mitigate security issues, enhances security by identifying and addressing unwanted access and security concerns. The system's usefulness is confirmed via simulation, showcasing its efficacy in improving security.

In the future, we will validate our proposed model by hardware implementation with enhanced capabilities to detect and counter intricate cyberattacks by developing advanced methods. In addition, we guarantee the implementation of robust measures for safeguarding user privacy, including secure data storage, transfer, and access control.

The study proves that the suggested smart home automation system may enhance security in smart houses. This contribution is crucial in smart home technologies since security is paramount for several prospective consumers.

ACKNOWLEDGMENT

This research is supported by University of Chittagong, Chattogram, Bangladesh.

REFERENCES

[1] Orfanos, V.A.; Kaminaris, S.D.; Papageorgas, P.; Piromalis, D.; Kandris, D., "*A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications*", J. Sens. Actuator Netw. 2023, 12, 30. https://doi.org/10.3390/jsan12020030.

[2] A. Aldahmani, B. Ouni, T. Lestable and M. Debbah, *"Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends,"* in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 281-292, 2023, doi: 10.1109/OJVT.2023.3234069.

[3] Ragothaman, Kaushik, Yong Wang, Bhaskar Rimal, and Mark Lawrence., *"Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions"*, Sensors 23, 2023, no. 4: 1805. https://doi.org/10.3390/s23041805.

[4] Baek, Jinsuk, Munene W. Kanampiu, and Cheonshik Kim., *"A Secure Internet of Things Smart Home Network: Design and Configuration"*, Applied Sciences 11, 2021, no. 14: 6280. https://doi.org/10.3390/app11146280.

[5] Cimorelli Belfiore, Roberta, and Anna Lisa Ferrara., *"Security Analysis of Access Control Policies for Smart Homes."*, In Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, pp. 99-106. 2023.

[6] Alghamdi, Samiah, and Steven Furnell., *"Assessing Security and Privacy Insights for Smart Home Users."*, In ICISSP, pp. 592-599. 2023.

[7] Keshk, Arabi Elsayed, Mahmoud Hussein, and Eman M. Mohamed., *"A Review on Improving Performance of Multi-Users Smart Homes Applications Based IoT."*, International Journal of Computers and Information (2023).

[8] H. Li, D. Han and C. -C. Chang, *"DAC4SH: A Novel Data Access Control Scheme for Smart Home Using Smart Contracts,"* in IEEE Sensors Journal, vol. 23, no. 6, pp. 6178-6191, 15 March15, 2023, doi: 10.1109/JSEN.2023.3241093.

[9] Zou, Qingsong, Qing Li, Ruoyu Li, Yucheng Huang, Gareth Tyson, Jingyu Xiao, and Yong Jiang., *"IoTBeholder: A Privacy Snooping Attack on User Habitual Behaviors from Smart Home Wi-Fi Traffic"*, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 7, no. 1 (2023): 1-26.

[10] Dr.D.Devi Aruna, *"Secure Smart Home Design and Analysis for Elderly People Using Internet of Things (IoT) Technologies"*, EPRA International Journal of Multidisciplinary Research (IJMR), vol. 9, no. 9, pp. 65–67, Sep. 2023.

[11] Kabir, M.H.; Chowdhury, J.A.; Fahim, I.M.; Hasan, M.N.; Hasnat, A.; Mahdi, A.J. Design and Simulation of AI-Enabled Digital Twin Model for Smart Industry 4.0. Eng. Proc. 2023, 58, 119. https://doi.org/10.3390/ecsa-10-16235.

[12] Stolojescu-Crisan, Cristina, Calin Crisan, and Bogdan-Petru Butunoi., *"Access control and surveillance in a smart home"*, High-Confidence Computing 2, no. 1 (2022): 100036.

[13] S. R, A. K. Kumar, A. Titus, S. Hemajothi, J. Venkatesh and L. A, *"Design and Development of an AI based Intelligent Door for Home Security System,"* 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10200307.

[14] Amr T. A. Elsayed, Almohammady S. Alsharkawy, Mohamed S. Farag and S. E. Abo-Youssef, *"Secure Data Sharing in Smart Homes: An Efficient Approach Based on Local Differential Privacy and Randomized Responses"* International Journal of Advanced Computer Science and Applications(IJACSA), 14(8), 2023.

[15] Pandya, Sharnil, Hemant Ghayvat, Ketan Kotecha, Mohammed Awais, Saeed Akbarzadeh, Prosanta Gope, Subhas Chandra Mukhopadhyay, and Wei Chen., *"Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol"*, Applied System Innovation 1, 2018, no. 4: 42. https://doi.org/10.3390/asi1040042.

[16] Kabir, M.H.; Kabir, M.A.; Islam, M.S.; Mortuza, M.G.; Mohiuddin, M. Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols. Eng. Proc. 2021, 10, 47. https://doi.org/10.3390/ecsa-8-11285.

[17] Hind Meziane and Noura Ouerdi, *"A Study of Modelling IoT Security Systems with Unified Modelling Language (UML)"*, International Journal of Advanced Computer Science and Applications(IJACSA), 13(11), 2022.

[18] Aissam Outchakoucht, Anas Abou El Kalam, Hamza Es-Samaali and Siham Benhadou, *"Machine Learning based Access Control Framework for the Internet of Things"* International Journal of Advanced Computer Science and Applications(IJACSA), 11(2), 2020.

[19] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi and Saleem Ullah, *"Security Issues in the Internet of Things (IoT): A Comprehensive Study"*, International Journal of Advanced Computer Science and Applications(IJACSA), 8(6), 2017.

[20] M. Başer, E. Y. Güven and M. A. Aydın, *"SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot,"* 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 2021, pp. 806-811, doi: 10.1109/UBMK52708.2021.9558948.

[21] Majidha Fathima, K. M. *"A survey of the exemplary practices in network operations and management."* In Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2020, pp. 181-194. Springer Singapore, 2021.

[22] Ylonen, Tatu., *"SSH–secure login connections over the Internet"*, In Proceedings of the 6th USENIX Security Symposium, vol. 37, pp. 40-52. 1996.

[23] V. HASHIYANA, T. HAIDUWA, N. SURESH, A. BRATHA and F. K. OUMA, *"Design and Implementation of an IPSec Virtual Private Network: A Case Study at the University of Namibia,"* 2020 IST-Africa Conference (IST-Africa), Kampala, Uganda, 2020, pp. 1-6.

[24] S. Tongkaw and A. Tongkaw, *"Multi-VLAN Design over IPSec VPN for Campus Network,"* 2018 IEEE Conference on Wireless Sensors (ICWiSe), Langkawi, Malaysia, 2018, pp. 66-71, doi: 10.1109/ICWISE.2018.8633293.

[25] F. Hauser, M. Häberle, M. Schmidt and M. Menth, *"P4-IPsec: Site-to-Site and Host-to-Site VPN With IPsec in P4-Based SDN,"* in IEEE Access, vol. 8, pp. 139567-139586, 2020, doi: 10.1109/ACCESS.2020.3012738.

[26] Abdul Wahab Ahmed, Omair Ahmad Khan, Mian Muhammad Ahmed and Munam Ali Shah, *"A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT"*, International Journal of Advanced Computer Science and Applications(IJACSA), 8(7), 2017.

[27] Ruíz-Lagunas Juan Jesús, Antolino-Hernández Anastacio, Reyes-Gutiérrez Mauricio René, Ferreira-Medina Heberto, Torres-Millarez Cristhian and Paniagua-Villagómez Omar, *"How to Improve the IoT Security Implementing IDS/IPS Tool using Raspberry Pi 3B+"*, International Journal of Advanced Computer Science and Applications(IJACSA), 10(9), 2019.

[28] Yasir Mahmood, Nazri Kama, Azri Azmi and Suraya Ya'acob, "An IoT based Home Automation Integrated Approach: Impact on Society in Sustainable Development Perspective" International Journal of Advanced Computer Science and Applications(IJACSA), 11(1), 2020.

[29] Mubashir Ali, Zarsha Nazim, Waqar Azeem, Muhammad Haroon, Aamir Hussain, Khadija Javed and Maria Tariq, *"An IoT based Approach for Efficient Home Automation with ThingSpeak"*, International Journal of Advanced Computer Science and Applications(IJACSA), 11(6), 2020.

[30] Omar Almutairi and Khalid Almarhabi, *"Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia"*, International Journal of Advanced Computer Science and Applications(IJACSA), 12(4), 2021.

[31] Rihab Fahd Al-Mutawa and Fathy Albouraey Eassa, *"A Smart Home System based on Internet of Things"*, International Journal of Advanced Computer Science and Applications(IJACSA), 11(2), 2020.