International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228539

Analysis and Implementation of 5G-IoT based Smart Residential Buildings using Cisco Packet Tracer 8.1

Narendra Gurjar*[1], Jitendra Dangra[2]

*[1]Department of Computer Science and Engineering, Laxmi Narain Collage of Technology and Science (RIT), Indore, Madhya Pradesh, India

[2]Department of Information Technology, Laxmi Narain Collage of Technology and Science (RIT), Indore, Madhya Pradesh, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 343-352

Article History
Accepted: 12 Nov 2022
Published: 29 Nov 2022

ABSTRACT

Integration of IoT and 5G enables us to fulfil today's need to create smart residential buildings to enhance life quality and safety in various aspects. This paper proposes the design and implementation of a 5G IoT based Smart Residential Building using the most recent version of CISCO Packet Tracer (a simulation software). Different smart IoE devices were used for automation which allow distant monitoring and controlling. Since these buildings are vulnerable to cyber-attacks and security threats, this paper also analyzes the proposed security framework and how such an implementation on using various sensors and actuators enables us to enhance the security and safety. In addition to this, we also outline the measures to be taken by the government and building owners to strengthen the security. The simulation results show that integrating 5G and IoT is a promising and cost-effective if it gets implemented practically in the real world.

Keywords: Smart Residential Buildings, 5G, IoT, Cisco Packet Tracer Simulator

I. INTRODUCTION

Internet of Things (IoT) and 5G are like "two halves of a whole". The main goal of integrating 5G and IoT lies behind its ability to drive advancements and achieve a sustainable future.

The powerful integration of IoT and 5G has spurred a more practical implementation of technologies such as that of Smart Residential Buildings. The motivation of this paper is to integrate the IoT and 5G in home automation using a simulator Cisco Packet Tracer version 8.1 and to incorporate several security and safety features into our implementation which in turn makes it a "Smart Residential Building".

While rest of the paper is organized as follows: Section II presents the review of the related study, followed by Section III methodology while Section IV the implementation. Further, Section V is the analysis of security and safety features. Finally, the conclusion

and future scope are included in Sections VI and VII, respectively.

II. LITERATURE REVIEW

Researcher Darrell West in [1] concludes, that with the emerging 5G and IoT, it is possible to deploy technologies like that of smart residential buildings which promote long-term sustainability. In the case study [2], the researchers highlight how sustainable smart buildings contribute to maximizing energy and water efficiency in smart cities.

Integrating IoT with 5G Wireless Communications

The IoT is witnessing a very sharp growth, with billions of devices already in the market [3]. The low latency of a 5G communication proves itself to be a reliable solution in-order to overcome the problem of lags in data transfer in IoT devices.

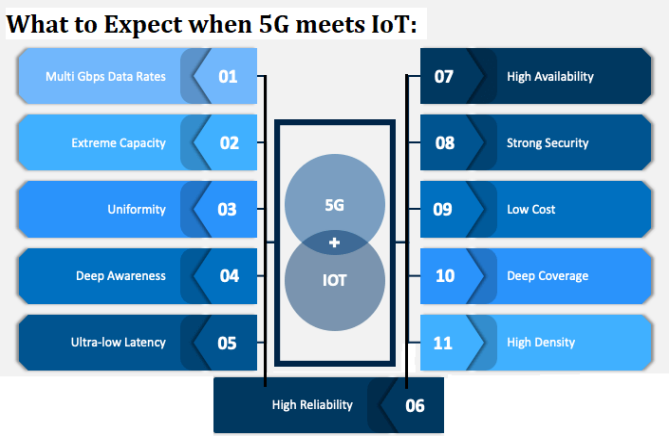

Figure 1: 5G and Internet of Things

Today recognizing the potential of 5G and IoT integration has become a worldwide interest. Government institutes, and major tech players in the private sector are funding research projects based on this integration. Researchers in [4] presented a novel architecture based on 5G-IoT.

Since 5G possesses the attribute of network slicing, therefore it has the capability to respond to the varying needs of massive IoT, which mostly finds its use in devices used in smart homes [5]. In [6,7] authors proposed to enable smart homes with three different 5G network slices. In other terms, 5G is an efficient network in terms of improving the lives of residents which also extends support to sensor-based IoT actuators.

1) Increased Cyber Security Concerns

The nature of 5G networks expands cyber risks. Since it has shifted to a distributed, software-defined digital routing, it is more vulnerable to cyber-attacks than its predecessors. Its integration with billions of hackable smart IoT-based devices has led to a multidimensional vulnerability. The software managing the 5G network itself can be vulnerable. Small-cell antennas installed in the urban areas have become new hard targets [8]. Researchers in [9] studied and classified potential security attacks at each layer of the 5G-IoT architecture.

Today the security of fifth-generation networks has become paramount. Certainly, the implementation of M.L. and A.I. can help improve the security in a 5G network [10]. Also, technical solutions like using Wideband Antennas systems can come out to help extend capacity and increase the IoT security [11].

2) Integrating A. I. with 5G-IoT

The fusion of the trio of A.I., 5G and IoT was named "The Fifth Wave of Computing". A.I. helps by processing massive raw data generated by a huge number of smart devices at the edge to reduce data size, giving insights, and making efficient decisions out of it. These applications rely on 5G's fast bandwidth [12,13,14]. In the 5G context, AI can directly benefit the driving technologies such as SDN and NFV to be integrated into MEC and IoT.

3) Cisco Packet Tracer version 8.1

Cisco Packet Tracer is a proprietary multi-platform simulator that enables learners to design and construct complex networks, explore, and simulate numerous smart IoT devices, actuators, and sensors and configure them to implement the concept of

smart homes, cities, and grids [16]. In our paper, we have used its latest version which is, Cisco Packet Tracer 8.1 It is available for a free download for all learners and teachers with a valid NetAcad account [17].

III. METHODOLOGY

To implement a smart residential building, we used various smart devices, a home gateway, 5G antennas, a C.O. server, a switch, an IoT server and a DNS server. Talking about the network topology, it includes a C.O. server installed at the ISP end whose backbone and cell tower were configured. Then, a 5G cellular network was established with a base station near our residential city. Now, the DHCP service was activated on the C.O. server and the IP address of the DNS server was provided. The cloud IoT server is connected. The IoT server and DNS server have been given a static IP. The IoT server is using a platform like SaaS. The user can connect to the live IoT monitoring page while being at a remote location.

A. Algorithm

Step 1: Start the project

Step 2: Drag a home gateway onto the Packet Tracer 8.1 workspace, configure the network from defaults, and set the password.

Step 3: Now, drag all the required smart devices and connect them to the home gateway. The wireless connection is established using a password that was set in the home gateway.

Step 4: Drag all the other devices to form the ISP network, IoT server and a cellular 5G network and connect them.

Step 5: Now set up the C.O. server configuration i.e., both Backbone and Cell Tower. Turn on the DHCP service.

Step 6: Enable the DNS services like- HTTP, DNS etc.

Step 7: Connect the home gateway to the 5G base station. Home Gateway will get an automatic IP address.

Step 8: Now provide static IP to both- the DNS server and the IoT server. This will ensure that the smart devices are always connected to it.

Step 9: Turn ON the Registration Server. And configure all the IoT devices by turning on the Remote Server option, writing the IoT server's IP address and username and password.

Step 10: To check whether the data collected by sensors in smart devices is successfully being sent to the IoT server, ping the server using a laptop connected to Home Gateway.

Step 11: To access the IoT home page, log on to the IoT Monitor app or put the IoT server's IP address i in a browser. After logging in to the system, the real-time status of all the smart devices will appear.

IV. IMPLEMENTATION AND RESULTS

Figures 2 and 3 show the implementation of the proposed 5G IoT-based Smart Residential Building using Cisco Packet Tracer version 8.1. The topology was clustered to make it easily understandable.

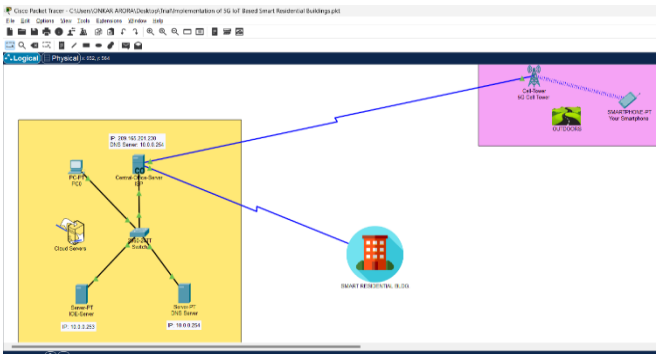

Figure 2 : Smart Residential Building architecture in Logical Workspace of Cisco Packet Tracer 8.1

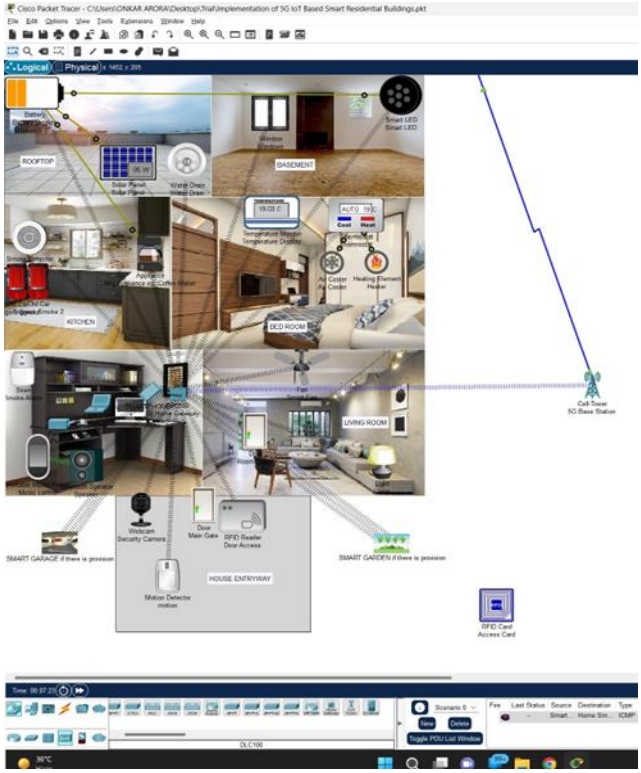

Figure 3: Smart Residential Building architecture in Logical Workspace of Cisco Packet Tracer 8.1

Figure 3 shows that if there is a provision of a garden in our residential building, a Smart Garden can also be implemented where lawn sprinklers and trip sensors work automatically based on the readings of the Humiture Monitor. A wind detector can also be installed if required

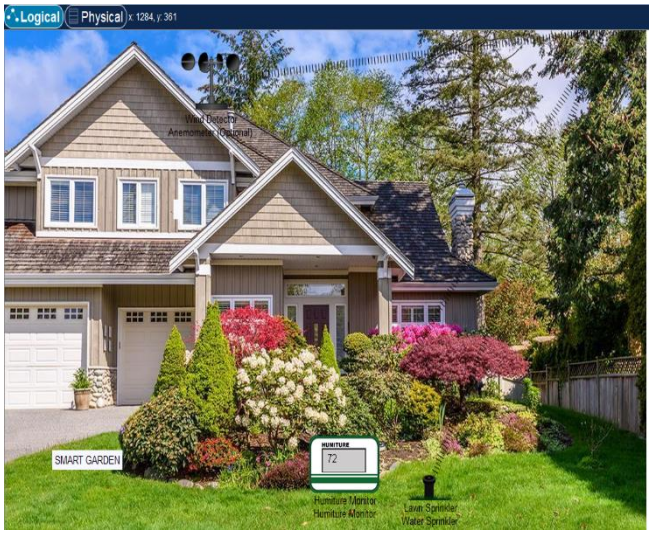

Figure 4: Implementation of Smart Garden (if there is a provision)

Similarly, Figure 5 highlights that if there is a provision of a garage in our residential building, a Smart Garage can also be implemented where the door and windows automatically get opened in case of fire or smoke

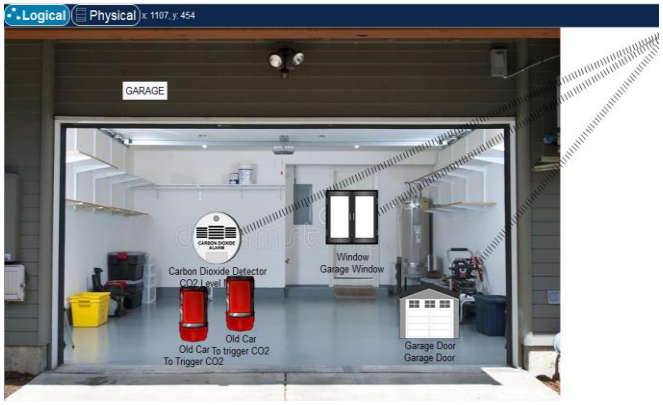

Figure 5: Implementation of Smart Garden (if there is a provision)

As illustrated in figure 6 when outdoors, the user can access the IoT server after verification using the log-in credentials available to him

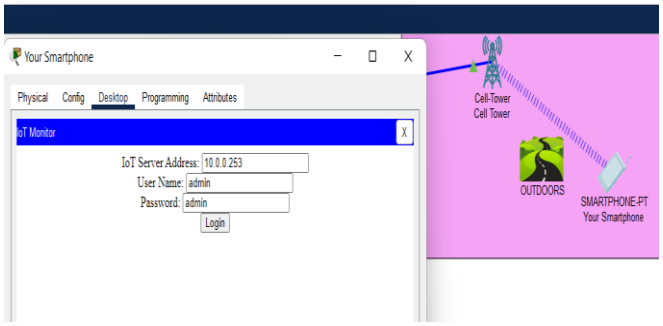

Figure 6: Logging into the IoT Server using a Smartphone.

As illustrated in figure 7, the user can see the live status of the devices and can manage things remotely.

Figure 7 : Real-time status of the registered IoT devices

As highlighted in figure 8, the user can add new rules and edit the pre-set conditions to control the IoE devices as per his/her demands.

Since Cisco Packet Tracer 8.1 comes up with several programmable MCUs and sensors, we added more security and safety features to our existing implementation as shown in figure 9.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Fan-On	Thermostat Temperature > 20.0 °C	Set Smart Fan Status to High
Edit Remove	Yes	Fan-Off	Thermostat Temperature < 15.6 °C	Set Smart Fan Status to Off
Edit Remove	Yes	co2-on	CO2 Level Monitor Level >= 0.17	Set PTT0810GZQ7- On to 1 Set Garage Door On to true
Edit Remove	Yes	co2-off	CO2 Level Monitor Level < 0.17	Set PTT0810GZQ7- On to 0 Set Garage Door On to false
Edit Remove	Yes	cam-on	motion On is true	Set Security Camera On to true
Edit Remove	Yes	cam-off	motion On is false	Set Security Camera On to false
Edit Remove	Yes	water-on	Humiture Monitor Humitor < 70	Set Water Sprinkler Status to true
Edit Remove	Yes	water-off	Humiture Monitor Humitor >= 70	Set Water Sprinkler Status to false
Edit Remove	Yes	access-on	Door Access Card ID = 1001	Set Door Access Status to Valid
Edit Remove	Yes	access-off	Door Access Card ID != 1001	Set Door Access Status to Invalid
Edit Remove	Yes	door-close	Door Access Status is Invalid	Set Main Gate Lock to Lock
Edit Remove	Yes	door-open	Door Access Status is Valid	Set Main Gate Lock to Unlock
Edit Remove	Yes	lamp-on	Room Doors Lock is Unlock	Set Lamp Status to On
Edit Remove	Yes	lamp-dim	Room Doors Lock is Lock	Set Lamp Status to Dim
Edit Remove	Yes	siren-on	Smoke Detector Level >= 0.15	Set Smoke Alarm On to true

Figure 8 : Setting conditions for Automation

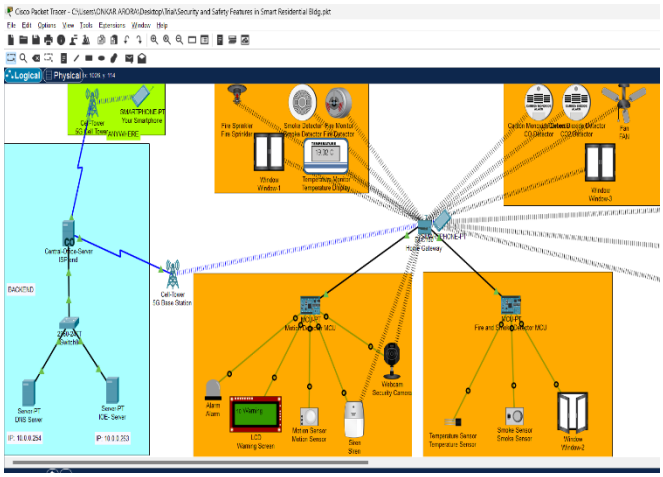

Figure 9 : Adding more safety features to our Implementation

V. Analysis of the Proposed Security Framework

To make our implementation secure, the home gateway is configured with WPA-PSK/WPA2 enterprise for authentication and validation which is a strong encryption method. We have changed the wi-fi router's default name and created a strong password. Also, the building wi-fi network presented is a "guest network" dedicated solely to IoT devices. This makes it detached and split up from the main network. Even if security gets compromised, the hackers do not get access to the sensitive and valuable information stored in our phones and laptops.

Each layer of the OSI model is encrypted in our implementation. The concept of Access Control Lists (ACLs) will also be integrated. Access to the IoT server can be restricted by limiting a user to his devices. In [18], the researcher finds the network security of 5G enabled smart homes in micro-segmentation.

SaaS and IaaS providers for IoT prioritize security and privacy. They have standard cybersecurity protocols for M2M communications and help authenticate and register all the devices and encrypt relevant data while in route. They also help in the implementation of ML algorithms at the edge. Also, it will be empowered by Disaster Recovery, which helps regain

access and functionality in case a natural disaster, bombings, or cyber-attacks occur.

Currently, 5G uses 128-bit encryption, but in future, it will support 256-bit level on using advanced cryptography algorithms. Also, 5G network security is being driven by AI and ML applications. AI and machine learning (ML) play a vital role in designing, modelling, and automation of many efficient security protocols against a diverse range of threats [19].

In [20], the researchers propose a Deep Learning and blockchain-powered security framework for intelligent 5G-enabled IoT that leverages DL competency for intelligent data analysis operation and blockchain for data security.

After implementing various programmable MCUs and sensors such as Motion Detector, RFID system, CCTV, temperature sensor, smoke sensor, etc. in our smart residential building, it now possesses several safety and security features, which are capable of preventing it from theft attempts and accidents such as fire, gas leak, etc. The MCUs are also configured to send alerts and emails in case of any emergency.

Figure 10 shows that if the motion detector recognizes some unauthorized access to the Smart Residential Building, the webcam gets turned ON and records the activity.

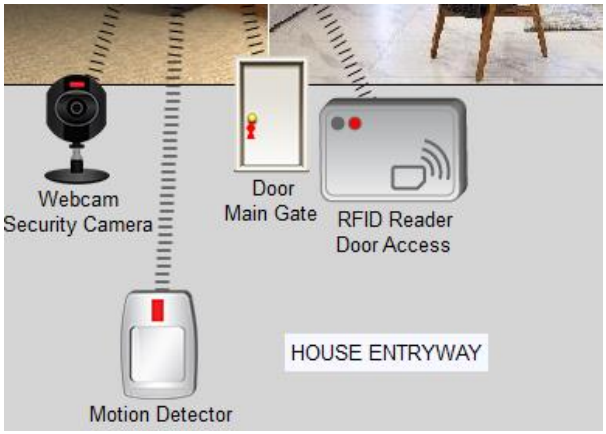

Figure 10: Webcam gets turned ON if Motion Detector detects any motion caption

The RFID system is also implemented as demonstrated in figure 11 and the concept is that- only when an authorized RFID Card passes onto the reader, the door lock will open otherwise, it remains locked.

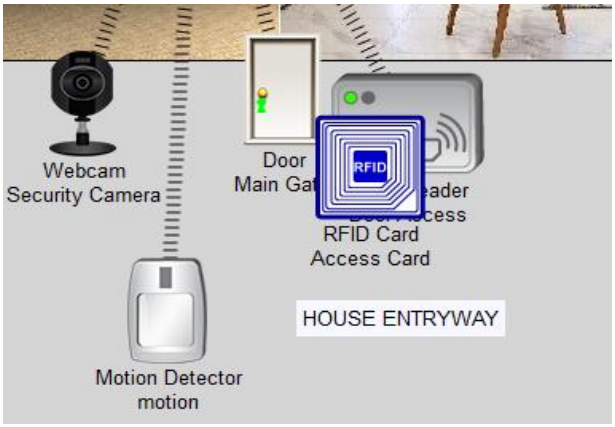

Figure 11: RFID reader giving entry only after swiping the Authorized Access Card

Figure 12 illustrates that to prevent thefts and robberies, in case of detection of any motion near the main door, the siren gets switched ON, the alarm starts showing a red-light and the LCD Screen shows a warning as a text message and simultaneously the Webcam gets turned ON. It can be done using a programmable MCU which also sends alerts to the owner.

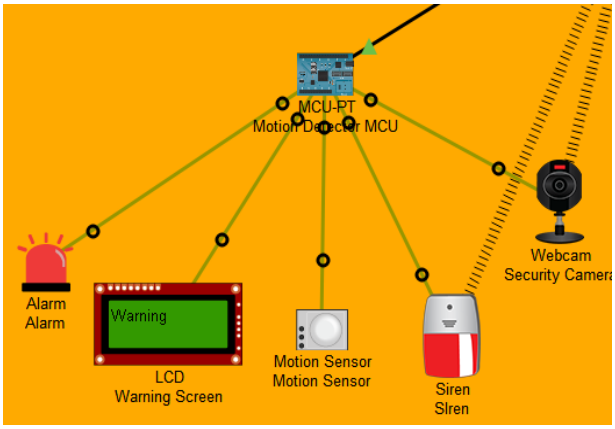

Figure 12: Alarming in case of a theft attempt

Also, to make it a highly-secured system, we can use the technology of Eye Retina Scan. It is configured with the unique patterns of retinal blood vessels.

Only when the retina scan successfully matches the sensor and gives a positive output, the motion sensor will start its process to serve home automation.

To safeguard our kitchen and garage area from fire, smoke, or gas leak, see Figure 13, the sensors can sense it using the IR values and smoke levels, automatically the water sprinklers get turned on and the windows get opened. And send alerts and notifications to the owner.

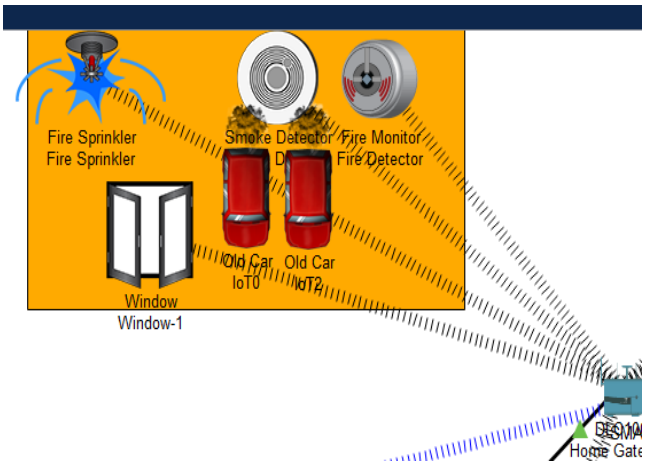

Figure 13: Fire and Ceiling Sprinklers System

Figure 14 demonstrates that, in case of any situation of gas leaks such as that of Carbon Monoxide or Carbon Dioxide, the respective sensors can sense it and automatically the fan gets turned on at high speed and the windows get opened for ventilation.

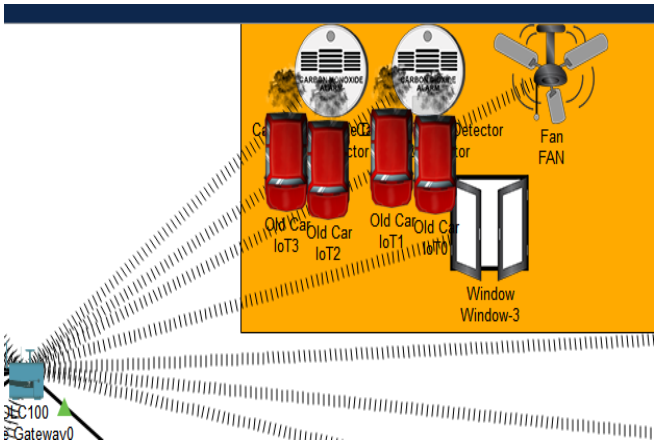

Figure 15: Aerating on detection of CO and CO2

Some conditions or terms of use that should be there to further strengthen the security of Smart Residential Buildings while implementing them practically in the real world are:

- To start 5G services in smart residential buildings, it should be made mandatory to take a certificate from ISO (International Organization for Standardization).
- Multi-factor authentication to be enabled by the owner and firmware to be updated.
- Public wi-fi networks must be avoided while accessing the IoT network
- The devices should be configured to automatically install the updates and security patches. Also, there should be regular audits and up-gradation of the devices.
- No Internet-connected smart home device or appliance be allowed to get sold as junk.
- The complete information about the engineers repairing the smart devices or network should be furnished to the owner.
- The governments and telecom ministries should fix the accountability of the ISP to keep the network secure. The ISP should be bound to send a monthly report of the internet operator. Also, if an outsider tries to use the network, then the ISP will have to report it to the consumer.

VI. Conclusion

In this paper, we presented a design, simulation, and implementation of a 5G IoT based Smart Residential Building on the latest version of Cisco Packet Tracer which also possesses various security and safety features as analyzed. The smart devices can be controlled remotely using end-user devices. 5G-IoT integration proves out to be very beneficial for implementing technologies like that of Smart Residential Buildings.

In our analysis, we found the security measures and framework to be very critical. On installing sensors such as Motion Detector, RFID system, CCTV, temperature sensor, smoke sensor, etc. in our implementation, the smart residential building now can prevent thefts and accidents such as fire, gas leaks, etc. This paper presented and analyzed a general security framework which outlines the major security requirements and needs of a 5G IoT based smart residential buildings.

Using Cisco Packet Tracer one can learn how to configure networks, connect smart devices to it and set conditions. With these simulations, design and implementation planning can be done in building smart residences in real life and in turn smart cities. The implementation also lets us conclude that smart residential buildings offer several features such as security, safety, energy efficiency, maintainability, comfort, and accessibility as well as environmentally friendliness.

VII. Future Scope

The aim of having smart residential buildings only starts with early planning in the design phase. Therefore, by using frameworks such as that of a Cisco Packet Tracer or Node-Red or NS3 to simulate IoT technology for automation in residential buildings, more complex simulations with more granular and better automation controls can also get implemented.

There is a high-need for assessment of existing security frameworks, their review and upliftment of security standards. Although in our proposed security framework, we endeavored to add as many security and safety features as we could, still many other security mechanisms and next-gen firewalls are needed to be integrated for further enhancement. “5G-IoT” field, its implementation in smart homes and the security frameworks for it, are still hot research topics.

Smart residential buildings are the future of India and the world. The technology is quite preferable for real-time security control, maintenance, and prevention of all types of accidents with quick solutions. The implementation of such smart and secure residential buildings in the real-world is required on a vast scale. Even though it still lacks awareness and understanding among the population, soon there will be a revolution to convert simple residential buildings into smart residential buildings for the comfort, convenience, safety, and security in life.

VIII. REFERENCES

[1] Ame Darrell M. West: “Achieving sustainability in a 5G world” (2019) Brookings Institute’s Research Paper https://www.brookings.edu/wp-content/uploads/2016/11/gs_20161201_smartcities_paper.pdf

[2] Implementing ITU-T International Standards to Shape Smart Sustainable Cities: The Case of Dubai Accessible: www.itu.int/en/publications/Documents/tsb/2016-DubaiCase/files/downloads/Dubai%20Case%20Study-410059-FINAL.pdf

[3] Ravi Kumar, Kanchan Kumari, Lokesh Kumar, Hitesh Kumar, Dr. C. H. Patil, „Literature Review of IoT & 5G”. Special Issue - 2020 International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICSITS - 2020 Conference Proceedings

[4] H. Rahimi, A. Zibaeenejad and A. A. Safavi, "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference

(IEMCON), 2018, pp. 81-88, doi: 10.1109/IEMCON.2018.8614777.

[5] Waleed Ejaz, Alagan Anpalagan, Muhammad Ali Imran, Minho Jo, Muhammad Naeem, Saad Bin Qaisar, Wei Wang: "Internet of Things (IoT) in 5G Wireless Communications" (January 2016) IEEE Access 4:10310-10314

[6] Dzogovic, Bruno, Bernardo Santos, Josef Noll, Van Thuan Do, Boning Feng and Thanh Van Do. "Enabling Smart Home with 5G Network Slicing." 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS) (2019): 543-548.

[7] B. Dzogovic, B. Santos, T. Van Do, B. Feng, T. Van Do and N. Jacot, "Bringing 5G Into User's Smart Home," 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2019, pp. 782-787, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00145. //network slicing

[8] Tom Wheeler and David Simpson, "Why 5G requires new approaches to cybersecurity Brookings Institute's Research Paper" (2019) Accessible: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

[9] Rahimi, Hamed & Zibaeenejad, Ali & Rajabzadeh, Parsa & Safavi, Ali Akbar. (2018). On the Security of the 5G-IoT Architecture. SCIOT '18: Proceedings of the international conference on smart cities and internet of things. 1-8. 10.1145/3269961.3269968.

[10] Daichi Nozaki, Koki Okamoto, Toru Mochida, Xin Qi, Zheng Wen, San Hlaing Myint, Kiyohito Tokuda, Takuro Sato, Kazuhiko Tamesue: "AI Management System to Prevent Accidents in Construction Zones Using 4K Cameras Based on 5G Network" 2018 21st International Symposium on Wireless Personal Multimedia Communications (WPMC) published in the IEEE Xplore digital library Accessible: https://ieeexplore.ieee.org/document/8712896

[11] Johnson J.H. Wang, "Wideband Antennas and Phased Arrays for Enhancing Cybersecurity in 5G Mobile Wireless" (2018) IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting Accessible: https://ieeexplore.ieee.org/document/8609059

[12] N. Javaid, A. Sher, H. Nasir and N. Guizani, "Intelligence in IoT-Based 5G Networks: Opportunities and Challenges," in IEEE Communications Magazine, vol. 56, no. 10, pp. 94-100, OCTOBER 2018, doi: 10.1109/MCOM.2018.1800036.

[13] https://www.arm.com/blogs/blueprint/the-fifth-wave-of-computing-ai-5g-iot

[14] https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-how-5G-AI-and-IoT-are-shaping-future-of-storage.pdf

[15] Liyanage, Madhusanka & Porambage, Pawani & Ding, Aaron Yi & Kalla, Anshuman. (2021). Driving forces for Multi-Access Edge Computing (MEC) IoT integration in 5G. ICT Express. 7. 10.1016/j.icte.2021.05.007.

[16] Andrea Finardi, "IoT Simulations with Cisco Packet Tracer" (2018)

[17] [ONLINE] https://www.packettracernetwork.com/download/download-packet-tracer.htmlv

[18] Armin Wasicek, The future of 5G smart home network security is micro-segmentation, Network Security, Volume 2020, Issue 11, 2020, Pages 11-13, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(20)30129-X.

(https://www.sciencedirect.com/science/article/pii/S135348582030129X)

[19] https://arxiv.org/abs/2007.04490

[20] S. Rathore, J. H. Park and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," in IEEE Access, vol. 9, pp. 90075-90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

Cite this article as :

Narendra Gurjar, Jitendra Dangra, "Analysis and Implementation of 5G-IoT based Smart Residential Buildings using Cisco Packet Tracer 8.1 ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 343-352, November-December 2022.
Available at doi :
https://doi.org/10.32628/CSEIT228539
Journal URL : https://ijsrcseit.com/CSEIT228539