Enhancing Building Design: Integrating IP Telephony, Internet of Things (IoT), and Fire Detection and Alarm System (FDAS) Network for Smart Buildings

Engr. Jaime V. David
Engr. Luigi Carlo De Jesus
Engr. Leonardo M. Samaniego, Jr.

Mark Joshua A. Añonuevo
Joshua D. Bernados
Julius Iver A. Reyes

Abstract

With the advancement of sensor technologies, numerous applications have emerged in various fields and regions. Utilizing these innovations and recent advancements can greatly benefit building applications, enhancing smart functions, and improving user comfort. In particular, the detection of fire plays a crucial role in preventing property destruction and potential loss of life. Fire Detection and Alarm Systems (FDAS) are intelligent frameworks aimed at providing automated management of control services and optimizing resource utilization. In this proposed model, all devices are registered in the IOE server and administered by an Administrator, while an IP Telephony network facilitates long-distance calls and Voice over Internet Protocol (VoIP) applications. The proponents have employed Cisco Packet Tracer, along with VLAN networks, to simulate the proposed model, and for real-life scenarios, they have implemented a cost-effective design for the Internet of Things (IoT) and FDAS-based Evacuation Service.

Keywords: *VLAN Networks, Cisco Packet Tracer, IoT, FDAS, IP Telephony*

Introduction

One of the most destructive aspects of fire is its rapid and uncontrollable spread (A. Bröring, 2011). Therefore, timely fire detection is crucial for preventing fire hazards. The Internet of Things (IoT) consists of interconnected sensors, actuators, and programmable devices embedded in home appliances, physical devices, and vehicles, enabling them to exchange data and improve the efficiency of everyday devices using computer-based systems (Anwar, 2018). In addition to enhancing device efficiency, IoT also offers economic benefits and aims to simplify human life by creating smart devices.

IoT extends the connectivity of objects beyond conventional devices used for everyday purposes. In this paper, the proponents have developed an IoT-based alarm system, where registered devices in the IOE server act as a home gateway controlled through the IoT monitor. This paper provides a detailed presentation of the design and implementation of monitoring products for the fire protection system based on IoT. The IoT terminal devices are responsible for monitoring the operational status of the fire suppression and safety system, including building fire department alarms, hydrant pipe flow, environmental temperature, and more. Through IoT, effective sensing, reliable transmission, and centralized and efficient management of the fire system become achievable (L. Huang, 2011).

Thus, the Fire Detection and Alarm System (FDAS) is widely adopted as the primary safety system for high-rise residential, commercial, and industrial establishments, as it acts as a protective measure to prevent accidental fires from escalating into unmanageable outbreaks. Traditional FDAS systems were traditionally constructed using wired transmission and the CAN (controller area network) bus protocol (Shu-guang, 2011). However, wired fire detection and alarm systems come with drawbacks, such as installation and maintenance costs, construction and expansion complexities, susceptibility to corrosion, aesthetic concerns, high fault rates, and a high count of false alarms due to limited cable transmission distance.

The network also includes an IP Telephony component, which showcases the basic setup of IP telephones within a specific building or establishment. These facilities facilitate long-distance voice communication or calls, allowing IP phones to be configured for internal and external calls within a specific location.

Methodology

The overall system is built using Cisco Packet Tracer, a proprietary multi-platform tool that allows for the creation of networking and IoT simulations without the need for hardware or an existing network. Each zone of the system includes a fire monitor and sensor nodes equipped with ceiling sprinklers, siren, temperature sensor, and smoke detector. These smart components are connected to a microcontroller and can be linked to the network by connecting the microcontroller to the Home Gateway wirelessly. The entire system is responsible for processing data and sending control signals to activate the notification devices, and data processing and monitoring can be accessed through the software.

Cisco Packet Tracer offers several advantages. First, it is easy to use, making it accessible to a wide range of users. Additionally, it can be accessed anywhere and anytime, providing flexibility and convenience to its users. Another advantage is its ability to simulate configurations related to Cisco devices, allowing users to test and troubleshoot network designs before implementing them in real-life scenarios. Moreover, it provides information-driven operation efficiencies that reduce inventory, downtime, and time to market. Finally, it offers a greater ability to support business evolution from a reliable, transparent technology foundation that is viable with future innovation discharges.

TABLE 1

Devices Used in the Network and their Function

DEVICE	FUNCTION / DESCRIPTION
Router 2811	Supports multiple WAN interfaces.
Switch 2960	Easy to deploy, manage, and troubleshoot. It offers automated software installation and port configuration.
IP Phone 7960	Full-feature telephones that provide voice communication over an IP (Internet Protocol) network.
Personal Computer (PC)	Connection to access layer
Laptop	
Tablet	Manipulating, storing, calling up information for the user in changed format if required.
Smartphones	
Server	Monitors intelligent things that are recorded on it and have specific database features.
Central Server	Used to link the router with the cellular network.
Cell Tower	Cellular-enabled mobile device site where antennas and electronic communications equipment are placed to create a cell in a cellular network.
Home Gateway	Allows data to flow from one discrete network to another.
Microcontroller (MCU-PT)	Used to connect various intelligent things.
Ceiling Sprinkler	Provides an appropriate amount of water to extinguish fires before they get the opportunity to grow and spread throughout the room.
Siren	Designed to sound the alert in the event of a fire-related emergency.
Lights	Visible lights
RFID Reader	Type of communication device that involves connection and communication between a transmitter (transponder or tag) and a receiver (reader).
Smoke Sensor	Used to detect smoke in a specific room, surroundings or area.
Temperature Sensor	Measures the temperature of its environment and converts the input data into electronic data to record, monitor, or signal temperature changes.

Table 1 presents a comprehensive overview of the devices utilized in a network configuration, along with their respective functions. The Router 2811 is specifically designed to support multiple WAN interfaces, enabling seamless and efficient network connectivity. In contrast, the Switch 2960 offers a user-friendly experience, allowing for easy deployment, management, and troubleshooting. It also boasts automated software installation and port configuration capabilities, streamlining operational processes.

The IP Phone 7960 is a sophisticated telecommunications device that facilitates voice communication over an IP network, offering a wide range of telephony features. Additionally, personal computers (PCs), laptops, tablets, and smartphones serve as versatile tools for accessing and manipulating information in various formats, tailored to individual user requirements.

Servers play a vital role as monitoring systems for intelligent devices, efficiently recording and storing data with specialized database features. The central server acts as a vital intermediary between the router and the cellular network, ensuring effective communication between the two.

Cell towers are indispensable components of cellular networks, housing antennas and communication equipment to establish reliable cellular coverage within specific areas. Home gateways are responsible for facilitating seamless data flow between discrete networks, ensuring uninterrupted connectivity. Microcontrollers (MCU-PT) play a pivotal role in establishing connections between diverse intelligent devices within the network infrastructure.

To enhance safety measures, ceiling sprinklers are employed to deliver an appropriate amount of water, effectively extinguishing fires and preventing their propagation throughout a room. Sirens are specifically designed to emit audible alerts during fire-related emergencies. Lights serve as visible indicators within the network, providing visual cues to users. RFID Readers facilitate communication between transmitters (tags) and receivers, enabling seamless data exchange. Smoke sensors are dedicated to detecting smoke within specific areas, while temperature sensors accurately measure the ambient temperature, converting this data into electronic format for monitoring, recording, or signaling temperature fluctuations.

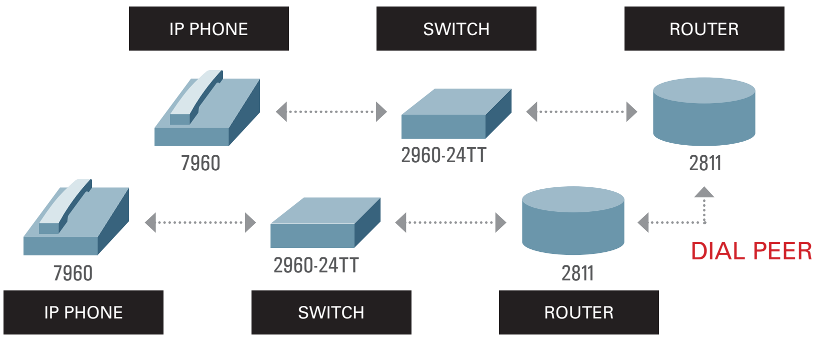
Design and Implementation

The proponents utilized the following devices as discussed in the methodology in implementing the design for the network system of IP Telephony, IoT, and FDAS. The implemented design and network diagram for this project will be shown in this section.

C.1. Block Diagram

FIGURE 1

IP Telephony Block Diagram



In Figure 1, the transmission of voice or audio signals between two specific IP Phones is depicted. The setup process involves several steps to ensure proper connectivity and secure data transmission.

To begin, VLANs are established by configuring the switch. This entails assigning VLANs, configuring interface ports, and enabling access to the designated VLANs. Concurrently, network assignments are configured on the router, with the inclusion of an encapsulation method to enhance security and data reliability. Additionally, configurations for telephony services and the assignment of IP Phone directories or numbers are implemented on the respective devices.

Once the network setup is complete, the router needs to be connected to the other router's network. This requires assigning an IP Address and Gateway to both routers. Static routing is then configured to enable mutual recognition of transmitted data. Finally, to enable voice communication and transmission within the network, dial-peer configurations are performed. This type of configuration directs calls to a specific network based on assigned destination patterns and session targets, ensuring efficient communication between the IP Phones.

By following these steps, a secure and reliable voice communication system can be established within the network, facilitating smooth and effective transmission of audio signals between the designated IP Phones.

FIGURE 2

FDAS Block Diagram

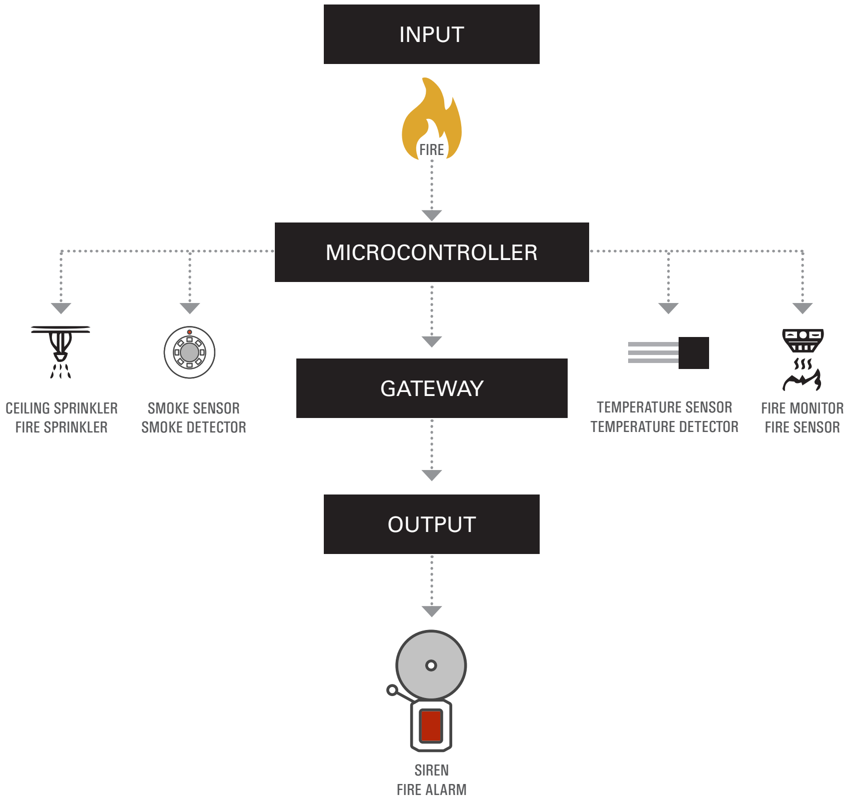


Figure 2 illustrates the block diagram of the Fire Detection and Alarm System (FDAS). In this configuration, devices such as the smoke sensor, temperature sensor, fire monitor, and ceiling sprinkler are interconnected with the MCU-PT Microcontroller. The control of these devices is facilitated through programming codes developed and compiled specifically for the MCU-PT Microcontroller. To establish connectivity with the Home Gateway, the proponents have incorporated a wireless module. This integration enables the IoT monitor to identify and communicate with the MCU-PT Microcontroller, as well as other connected home and industrial devices and appliances. Subsequently, specific conditions have been established and implemented to trigger the alarm siren and activate the ceiling sprinkler when a fire is detected by the sensors.

C.2. IP Addresses and Configurations

The network setup incorporates specific IP address configurations for the router, VLAN, microcontroller, and server. The router, serving as a central hub, is allocated a unique IP address within its respective Virtual Local Area Network (VLAN). This IP address enables the router to establish communication with other devices within the network, facilitating the seamless transfer of data between different VLANs.

Likewise, the microcontroller, playing a vital role in connecting various intelligent devices, is also assigned an IP address. This address allows the microcontroller to communicate with other devices within the network, ensuring efficient data transmission. By having an IP address, the microcontroller becomes an identifiable entity within the network architecture, enhancing its integration and functionality.

Similarly, the server, functioning as a monitoring system and housing critical data, is configured with its own IP address. This IP address facilitates connections between the server and other devices within the network, enabling the retrieval and transmission of data as required. It establishes a reliable communication channel between the server and other devices, ensuring effective data management and analysis.

In summary, the assignment of IP addresses to the router, VLAN, microcontroller, and server is fundamental for the proper configuration and optimal functioning of the network. It enables efficient communication and data exchange between these devices, thereby enhancing the overall functionality and reliability of the network infrastructure. The IP addresses of the mentioned devices are displayed in Tables 2, 3, 4, and 5.

TABLE 2

Router Interface

Router	Interface	IP Address	Subnet Mask
Main Bldg. 1	Eth 1/0	20.20.20.1	255.255.255.0
	Eth 1/1	10.10.10.1	255.255.255.0
Main Bldg. 2	Eth 1/0	10.10.10.2	255.255.255.0
	Eth 1/1	30.30.30.1	255.255.255.0
Annex	Eth 1/0	20.20.20.2	255.255.255.0
	Eth 1/1	30.30.30.2	255.255.255.0

TABLE 3

DATA and VOICE VLANs

VLAN	Main Bldg. 1	Main Bldg. 2	Annex
DATA	192.168.10.0	192.168.30.0	172.16.69.0
VOICE	192.168.20.0	192.168.40.0	172.16.96.0

TABLE 4

Servers

VLAN	Main Bldg. 1	Main Bldg. 2	Annex
Floor 3 Server 1	Fa 0	192.168.10.1	255.255.255.0
Floor 3 Server 2	Fa 0	192.168.10.1	255.255.255.0
Central Office Server	Fa 0/0 or backbone	162.69.0.2	255.255.255.0
	Cell Tower	172.16.1.1	255.255.255.0

TABLE 5

MCU-PT Microcontroller

Microcontroller	Gateway	DNS Server
1st Floor MCU-PT Microcontroller	192.168.25.1	0.0.0.0
2nd Floor MCU-PT Microcontroller	192.168.25.1	0.0.0.0
3rd Floor MCU-PT Microcontroller	192.168.25.1	0.0.0.0
4th Floor MCU-PT Microcontroller	192.168.25.1	0.0.0.0
5th Floor MCU-PT Microcontroller	192.168.25.1	0.0.0.0
Annex MCU-PT Microcontroller	192.168.25.1	0.0.0.0

C.3. Network Diagrams

FIGURE 3

Network Diagram of Floors 1, 2 and 3

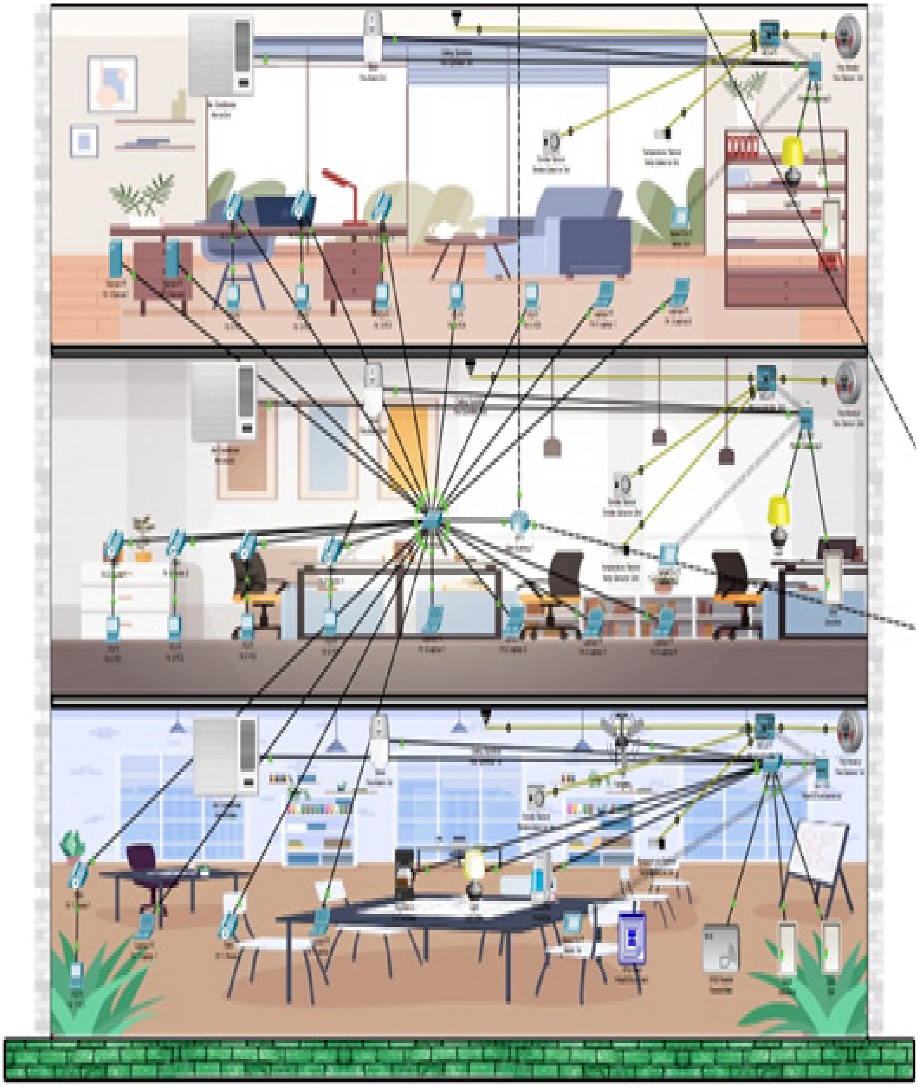
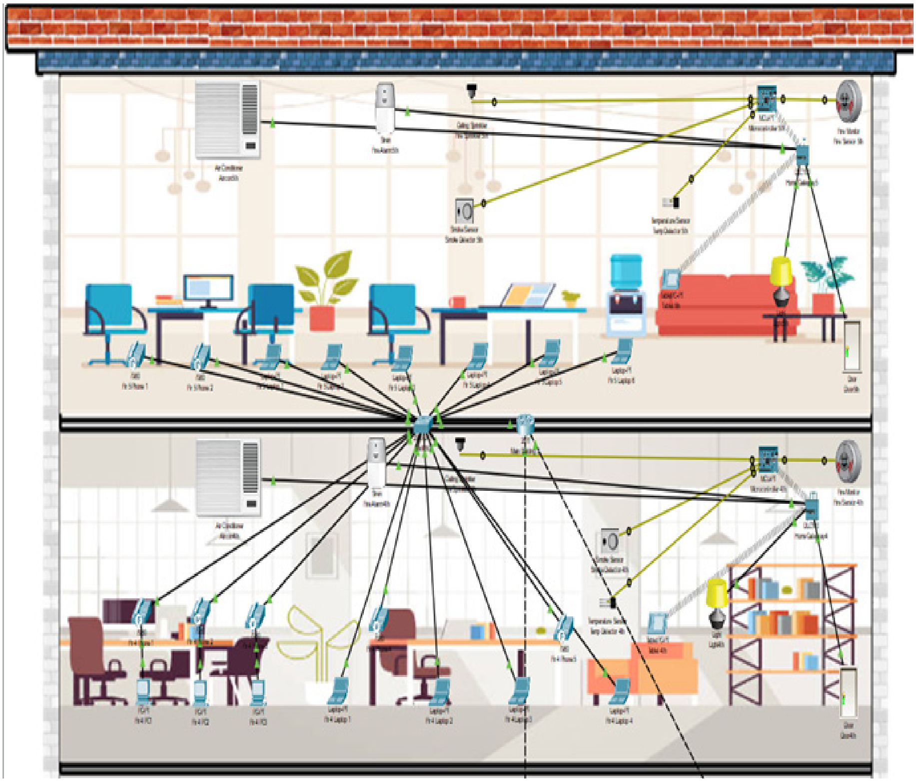


FIGURE 4

Network Diagram of Floors 4 and 5



The network system and diagram for the main building, shown in Figures 3 and 4, incorporate the use of two routers across different floors. Specifically, Main Building-1 (Router) is assigned to floors 1, 2, and 3, while Main Building-2 (Router) is designated for floors 4 and 5. The router configuration remains mostly consistent per floor, differing only in terms of VLAN settings and IP Phone assignments.

Within each floor, there is a Home Gateway and an MCU-PT Microcontroller responsible for facilitating communication among various devices in the IoT and FDAS network. These devices include sirens, lights, sprinklers, smoke sensors, coffee maker, fans, humidifier, doors, air conditioners, temperature sensors, fire monitors, RFID readers, RFID Cards, Smartphones, and tablets.

Additionally, the IP Telephony network involves devices such as IP Phones, routers, PCs, laptops, and switches. Each floor is equipped with a specific set of devices connected to a switch, aligning with the corresponding range of the router.

FIGURE 5

Network Diagram of the Annex Building

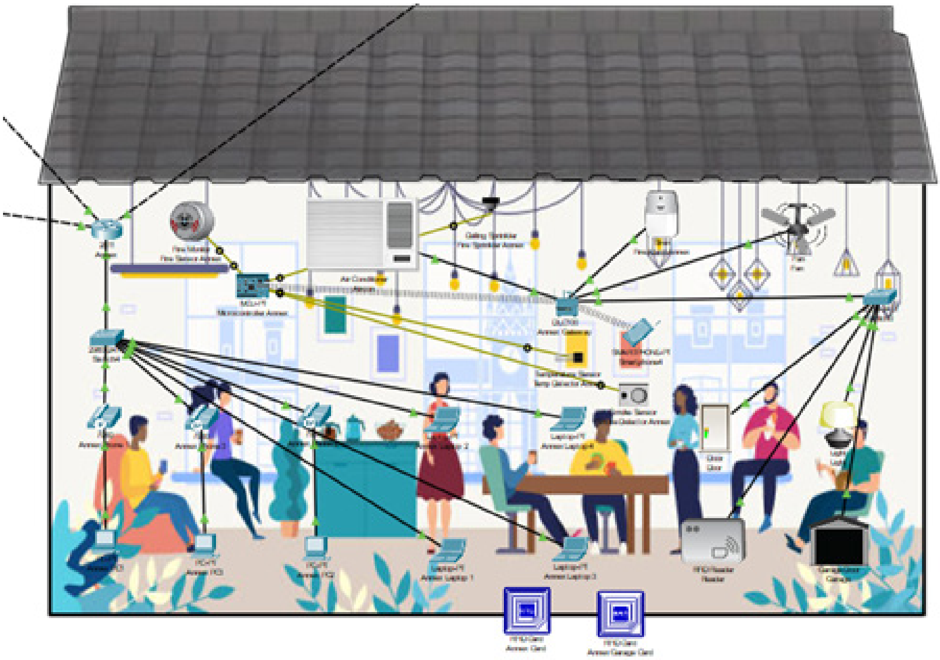
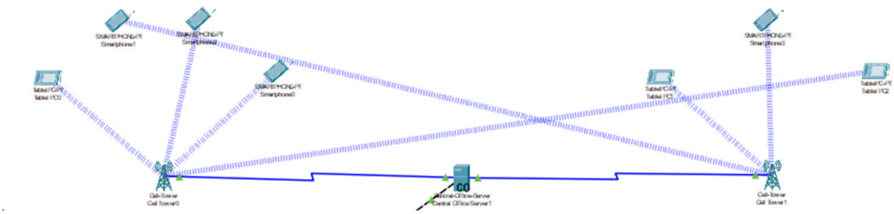


FIGURE 6

Network Diagram of the Cell Towers



For the creation of the network system and diagram in Annex as shown in Figure 5, a single router is utilized to serve the entire building, with the Annex's Router connected to a Central Office Server. The configuration of the router in Annex shares similarities with the routers in the Main Building, differing primarily in terms of VLANs, Network Address, and assignment of IP Telephone numbers. In addition, the building is equipped with a Home Gateway and an MCU-PT Microcontroller, facilitating communication among devices within the IoT and FDAS network.

Moreover, the IP Telephony network involves various devices such as IP Phones, Routers, PCs, Laptops, and Switches. Additionally, the Central Office Server is connected not only to the Annex's Router but also to two cell towers located outside the building shown in Figure 6.

Conclusion and Recommendations

In this study, the researchers successfully integrated IP Telephony, FDAS, and IoT networks to develop a Smart Building concept. This concept encompasses various functions and services, all defined with hardware compatibility. The system not only accurately portrays a real-life scenario of an advanced building, but it also demonstrates the IP Telephony concept, enabling voice communication both within and outside the establishment.

The simulation conducted in this study was error-free, and it is recommended to load or open the PKT file a few minutes after the simulation to allow the devices to load the necessary IP and network configurations. The materials and devices used in the study are readily available in the market, ensuring the model's sustainability and feasibility. Consequently, the model or design created using Cisco Packet Tracer exhibits similar results and functionality to real-life IP Telephony, IoT, and FDAS implementations.

It is highly recommended that future researchers and practitioners explore the potential of integrating IP Telephony, FDAS, and IoT networks to implement the Smart Building concept. The successful integration showcased in this study not only provides an accurate representation of an advanced building but also highlights the practicality and effectiveness of IP Telephony for seamless voice communication.

References

A. Bröring, J. E. (2011). *New Generation Sensor Web Enablement. Sensors, 1, 48.*

Anwar, F. B. (2018). *A Real-Time Integrated Fire Detection and Alarm System for Network Based Building Automation. Indian Journal Science and Technology, 1.*

L. Huang, H. C. (2011). *A ZigBee-based monitoring and protection system for building electrical safety. Elsevier, 9.*

Shu-guang, M. (2011). *Construction of Wireless Fire Alarm System Based on ZigBee Technology. Engineering Procedia, 1, 6.*

ABOUT THE AUTHORS:

Engr. Jaime V. David is a graduate of BS in Electronics Engineering from UE – Caloocan (1991) and is currently a Part-time Instructor at the School of Engineering at NU-NU-Asia Pacific College (Corresponding author: jigsd@apc.edu.ph).

Engr. Luigi Carlo De Jesus is a graduate of BS in Electronics Engineering from FEU – East Asia College (2013) and Master of Engineering major in Computer Engineering from NU-Asia Pacific College (2021). He is the current Engineering and Science Laboratory Office (ESLO) Head of NU-Asia Pacific College - School of Engineering (E-mail: luigid@apc.edu.ph).

Engr. Leonardo M. Samaniego Jr. holds an Electronics Engineer license. He also holds a Master of Engineering degree with a major in Electronics Engineering from MAPUA Institute of Technology. He is currently the Executive Director of NU-Asia Pacific College's School of Engineering (E-mail: leonardojrs@apc.edu.ph).

Mark Joshua A. Añonuevo is a graduate of NU-Asia Pacific College, holding a Bachelor's degree in Electronics Engineering. With a strong foundation in electronic systems and a passion for innovation, he is eager to apply his technical expertise and contribute to the advancement of the field (E-mail: maanonuevo@student.apc.edu.ph).

Joshua D. Bernados is a graduate of NU-Asia Pacific College, having earned a Bachelor's degree in Electronics Engineering. Equipped with comprehensive knowledge of electronic systems and a penchant for problem-solving, he is poised to make significant contributions in the field of technology (E-mail: jdbernados@student.apc.edu.ph)

Julius Iver A. Reyes is a dedicated student pursuing a Bachelor's degree in Electronics Engineering at NU-Asia Pacific College. With a strong passion for technology and a curious mindset, he consistently seeks opportunities to expand his knowledge and practical skills in the field (E-mail: jareyes@student.apc.edu.ph).

Joshua Rivera is a graduate of NU-Asia Pacific College, having successfully earned a Bachelor's degree in Electronics Engineering. With a strong technical background and a passion for innovation, he is poised to make significant contributions in the field and tackle complex engineering challenges (E-mail: jdrivera@student.apc.edu.ph).

Janine Via Tubon is a graduate of NU-Asia Pacific College, holding a Bachelor's degree in Electronics Engineering. With a solid foundation in electronic systems and a drive for continuous learning, she is prepared to excel in the field and contribute to technological advancements (E-mail: jmtubon2@student.apc.edu.ph).