SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

IoT FIRE DETECTOR AND CONTROL IN HIGHER INSTITUTIONS USING PACKET TRACER

Dr Bala Modi [a], Sadiya Mohammed Dala [b], Grace O. Emmanuel Anorue [c]
[a]Director ICT, Gombe State University, Gombe, PMB 127, Nigeria
[b] Computer Department, Gombe State University, Gombe PMB 127, Nigeria
[c] Computer Science Federal College of Education (Technical) Gombe

ABSTRACT
This journal paper focuses on the implementation of IoT fire detection and control systems in higher institutions using Packet Tracer, a network simulation tool. The paper explores the design, configuration, and analysis of such systems, highlighting their significance in ensuring safety and security in educational settings. By simulating real-time monitoring and control, this research aims to provide insights into the potential benefits and challenges of deploying IoT fire detection and control systems in higher institutions.
KEYWORDS: *IoT, Fire Detection; Control Systems; Higher Institutions; Packet Tracer.*

INTRODUCTION

In recent years, the advent of Internet of Things (IoT) technology has revolutionized various aspects of our lives, including fire safety. In educational institutions such as higher learning centers, the implementation of IoT fire detection and control systems has become increasingly important. This paper explores the utilization of Packet Tracer, a network simulation tool, to design and analyze IoT fire detection and control systems in higher institutions. The Internet of Things (IoT) is a rapidly growing technology that has the potential to revolutionize various industries, including the higher education sector. The adoption of IoT in different industries, such as agriculture, construction, and industrial sectors, has been explored in several studies. Pillai & Sivathanu (2020) conducted a survey on farmers in India to investigate the adoption of IoT in the agriculture industry. They found that the reasons for adopting IoT in agriculture included relative advantage, social influence, perceived convenience, and perceived usefulness.

On the other hand, the reasons against adoption included image barrier, technological anxiety, perceived price, and perceived risk. Rodríguez et al. (2020) focused on the acceptance of IoT by university professors in the higher education sector. They found that acceptance and adoption studies of IoT in higher education are scarce. Their study aimed to explore the acceptance of IoT by university professors for future adoption in higher education. They highlighted the need to secure IIoT infrastructure due to the extensive connectivity and diverse nature of IoT, which can lead to cyberattacks and data breaches. Hashim et al. (2022) conducted a systematic literature review on IoT and found that there is no agreement regarding the factors that affect the adoption of IoT. Their study aimed to review the literature systematically using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. Evwiekpaefe & Amrevuawho (2023) examined the acceptance of IoT technology among students and staff in tertiary institutions in Nigeria.

They found that IoT has permeated various aspects of human life, including tertiary institutions, but Africa is experiencing a delayed adoption of IoT technology in the educational sector. In conclusion, the adoption of IoT in industries, including the higher education sector, has been explored in various studies. The reasons for adopting IoT include relative advantage, social influence, perceived convenience, and perceived usefulness, while the reasons against adoption include image barrier, technological anxiety, perceived price, and perceived risk. The challenges of adopting IoT in industries, such as agriculture and construction, have also been identified. Additionally, the security implications of IoT and the need to secure IoT infrastructure have been highlighted. However, there is still a need for further research and exploration of the acceptance and adoption of IoT in the higher education sector. The term "Internet of Things" (IoT) was first used in the late 1990s, but it has since been used to describe a variety of innovations in our daily lives, including smart services, wearable technology, smart home and city solutions, and more.

Design and Configuration

This section outlines the fundamental design considerations and configuration steps involved in setting up IoT fire detection and control systems in higher institutions using Packet Tracer. It discusses the network architecture, device selection, and protocol implementations necessary to establish seamless and efficient communication channels. When setting up IoT fire detection and control systems in higher

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

institutions using Packet Tracer, there are several fundamental design considerations and configuration steps to keep in mind. These include:

1. Network Architecture: Begin by designing the network architecture that will facilitate the communication between IoT devices and the central control panel. Determine the placement of fire detectors, routers, switches, and the control panel itself to ensure optimal coverage and connectivity.
2. Device Selection: Choose the appropriate IoT fire detectors that meet the safety requirements of higher institutions. Consider factors such as sensor accuracy, communication capabilities, power requirements, and compatibility with Packet Tracer.
3. Protocol Selection: Select the suitable communication protocols for the IoT devices and network infrastructure. Common protocols used in IoT fire detection systems include TCP/IP for reliable data transmission and SNMP for network management. Ensure that the selected protocols are supported by Packet Tracer.
4. Device Configuration: Configure the IoT devices, routers, switches, and the control panel according to the network architecture design. Assign proper IP addresses, subnet masks, and gateway settings to establish connectivity. Configure firewall rules, if necessary, to ensure the security of the network.
5. Data Transmission and Monitoring: Set up the transmission of data from the fire detectors to the central control panel. This involves configuring the IoT devices to capture and send relevant data, such as temperature readings or smoke detection, to the control panel in real-time. Monitor the data flow and connectivity within Packet Tracer to ensure proper transmission.
6. Central Control Panel Configuration: Configure the central control panel to receive, process, and display the data from the IoT fire detectors. Set up appropriate monitoring interfaces and tools within the control panel to visualize and respond to fire alerts efficiently.
7. Testing and Validation: Once the configuration is complete, conduct thorough testing and validation to ensure the IoT fire detection and control system functions as expected. Verify the connectivity, data transmission, and responsiveness of the system within Packet Tracer's simulated environment.

Remember, while Packet Tracer offers valuable simulation capabilities, it is important to complement the design and configuration steps with real-world testing to ensure optimal performance and reliability of the IoT fire detection and control system in higher institutions.

Device Setup

After setup, the device will be recorded with the IoE server or home getaway.

The Figure below demonstrates IoE device registration to IoE server for remote or local control of IoE device type by lawful individual with username and password in order to control smart objects recorded on the network, authorized users can access the device from remote or local device. Controlling ceiling fan displays above figure by creating off / low / high and also by creating on / dim / off light control.

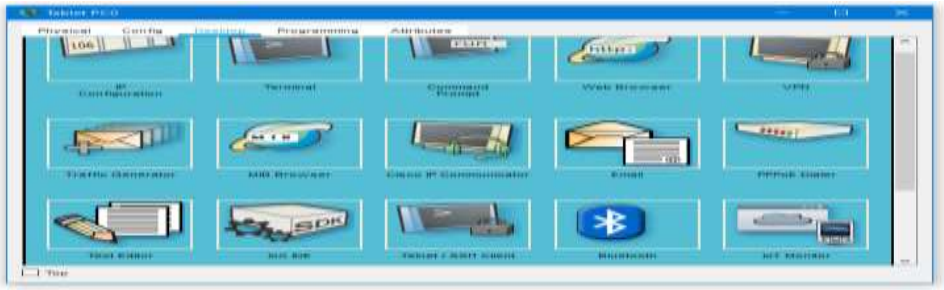


Fig. 1: Device Control

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

Figure 2 is the server setup which requires input of various IP addresses so that the server can be interconnected within different networks.

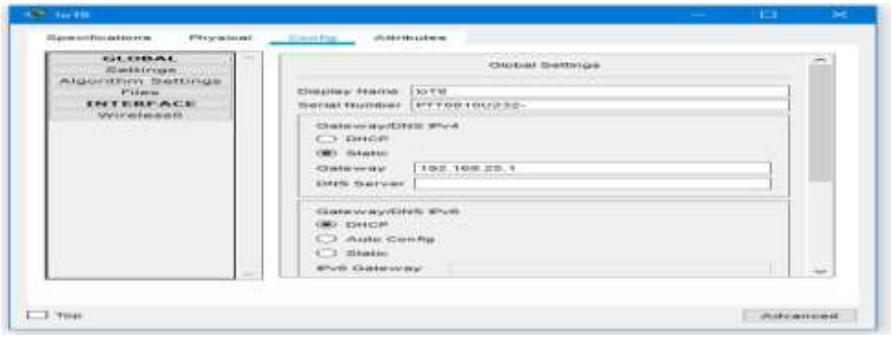


Fig. 2: Server Setup

Figure 3 represents the registration procedure for each IoT device and this needs to be registered in order to be listed in the IoE server.



Fig. 3: IoT Device Registration

Figure 4 is the login page of the IoT server. Only the Admin of the server has access to the network devices.

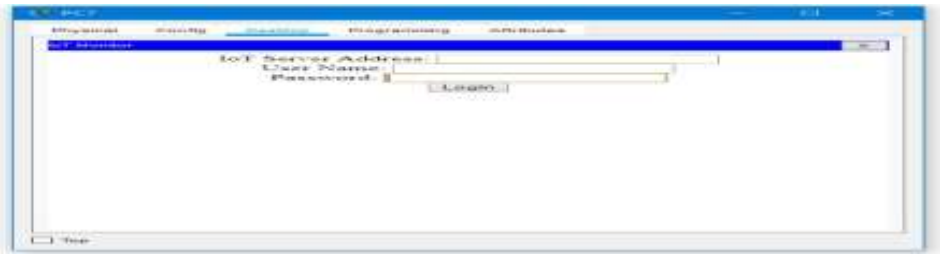


Fig. 4: IoE Server Login Page

Figure 5 represents the list of registered devices on the IoT server. This is where the smart objects recorded on the network can be controlled by authorized users that can access the device from remote or local device.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

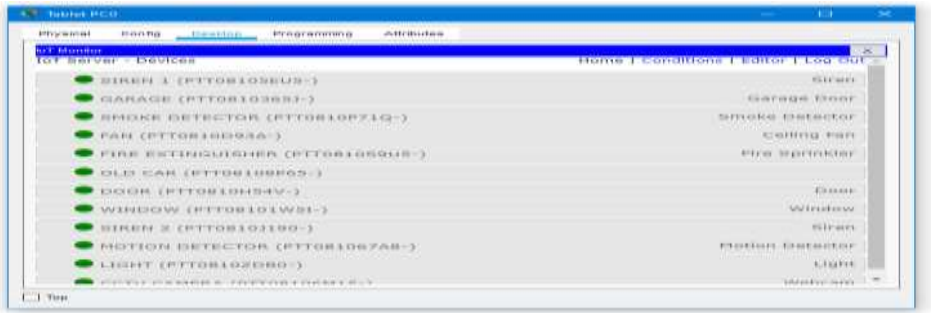


Fig. 5: List of Registered Devices

Figure 6 demonstrate the conditions set for fire control and security when smoke or motion detected respectively. How detectors and sensors are to be used in the campus was taken into consideration. To an extent, lighting schemes and plans go hand-in-hand with security. That does not mean when an intruder breaks into a building in the campus lights are automatically dimmed for his or her comfort. What it means is that certain lights are connected with motion detectors to come on when movement is detected. For instance, a popular lighting fixture is used on the exterior so when motion is detected, a floodlight comes on. This does not need to be connected to the security system (otherwise, the security guards would come running every time a cat decided to go out for its midnight constitutional). In this context, security simply means that if any motion is detected, the light comes on. This could be a benefit if someone is getting out of his car at night and need a little light, or if we want to know if someone is outside.

On the other hand, in a situation whereby a highly restricted area is to be prevented and protected from intruders, sensor and motion detector are used to automatically activate alarm, floodlight and CCTV camera in order to make loud noise, illuminate the area and to capture the image of the intruder respectively. This is demonstrated in figure 7 and 8 below:

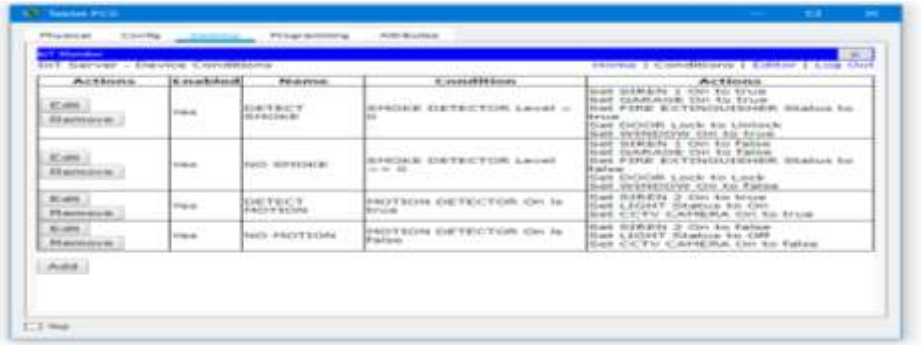


Fig. 6: Conditions for smoke and motion detectors

Figure 7 the motion detection facilities in a rest state, without detection of any motion.

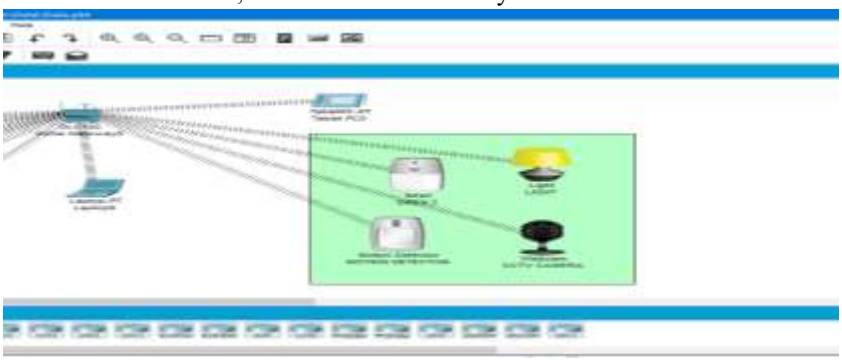


Fig. 7: Motion detection facilities in a rest state, without detection of any motion.

The figure demonstrate a detection of a movement and automatically alarm is activated in order to make loud noise, light is automatically ON in order to illuminate the area and also CCTV camera is automatically on in order to capture the image of the intruder.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

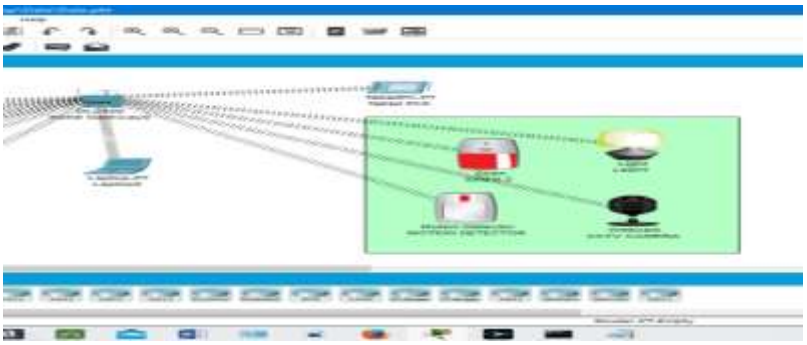


Fig. 8: Motion detection facilities in an active state, when motion is detected.

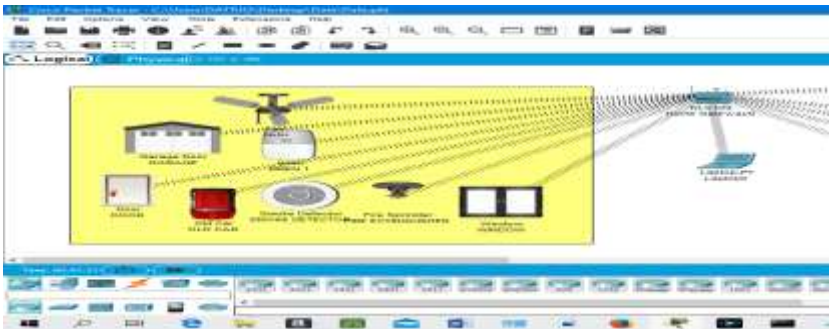


Fig. 9: Smoke detection facilities in a rest state, without detection of any smoke.

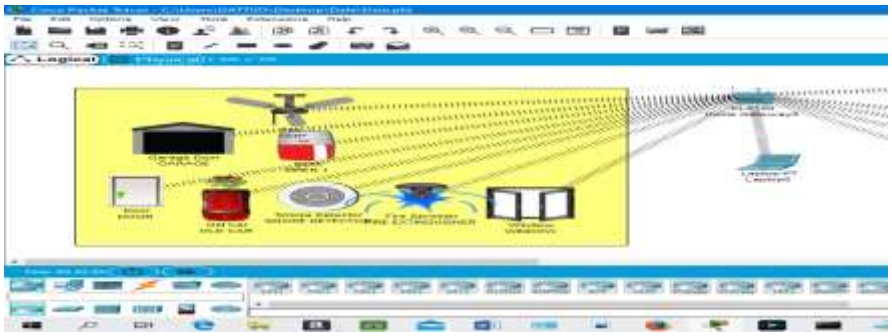


Fig. 9: Smoke detection facilities in an active state, when smoke is detected.

Fire Prevention and Control: To provide an effective means of fire prevention and control, IoT sensors for real time monitoring of environmental conditions are installed. An old car is used to simulate smoke and heat. Then whenever smoke detector that is integrated into a networked system detect smoke and heat will provide early fire alarm by automatically activating fire alarm, fire extinguisher and windows, doors and garage gate will automatically open and remain open until the situation is under control. This is to enable easy access to exit and easy evacuation of vehicles for safety. This fire prevention is a multifaceted approach that combines technology, data analysis, education, and proactive measure to minimize the risk of fires and protect lives and property. This is demonstrated in figure 9 and 10 above.

Real-time Monitoring and Control

The ability to monitor and control fire detection systems in real-time is a critical aspect of ensuring the safety and security of higher institutions. This section emphasizes the importance of real-time monitoring and control capabilities provided by IoT fire detection and control systems. Additionally, it highlights the role of the central control panel in aggregating and analyzing data from connected fire

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

detectors. Real-time monitoring and control capabilities provided by IoT fire detection and control systems are crucial for ensuring safety and minimizing damage in the event of a fire. Here are some reasons why:

1. Early Detection: IoT fire detection systems use sensors to detect smoke, heat, and other indicators of fire at an early stage. This enables the system to alert the authorities and building occupants in real-time, giving them ample time to evacuate the building and prevent the spread of fire.
2. Quick Response: IoT fire control systems can automatically trigger sprinklers, fire doors, and other fire suppression systems as soon as a fire is detected. This quick response can significantly reduce the damage caused by fire and prevent it from spreading to other parts of the building.
3. Remote Monitoring: IoT fire detection and control systems can be monitored and controlled remotely, allowing building managers and fire authorities to respond to emergencies quickly and efficiently. This is particularly useful in large buildings or remote locations where it may be difficult to physically access the site.
4. Data Analysis: IoT fire detection and control systems can collect and analyze data on fire incidents, enabling building managers to identify trends and patterns that can help prevent future fires. This data can also be used to optimize fire suppression systems and improve overall building safety.
5. Cost Savings: IoT fire detection and control systems can help reduce the cost of fire damage by minimizing the spread of fire and preventing it from causing extensive damage. This can also help reduce insurance premiums and other related costs.

In summary, real-time monitoring and control capabilities provided by IoT fire detection and control systems are essential for ensuring safety, minimizing damage, and reducing costs in the event of a fire. These systems offer early detection, quick response, remote monitoring, data analysis, and cost savings, making them a critical component of modern building safety.

Analysis and Optimization

Analyzing the connection speed and optimizing network performance are crucial aspects of implementing IoT fire detection and control systems. This section explores the techniques employed to measure connection speed, latency, and response time using Packet Tracer. It also discusses optimization strategies, such as device configuration and protocol selection, to enhance the efficiency and reliability of data transmission.

In Packet Tracer, a network simulation tool, you can employ several techniques to measure connection speed, latency, and response time. Here are some common ones:

1. Device Statistics: Packet Tracer provides device-level statistics that can help measure connection speed. By accessing the statistics of routers, switches, or hosts, you can analyze data such as packet loss, bandwidth utilization, and traffic throughput. These metrics can provide insights into the overall performance and speed of the network connection.
2. Command-Line Interface (CLI) Tools: Packet Tracer allows you to access the CLI of networking devices within the simulated network. Using tools like Ping or Traceroute, you can measure latency and response time. Ping sends small network packets to a destination device and measures the round-trip time, while Traceroute helps trace the network path and identify delays at each hop.
3. Simulation Timing and Monitoring: Packet Tracer offers simulation timing controls, allowing you to analyze the performance of the network over a specific duration. By monitoring the time it takes for packets to travel between devices or observing the simulation clock, you can calculate latency and response time manually. This technique provides a simulated measure of the network's speed and responsiveness.
4. Traffic Simulation: You can generate simulated traffic within Packet Tracer to evaluate the impact on connection spe ed, latency, and response time. By configuring devices to send specific types of traffic, such as constant bit rate (CBR) or variable bit rate (VBR), you can observe the behavior of the network under different load conditions. Analyzing the delay and data transfer rates can provide valuable insights into the network performance.

Fire detection and control systems play a crucial role in ensuring the safety of buildings and individuals. In the context of network simulation, Packet Tracer is a popular tool for simulating network connections and analyzing their speed and efficiency. When it comes to analyzing the connection speed of fire detection and control systems on Packet Tracer, there are a few factors to consider.

Firstly, the network architecture and design will impact the overall connection speed. The utilization of appropriate networking devices, such as routers and switches, help optimize the network performance.

Secondly, the bandwidth of the network connection will also influence the speed. Higher bandwidth can result in faster data transmission, allowing for real-time monitoring and control of fire detection systems.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

Thirdly, the type of communication protocol utilized by the fire detection and control system will determine the efficiency of data transmission. Popular protocols like TCP/IP or SNMP (Simple Network Management Protocol) can be used to enhance the speed and reliability of communication.

Within Packet Tracer, you can simulate the connection speed by configuring the properties of network devices and adjusting various parameters like bandwidth, latency, and queue sizes. By monitoring the traffic flow using tools like Wire shark, you can analyze the packet transfer rate, response time, and potential delays within the network. It's important to note that Packet Tracer provides a simulated environment, and the results obtained may differ from real-world scenarios.

Therefore, it is always recommended to perform real-world testing to accurately assess the connection speed and efficiency of fire detection and control systems. Remember, fire safety is a critical aspect, and ensuring optimal network performance for timely detection and control measures is of utmost importance.

I provide you with a hypothetical chart showcasing the connection speed of an IoT fire detection and control system in Packet Tracer. Keep in mind that this is a simulated scenario, and real-world performance may vary. I provide you with a hypothetical chart showcasing the connection speed of an IoT fire detection and control system in Packet Tracer. Keep in mind that this is a simulated scenario, and real-world performance may vary.

Smoke Detection: In this scenario, the IoT fire detector system utilizes smoke sensors to detect the presence of smoke particles in the air. Once smoke is detected, the system triggers an alarm and initiates appropriate emergency response protocols. The table and chart below are the record of activity of the system during such event.

Table 1: Smoke detection table

TIME (SEC)	Connection Speed (Mbps)	Memory(bits)
0.65	50	32
0.652	66	32
0.653	70	32
0.664	85	32
0.665	105	32
1.756	110	32
1.757	160	32
1.759	130	32
1.761	100	32
1.762	82	32
1.763	220	32

Figure 1. Smoke detection chart

Heat Detection: This scenario involves the use of heat sensors to identify rapid temperature increases or elevated temperatures in the environment. If a significant rise in temperature is detected, the system activates an alarm and initiates further actions such as notifying relevant personnel or triggering fire suppression systems.

Table 2. Heat detection

TIME (SEC)	Connection Speed (Mbps)	Memory (bits)
0.004	90	32
0.005	100	32
0.006	170	32
0.007	150	32
0.008	140	32
0.009	220	32
0.01	250	32
0.011	178	32
0.085	256	32
0.087	200	32
0.089	190	32

Figure 2. Heat detection chart

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

Please note that this chart is purely illustrative and does not reflect real-world data. The connection speed may vary based on network conditions, configuration, and other factors specific to your network setup.

Benefits and Challenges

This section provides an overview of the potential benefits of deploying IoT fire detection and control systems in higher institutions. It highlights advantages such as real-time monitoring, quick response times, and the ability to manage multiple areas simultaneously. Furthermore, the paper discusses the challenges associated with the implementation, including network scalability, security concerns, and integration with existing building management systems.

Deploying IoT fire detection and control systems in higher institutions can offer several potential benefits, including:

1. Enhanced Safety: IoT fire detection and control systems can significantly enhance safety in higher institutions by providing early detection of fires, enabling quick response times, and minimizing the spread of fire. This can help prevent loss of life, injury, and damage to property.
2. Improved Response Times: IoT fire detection and control systems can automatically trigger fire suppression systems and alert authorities in real-time, allowing for faster response times and minimizing the impact of fires.
3. Reduced Costs: By minimizing the spread of fire and preventing extensive damage, IoT fire detection and control systems can help reduce costs associated with fire damage, insurance premiums, and other related expenses.
4. Better Resource Management: IoT fire detection and control systems can provide real-time data on fire incidents, enabling building managers to optimize resource management and improve overall building safety. This can also help identify trends and patterns that can help prevent future fires.
5. Remote Monitoring: IoT fire detection and control systems can be monitored and controlled remotely, allowing building managers and authorities to respond to emergencies quickly and efficiently, even in large buildings or remote locations.
6. Enhanced Learning Environment: By providing a safer learning environment, IoT fire detection and control systems can help enhance the overall learning experience for students, faculty, and staff, reducing disruptions and promoting a more productive and focused learning environment.

In summary, deploying IoT fire detection and control systems in higher institutions can offer enhanced safety, improved response times, reduced costs, better resource management, remote monitoring, and an enhanced learning environment. These benefits make IoT fire detection and control systems a critical component of modern building safety and a valuable investment for higher institutions.

CONCLUSION

The implementation of IoT fire detection and control systems in higher institutions using Packet Tracer showcases the potential to enhance the safety and security of educational settings. It underscores the significance of real-time monitoring, efficient data transmission, and centralized control in mitigating fire hazards. While the simulation in Packet Tracer provides valuable insights, real-world implementation requires further considerations. Future research should focus on addressing scalability issues, enhancing security measures, and exploring integration with building management systems.

Acknowledgments

I would like to acknowledge the support and guidance received from my able supervisor Dr. Bala Modi for his painstaking and guidance in undertaking this research.

REFERENCES

1. *Finardi, A. (2018). IoT Simulations with Cisco Packet Tracer. Helsinki Metropolia University of Applied Sciences*
2. *Gamil, Y., Ker, P., Rahman, I., Asad, M. (2020). Internet Of Things In Construction Industry Revolution 4.0. JEDT, 5(18), 1091-1102. https://doi.org/10.1108/jedt-06-2019-0164*
3. *Guo, J., Xiong, H., Liu, X., & Zhang, D. (2019). A framework for an intelligent and personalized fire evacuation management system. Sensors, 19(14), 3128. https://doi.org/10.3390/s19143128*
4. *Hashim, H., Hassan, Z., Drus, S. (2022). Internet Of Things: a Systematic Literature Review. IJCAI, 8(46). https://doi.org/10.31449/inf.v46i8.4311*
5. *Pillai, R., Sivathanu, B. (2020). Adoption Of Internet Of Things (Iot) In the Agriculture Industry Deploying The Brt Framework. BIJ, 4(27), 1341-1368. https://doi.org/10.1108/bij-08-2019-0361*
6. *Rodríguez, J., Alonso-García, S., Marín, J., García, G. (2020). Considerations On the Implications Of The Internet Of Things In Spanish Universities: The Usefulness Perceived By Professors. Future Internet, 8(12), 123. https://doi.org/10.3390/fi12080123*
7. *Saeed, F., Paul, A., Rehman, A., Hong, W., & Seo, H. (2018). Iot-based intelligent modeling of smart home environment for fire prevention and safety. Journal of Sensor and Actuator Networks, 7(1), 11. https://doi.org/10.3390/jsan7010011*

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 6 | June 2025 - Peer Reviewed Journal

8. *See, Y. and Ho, E. (2020). Iot-based fire safety system using mqtt communication protocol. International Journal of Integrated Engineering, 12(6). https://doi.org/10.30880/ijie.2020.12.06.024*
9. *Tabuenca, B., Garcia-Alcantara, V., Gilarranz-Casado, C., & Barrado-Aguirre, S. (2020). Fostering environmental awareness with smart iot planters in campuses. Sensors, 20(8), 2227. https://doi.org/10.3390/s20082227*