Smart Security Framework for Educational Institutions Using Internet of Things (IoT)

DINESH A
Amrita Vishwa Vidyapeetham
Coimbatore
cb.en.u4cce20019@cb.students.amrita.edu

HARIVIYAAS B
Amrita Vishwa Vidyapeetham
Coimbatore
cb.en.u4cce20023@cb.students.amrita.edu

MALAVIKA MENON T
Amrita Vishwa Vidyapeetham
Coimbatore
cb.en.u4cce20031@cb.students.amrita.edu

MANOJ PARTHIBAN
Amrita Vishwa Vidyapeetham
Coimbatore
cb.en.u4cce20032@cb.students.amrita.edu

***Abstract* — An Internet of Things (IoT) smart security framework for educational institutions is a system that uses IoT devices and sensors to enhance security and safety in schools. This framework can include a variety of IoT devices, such as smart cameras, door and window sensors, and wearable devices for students and staff. These devices can be connected to a central network and used to monitor the premises, detect potential security threats, and alert authorities in the event of an emergency. The framework can also include features such as access control, whereby only authorized personnel are able to enter certain areas of the school. This can be achieved through the use of smart card readers or biometric scanners. Additionally, the framework can incorporate analytics and machine learning algorithms to identify patterns and anomalies in the data collected by the IoT devices, helping to detect potential security threats before they occur. Overall, a smart security framework using IoT technology can help educational institutions to improve safety and security on their premises, and provide a more secure learning environment for students and staff.**

Keywords — framework, anomalies, Internet of things, smart security framework.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we think about security and has provided numerous benefits to educational institutions. However, it has also introduced new security challenges that need to be addressed in order to ensure the safety and privacy of students and faculty. One way to address these challenges is through the use of a smart security framework. This framework utilizes the capabilities of IoT to create a more comprehensive and proactive approach to security. It involves the integration of various sensors and devices, such as cameras and access control systems, to monitor and secure the physical and digital aspects of an educational institution.

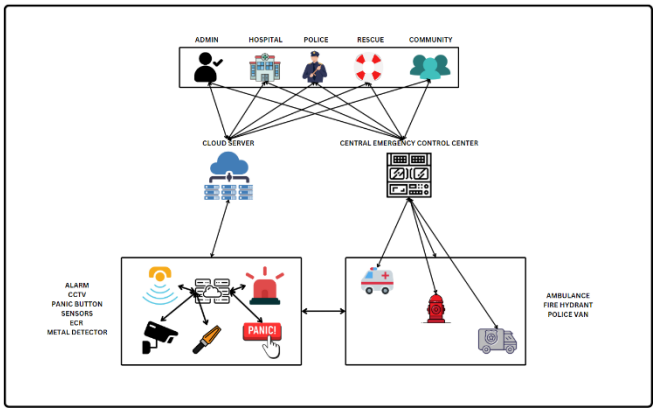
The smart security framework also utilizes advanced analytics and networking protocols to detect and respond to potential threats in real-time. It can identify patterns and anomalies that may indicate a security breach or other problem, and alert the appropriate personnel to take action. Additionally, the smart security framework can be customized to meet the specific needs of each educational institution. This allows for a tailored approach to security that addresses the unique vulnerabilities and risks faced by each institution.

Overall, the smart security framework using IoT is a powerful tool that can help educational institutions maintain a safe and secure environment for their students and faculty. It allows for a proactive approach to security that helps prevent potential threats and ensures the privacy and security of all stakeholders.

A. The main contribution of this paper

- To create an SSF for educational institutions in order to promptly alert the concerned departments in order to oppose or limit the calamity.
- To remotely monitor and operate sensors and security equipment during normal or operating circumstances in order to have complete control over them at any time and from any location. Not only can they be monitored, but they can also be remotely programmed and configured.
- Collecting and evaluating data from all sensors and security systems in order to make sound judgements during an emergency or in unusual circumstances.

B. *The Smart Security Framework (SSF)*



In this SSF proposal, Different types of sensors, threat intelligence detectors, and security cameras are utilized in the proposed SSF. These units are linked to the Emergency Control Room (ECR) using cable and wireless technology, and the Central Emergency Control Center (CECC). In an emergency, the suggested technology promptly alerts the concerned and begins broadcasting all sensors and security cameras to ECR. The panic button on the smart watch is used to manually activate the SSF.

SSF collects data from all installed security devices using a variety of methods. These algorithms assist in categorizing the alarm. With live broadcasting, an alert is sent to the concerned departments. The CECC serves as the region's focal point. Members of CECC come from the police, fire, and ambulance services. On monitoring panels, live updates and the nature of the assault are provided. To make wise judgements, all top stack holders supervise and supervise the operation from that center.

All the stacks of sensors and actuators, Routers switching devices, Access points, L2 devices, Monitors, smartphone, tablet laptops, etc. are implemented using Cisco Packet Tracer which is a simulation tool used in networking.

II. System Model

SSF makes use of IoT, fog, and cloud ideas. IoT devices detect their surroundings. This data is then sent to fog cloud servers. When there are warnings or requests, they are sent to cloud centres. Higher authorities make choices based on sensor data. The quality of decisions and operations is dependent on the quality of sensing and conveying data to control centres. In this part, we assessed how well the proposed framework worked. Combining IoT into safety and emergency alerting methods might be quite beneficial. The SSF is implemented using a variety of sensors. All of the sensors are always operational and connected to the internet.

A. *Smart sensor board*

A Smart Sensor Board is a circuit board that contains many sorts of sensors. Pressure, temperature, humidity, smoke, motion, fires, and high-sensitivity speech sensors are all included on every sensor board. Embedded technology is used in smart boards. Algorithms are employed to send data to the ECR and the CECC. Other smart security solutions employed include smart metal detectors, smart walk-through gates, smart alarm systems, and security cameras.

B. *Sensors*

1) *Temperature sensor*

The temperature changes when there are flames, shooting, or explosions. This fluctuation is used to classify the warning and establish its cause. If the temperature exceeds the initial threshold value, ECR is notified. The CECC receives an emergency notice if the temperature rises after passing over the second threshold point. The temperature information is presented continually on the ECR display board.

2) *Vibration/wind sensor*

A powerful wave force is produced by firing or explosion. The smart board's vibration sensors detect any form of vibration in the walls. The "x" and "y" vibrations are easily identified and classified as to what object has struck the wall. This vibration assists the CECC staff in classifying the sort of alarm. If the vibration exceeds the first level, an alarm is issued to ECR, and if it exceeds the second threshold, CECC is contacted.

3) *Light sensor*

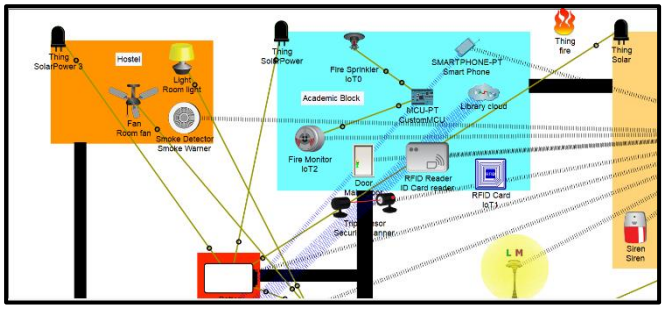
During flames, fire, and explosions, light varies. These variations aid in categorising the nature of the warning.

4) *Smoke sensor*

The presence of smoke indicates the presence of flames or shooting. In the event of a fire, it promptly notifies the appropriate authorities. If the smoke exceeds the original threshold value, ECR is notified, followed by CECC. The ECR display board continually displays the smoke reading.

5) *Metal detector*

The entry has a smart metal detector and walk through gates. ECR is alerted if metal is discovered on someone's entrance. This also aids in the monitoring of security guards, as most security officers do not thoroughly check persons at the entry. In such cases, security guards may be ordered to rescan the individual.



III. EMERGENCY CONTROL ROOM

The edge of IoT and cloud computing is fog computing. Rather of sending all data to the cloud for processing, it is largely sent to local devices for processing. The ECR makes advantage of the fog computing idea. This eliminates the need to transfer all streams to cloud servers. Despite the fact that CECC may access the gateway at any moment to monitor the situation. ECR is linked to all sensors, metal detectors, security cameras, emergency alert, and panic button. ECR is alerted of all first alarms.

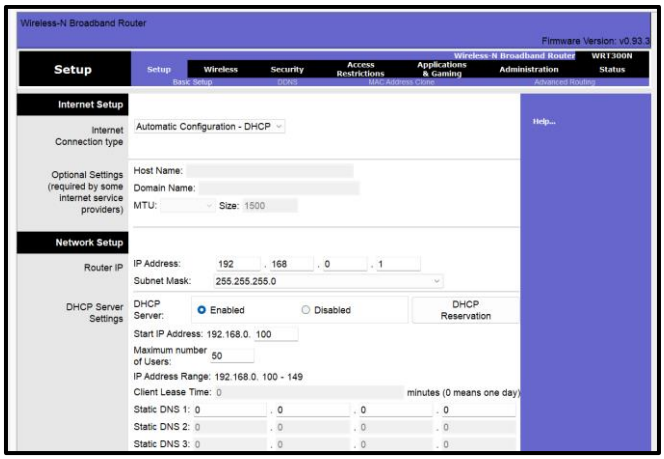


Fig: ECR Router configuration.

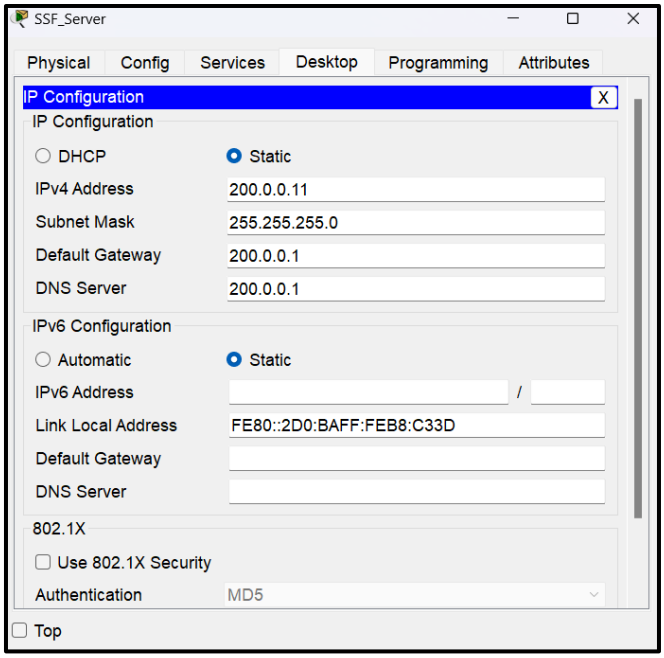


Fig: IP addresses configuration.

6) *Cloud server*

IoT and cloud services complement one other. IoT includes billions of gadgets and generates vast amounts of data. The infrastructure for processing and storing this massive quantity of data is provided by cloud computing. When an emergency call is received, the cloud server begins to receive live streaming from different sensors.

The type of the assault is classified using several methods. Notifications are delivered to the appropriate departments. Incoming streaming is aimed towards CECC.

Experimental Setup

For IoT network simulation, we utilised Cisco Packet Tracer 7, which is a widely known simulation tool. Cisco Packet Tracer 7 was created specifically to mimic IoT applications. For simulation, this package comprises several IoT devices, sensors, gateways, and IoT servers.

All sensors in the first layer read the environment. Fog computing technologies are used on the second layer to evaluate this data and transmit an alarm to the ECR and CECC. On the third tier, all concerned departments and CECC are at work. All of the sensors are monitored and controlled remotely, and intelligent judgements are made.

Type of test	***Checking working of CPT***
Source device	Security cameras
Target device	ECR & CECC
Expected result	Webcam video streaming at ECR
Response time	0.01
Avg. transfer time	0.111

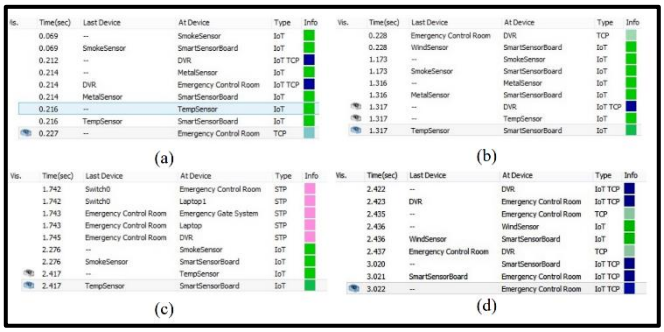


Fig: The testing of all the sensors and network devices

Protocols used in our project

Device	**Protocol Used to Com with CECC**
DVR	ICMP
Laptop	ICMP, ARP
Panic Button	ICMP, STP, IOT
Metal Detector	ICMP, STP, IOT
Smoke Detector	ICMP, STP, IOT
Temperature Sensor	ICMP, STP, IOT
Motion Sensor	ICMP, STP, IOT

ICMP - The Internet Control Message **Protocol**
Spanning Tree Protocol (STP) is a Layer 2
ARP - **Address Resolution Protocol**

IV. NOVELTY

- ✓ Well defined Educational Institute layout: A complete layout of an institution highlighting the most happening places in it was created to provide a better framework.
- ✓ Fog Layer: The original project stored and communicated data with the cloud storage. In this project in addition to the cloud layer, we added an intermediate fog layer to process the data immediately and provide a better and quicker response to the emergency site.
- ✓ Cloud network for storage - A separate cloud network was created to store all the sensory data and log them. This is helpful in the post emergency period to analyse the place of origin, time, cause of the emergency.
- ✓ To the existing sensors in the provided framework, multiple sensors that could be implemented in reality to sense the anomalies were added and simulated in our project.
- ✓ This model can sense the pressure through networks only and it can check the confidence rate.
- ✓ Live surveillance cameras were implemented at various parts of the institute to verify the genuineness of the emergency and to also predict the flow of the anomaly (like an attack/explosion). This will assist in blocking the affected path and ensure a safe emergency exit of the people.

V. WHAT DOES THE FUTURE HOLD

The Smart Security Framework (SSF) for educational institutions has been introduced in this article. Many priceless lives have been lost in recent atrocities. This could be depreciated by implementing an effective and intelligent warning system. SSF alerts concerns in an effective and intelligent manner in the event of an emergency. Different types of sensors are put around the facility, reading the surroundings 24 hours a day, seven days a week. If a warning is detected, an alarm is issued to the Emergency Control Room (ECR) as well as the Central Emergency Control Centre (CECC).

Smart emergency doors are linked to the proposed system, which opens automatically in the event of an alarm detection. SSS is not limited to educational institutions; it may also be utilised in any other organisation for security purposes. Our long-term goal is to expand this framework for the Smart Security Framework for Cities (SSSC). Sensors will be put in streets, public locations, and notably religious sites in the SSSC to alert authorities in real time.

REFERENCES

[1] An, J. G.; Le Gall, F.; Kim, J.; Yun, J.; Hwang, J. et al. (2019): Toward global iot enabled smart cities interworking using adaptive semantic adapter. IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5753-5765.

[2] Anitha, A. (2017): Home security system using internet of things. IOP Conference Series: Materials Science and Engineering.

[3] Baccarelli, E.; Vinueza Naranjo, P. G.; Scarpiniti, M.; Shojafar, M.; Jema, H. et al.

[4] (2017): Fog of everything: energy-efficient networked computing architectures, research

[5] Badshah, A.; Jalal, A.; Tauseef, U. R. (2015): Sla based infrastructure resources allocation in cloud computing to increase iaas provider revenue. Research Journal of IT Management, vol. 4, no. 4, pp. 37-43.

[6] Bedi, G.; Venayagamoorthy, G. K.; Singh, R.; Brooks, R. R.; Wang, K. C. (2018): Review of internet of things (IoT) in electric power and energy systems. Internet of Things Journal, vol. 5, no. 2, pp. 847-870. Bhawna, S.; Shweta, T. (2017): Smart threat alert system using IoT. International Conference on Computing, Communication and Automation.

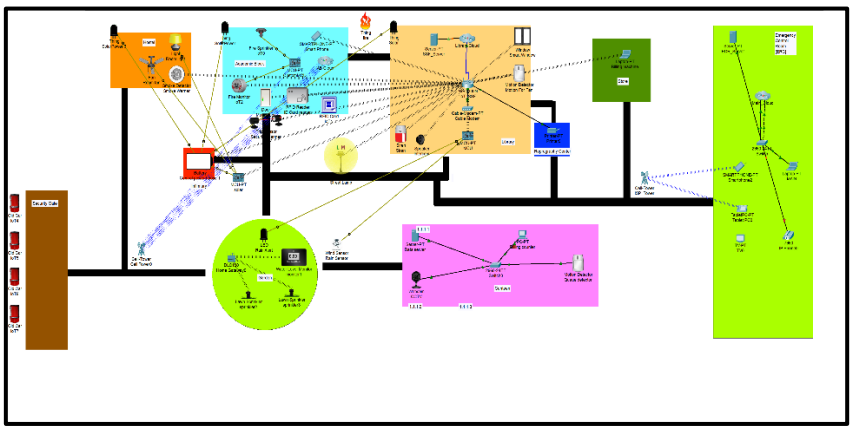


Fig: Cisco Packet Tracer Workspace