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

Afzal Badshah[1], Anwar Ghani[1], Muhammad Ahsan Qureshi[2] and Shahaboddin Shamshirband[3, 4, *]

Abstract: Educational institutions are soft targets for the terrorist with massive and defenseless people. In the recent past, numbers of such attacks have been executed around the world. Conducting research, in order to provide a secure environment to the educational institutions is a challenging task. This effort is motivated by recent assaults, made at Army Public School Peshawar, following another attack at Charsada University, Khyber Pukhtun Khwa, Pakistan and also the Santa Fe High School Texas, USA massacre. This study uses the basic technologies of edge computing, cloud computing and IoT to design a smart emergency alarm system framework. IoT is engaged in developing this world smarter, can contribute significantly to design the Smart Security Framework (SSF) for educational institutions. In the emergency situation, all the command and control centres must be informed within seconds to halt or minimize the loss. In this article, the SSF is proposed. This framework works on three layers. The first layer is the sensors and smart devices layer. All these sensors and smart devices are connected to the Emergency Control Room (ECR), which is the second layer of the proposed framework. The second layer uses edge computing technologies to process massive data and information locally. The third layer uses cloud computing techniques to transmit and process data and information to different command and control centres. The proposed system was tested on Cisco Packet Tracer 7. The result shows that this approach can play an efficient role in security alert, not only in the educational institutions but also in other organizations too.

Keywords: Internet of things, smart security framework, massacres, terrorism, smart emergency alert.

[1] Department of Computer Science and Software Engineering, International Islamic University, Islamabad, 44000, Pakistan.

[2] Faculty of Computing and Information Technology, University of Jeddah, Khulais, 21959, Kingdom of Saudi Arabia.

[3] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam.

[4] Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam.

[*] Corresponding Author: Shahaboddin Shamshirband. Email: shahaboddin.shamshirband@tdtu.edu.vn.

CMC. doi:10.32604/cmc.2019.06288

1 Introduction

Educational institutions massacres are the severe threat to security in increasing terrorist attacks. These are easy targets. The recent history reveals that thousands of children have been killed in such as attacks. In 2004, 334 students killed and 783 were injured in Beslan School Siege, Russia. In 2000, 191 students were killed and hundreds were injured in Walisongo School in Indonesia. In 1990, 158 students were killed and hundreds were injured in Eastern University, Srilanka. In 2016, 153 students were killed and hundreds were injured in Army Public School Peshawar, Pakistan.

Numbers of security system have been devolved. Security agencies have launched the number of initiatives to notify the attack on the institutions immediately. Emergency mobile phone numbers, alarm systems, and smart security cameras installed. Instead of spending billions of assets on security, no new technologies have been adopted to undertake these issues smartly. All these existing systems need to be updated to the new demands of threat and technology. The basic alarm system is not a valid solution for increasing attacks on educational institutions. To safeguard our children and assets, a smart alarming system must be installed in institutions [Tsakalozos, Verroios, Roussopoulos et al. (2017)].

IoT is becoming very popular in academia and day to day life as an emerging intelligent technology, in which smart devices are connected to the cloud. It uses the idea of fog and cloud computing to process a large amount of data. Its basic concept is to connect the smart devices to the cloud through the internet. IoT facilitates users to take the whole world on the smartphone. IoT is changing human lives by making it smart and easy. Data management, wireless communications, and real-time decisions are the key features of IoT. There has been a great deal of IoT research on different applications, such as smart homes, e-health systems, wearable devices, etc. According to the Industrial Analytical Firm (IAF), it is expected that about 50 billion devices will be connected to the internet up to 2020. Embedded technology is used in devices and sensors. Wireless technology enables them to connect with other devices or internet [Vermesan and Friess (2014)].

Smart home, smart e-health, and smart cities are popular topics in recent years, but Smart Security Frameworks have not been well investigated. IoT is the ideal technology to deal with such issues. The most beneficial is that existing infrastructure such as security cameras and control rooms may be utilized to convert them to the SSF.

The main contribution of this article is

- To design an SSF for educational institutions to instantly notify the concern departments to resist or to minimize the disaster.
- To remotely monitor and control the sensors and security devices during normal or in operational conditions to get full control over it at any time and from any place. Not only to monitor them but also to remotely program and configure all these devices.
- Collecting and analyzing data of all sensors and security devices to make smart decisions during an emergency or in abnormal situations.

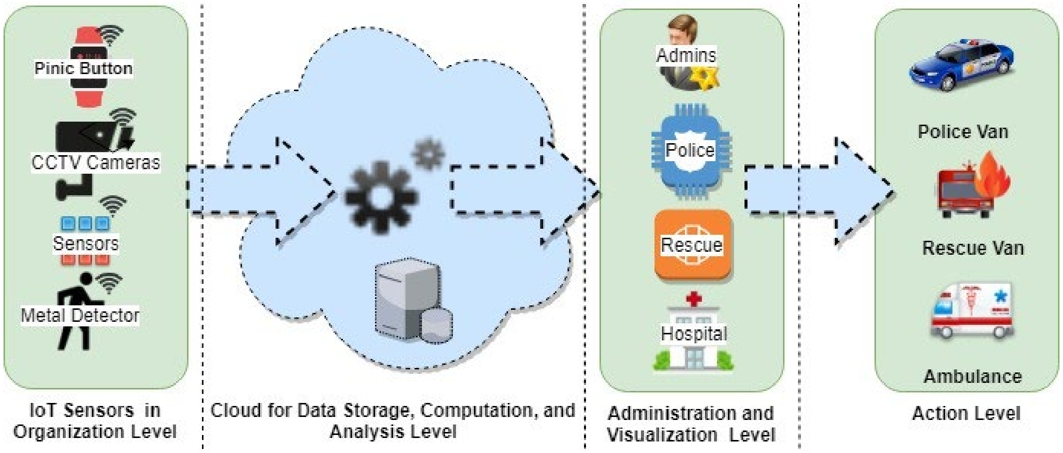

Pinic Button
CCTV Cameras
Sensors
Metal Detector
Admins
Police
Rescue
Hospital
Police Van
Rescue Van
Ambulance
IoT Sensors in Organization Level
Cloud for Data Storage, Computation, and Analysis Level
Administration and Visualization Level
Action Level

Figure 1: Data flow diagram of smart security framework

In the proposed SSF, different types of sensors, security threat detectors, and security cameras are used. These devices are connected to the Emergency Control Room (ECR) and Central Emergency Control Center (CECC) by wire and wireless technologies. In an emergency situation, the proposed system instantly notifies the concerns within a second and starts all sensors and security cameras streaming to ECR. Panic button, installed on the smart watch, is used to activate the SSF manually. Fig. 1 shows the data flow of Smart Security Framework.

SSF uses several types of algorithms to get data from all installed security devices. These algorithms help to categorize the alert. An alarm is issued to the concern departments with live streaming. The CECC is the centralized place in the region. CECC has members from police, rescue and ambulance services. Live updates and attack nature is displayed on monitoring screens. All top stack holders control and monitor the operation from that centres to make smart decisions. Tab. 1 shows the symbols used in formulation.

The rest of the paper is arranged as follows. Section 2 reviews the related work on IoT, sensors and security systems. Section 3 discusses the proposed SSF model, different types of sensors, ECR and CECC for SSF. Section 4 discusses the proposed algorithms for the smart alerting system, smart decision and alarms. Section 5 discusses the experimental setup. The proposed system simulation was run for numbers of times to demonstrate the supremacy of the proposed approach. Finally, Section 6 concludes all work.

Table 1: Symbols used in the article

Symbol	Definition	Symbol	Definition
χ_{temp}	Temperate Sensor	χ_{p}	Air Pressure Sensor
χ_{voc}	Voice Sensor	χ_{vib}	vibration Sensor
χ_{mtl}	Smart Metal Detector	χ_{lgt}	Light Intensity Sensor
χ_{smok}	Smoke Sensor	χ_{hum}	Humidity Sensor
χ_{flm}	Flame sensor	f	Flames
$temp$	Temperate	ρ	Air Pressure
υ	Voice	vib	Vibration
S	Smoke	ι	Light Intensity
gps	GPS	hum	Humidity
τ_{temp}	Threshold Value of Temperature	τ_{ρ}	Threshold Value of Air Pressure
τ_{voc}	Threshold Value of Voice	τ_{vib}	Threshold Value of Vibration
τ_{smok}	Threshold Value of Smoke	τ_{l}	Threshold Value of Light Intensity
τ_{flm}	Threshold Value of Flames	τ_{hum}	Threshold Value of Humidity
φ	Crying Sounds	Cam	Security Cameras
γ	Explosion Sounds	λ	Firing Sounds
$\mathit{\Theta}$	Smartwatch	X	Smartphone
α	Emergency Alert	$\mathit{\Pi}$	Emergency Control Room
$\mathit{\Theta}$	Smart Emergency Alarm	ψ	Emergency Panic Button
A	Attack	P	Police
$\mathit{\Upsilon}$	Rescue	C	Community
$\mathit{\Xi}$	Centralized Emergency Control Center	H	Hospital
Cat	Category of the alert	ϵ	Fire Brigade

2 Related work

IoT is getting a full range of attention in today academia and market. Sensors are making this world smarter. Smart security systems are getting more attention due to the wide spread of terrorism. In Advanced Safety Life Support System, different sensors is used [Lei, Liao, Huang et al. (2010)]. The system gathers different information such as contactless fingerprint and vein sensor, the intelligent detector of moving objects, the self-management security system on a Web and the 3D facial shape measurement system etc. This is a low-cost security system and can be installed by those organizations that cannot support costly security system. This work is limited only to the fingerprint security. Cho et al. designed low power CMIOS Image Sensor with a variable resolution technique for a smart security

[Cho, Kim, Sohn et al. (2016)]. CIS is based on the high-resolution mode. During normal conditions, the pixel of the picture drops to one-fourth of the original pixels. When any movement is detected, the high pixel is restored, and data is being transmitted to the server. In normal conditions, no data is transmitted to the server to save the cost. This work is limited only to video streaming and cost saving in security systems.

Radio Frequency (RF) is widely used in security projects. Bhawana et al. [Bhawna and Shweta (2017)] used RF to design a smart threat alert system. They proposed an emergency alert system combined with IoT to overcome some drawbacks of present EASs. It uses various types of detectors to identify transmission of various frequencies. They used Raspberry Pi to generate and detect different types of transmissions. This work is limited to radio frequency detection only. The same RF technology was used [Ruinian and Capurso (2017)] to design smart shopping system. The first time, UHFRFID was used to enhance the shopping experience and security issues. They developed a prototype to test the smart shopping system. With a smart cart system, billing can be conducted from the shopping cart itself, preventing customers from waiting in a long queue at the checkout. This work is limited to shopping billing security. This article helped us in SSF framework creation.

Now a day, IoT is widely used in electricity grids and electrical appliances. It is the primary market of the IoT industry.Guneet Bedi discussed the specific role of IoT in different smart systems [Guneet, Ganesh, Rajendra et al. (2018)]. They provided a detailed assessment of the technical parameters of IoT. IoT reduces energy wastage and generates savings. it improves the efficiency, reliability, resiliency, security, and sustainability of the electric power networks. This article helped us to get familiar with IoT devices and its working. Li et al. [Li and Dong (2018)] developed a deep learning framework for large data coming from IoT sensors deployed in the complex environment. Because the nodes have limited capabilities of processing and storing, so they worked on the offloading framework to increase the performance of deep learning applications with edge computing. This article helps us how to process a large amount of data coming from different smart devices. Shoaib et al. [Shoaib, Havinga, Paul et al. (2016)] discussed the use of smoke sensors in smart devices, Deve et al. [Deve, Hanacke and Silva (2016)] discussed a smart system for fire detection and notification. Junhui et al. [Junhui and Guorong (2016)] worked on metal detectors. Alharbi et al. [Alharbi and David (2018)] discussed the motion detectors and lighting system for the city. Packet Tracer is the CISCO devices based network simulator. In its 7 versions, they have embedded IoT simulation tools. It is widely used for IoT devices simulation. Vijaya [Vijaya (2016)] discussed the use of Packet Tracer for different networking projects. They introduced a structured learning approach to learn Packet Tracer. These structure clear students in use of physical devices like router, access points, switch and their configurations. They introduced errors deliberately to remove errors in the simulations. In our proposed framework, we used Packet Tracer to simulate and evaluate the proposed framework. This article helped us in Packet Tracer usage.

3 System model

SSF uses IoT, fog and cloud concepts. IoT devices sense the environment. This data is further forwarded toward fog cloud servers. In case of alerts or request, this is streamed to cloud centers. Higher authorities take decisions according to the sensing data. The great type of decisions and operations depends on the good type of sensing and communicating data to the control centers. In this section, we evaluated the functioning of the proposed framework. This could be precise advantageous to combine IoT into safety and emergency alerting schemes. Several sorts of sensors are utilized to implement the SSF. All the sensors remain active and connected to the internet round the clock. Fig. 2 shows the proposed structure of the Smart Security Framework.

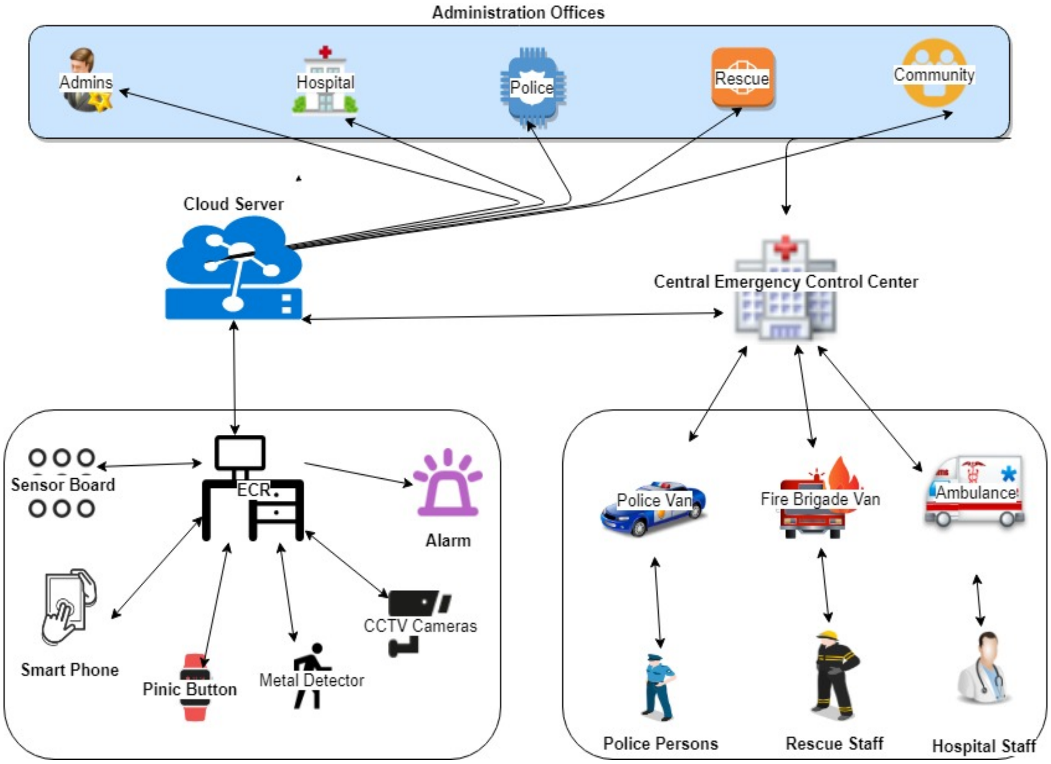


Figure 2: Proposed structure of smart security framework

3.1 Smart sensor board

Smart Sensor Board is a circuit board which has different types of sensors. Every sensor board has pressure, temperature, humidity, smoke, motion, flames and high-sensitive voice sensors. Smart board uses embedded technology. Algorithms are used to transmit its data to the ECR and to the CECC. Other smart security tools such as smart metal detectors, the smart walk through gats, smart alarm system and also security cameras are used. In case of any exceptions, it automatically notifies the concern admins. Smart sensor board uses Algorithm 1 to initialize the SSF. Tab. 2 shows the threshold values used in the experimental setup.

3.1.1 Temperature sensor

The temperature fluctuates during flames, firing or explosion. This fluctuation is used to categorize the alert and to determine the reason. ECR is alerted if the temperature rises from the initial threshold value. An emergency alert is sent to the CECC if the temperature rises from the second threshold value. The temperature reading is continuously displayed on the ECR display board.

Table 2: Threshold values used in article

Symbol	Threshold Value	Symbol	Threshold Value
χ_{temp_i}	52 C	$\chi_{temp_{ii}}$	60 C
χ_{vib_i}	15 mm/s at 5 MHz	$\chi_{vib_{ii}}$	15 mm/s at 15 MHZ
χ_{smok_i}	10 ppm	$\chi_{smok_{ii}}$	35 ppm
χ_{ap_i}	110 kPa	χ_{lgt_i}	150 cd
χ_{v_i}	100 dB	$\chi_{v_{ii}}$	157.5 dB

$$\alpha_{temp}(x) = \begin{cases} \Pi & if\ temp \geq \tau_{temp}i \\ \Xi & if\ temp \geq \tau_{temp}ii \\ temp^{\circ}C & otherwise \end{cases} \tag{1}$$

3.1.2 Vibration/wind sensor

Firing or explosion produces a strong wave force. Vibration sensors in smart board detect any type of vibration in the walls. The “x” and “y” vibration can easily be detected and categorized that what object has hit the wall. This vibration helps the CECC team to categorize the type of alert. If vibration increases from the first threshold, an alert is sent to ECR and if passes by the second threshold value, CECC is notified.

$$\alpha_{vib}(x) = \begin{cases} \Pi & if\ vib \geq \tau_{vib}i \\ \Xi & if\ vib \geq \tau_{vib}ii \\ NO & otherwise \end{cases} \tag{2}$$

3.1.3 Light sensor

Light fluctuates during flames, firing, and explosion. These fluctuations help to categorize the nature of the alert.

$$\mathrm{\alpha_{lgt}(x)} = \begin{cases} \Pi & \text{if lgt} \geq \tau_{\mathrm{lgt}} \\ \mathrm{NO} & \text{otherwise} \end{cases} \tag{2}$$

3.1.4 Smoke sensor

Smoke is the indication of flames or firing. In the case of fire, it timely informs the concern authorities. If the smoke crosses the initial threshold value, ECR is alerted, secondly, CECC is notified. Smoke reading is continuously displayed on the ECR display board.

$$\alpha_{\mathrm{smok}}(x) = \begin{cases} \Pi & \text{if smok} \geq \tau_{\mathrm{smok}} i \\ \Xi & \text{if smok} \geq \tau_{\mathrm{smok}} ii \\ S & \text{otherwise} \end{cases} \tag{3}$$

3.1.5 Sound sensor

The intensity of sounds not only help to alert the smart security system in an emergency but also help the CECC officials to categorize the alert. It also helps during operations. voice recognition software may also be used to categorize firing, explosions and screaming.

$$\alpha_{\upsilon}(x) = \begin{cases} \Pi\&\Xi & \text{if } \upsilon \geq \gamma\&\lambda\&\varphi \\ \mathrm{NO} & \text{otherwise} \end{cases} \tag{4}$$

3.1.6 Air pressure sensor

During the analysis of the nature of the alert, an air pressure sensor plays a good part. If the air pressure sensor is forcefully activated, it clearly shows that some explosion has taken place. Air pressure fluctuations also help to categorize the alert.

$$\alpha_{\mathrm{ap}}(x) = \begin{cases} \Pi & \text{if shock of wind detected} \\ \mathrm{NO} & \text{otherwise} \end{cases} \tag{5}$$

3.1.7 Metal detector

The smart metal detector and walk through gates are placed on the entrance. If metal is detected on someone entry, ECR is notified. This also helps to monitor the security guards too, because most of the security guards do not properly scan the people at the entrance. On such phenomenon, security guards may be directed to rescan the person.

$$\alpha_{\mathrm{met}}(x) = \begin{cases} \Pi & \text{if metal detected} \\ \mathrm{NO} & \text{otherwise} \end{cases} \tag{6}$$

3.1.8 Panic button

The panic button is installed on the smart watch. It is a traditional button instead of touch functionality. More than one person has the smart watch panic button so to press it instantly in case of any attack or danger.

$$\alpha_{\mathrm{pb}}(x) = \begin{cases} \Pi\ \&\ \Xi & \text{if pb is pressed} \\ \mathrm{NO} & \text{otherwise} \end{cases} \tag{7}$$

Type of alert may be classified by different sensors data such as the temperature, light intensity, wave shocks, value of smoke, and intensity of sound etc.

3.2 Emergency control room

Fog computing is the edge of IoT and cloud computing. Instead of sending all data to the cloud for processing, primarily, it is send to local devices for processing. The ECR uses the concept of fog computing. This saves the cost of sending all streaming to cloud servers. Although CECC may access the gateway any time to monitor the situations. All the sensors, metal detectors, security cameras, emergency alarm and the panic button is connected to ECR. All initial alerts is notified to ECR.

For the proposed simulation, we are using the following threat categorization techniques to categorize the alert. Implementers' or organization may alter it according to the requirements and sensitivity of the security.

$$\alpha \quad \leftarrow \alpha\, 1 \text{ if } \left(\chi_{\text{temp}} = \chi_{\text{temp}_{\text{i}}}\right) \otimes \left(\chi_{\text{vib}} = \chi_{\text{vib}_{\text{i}}}\right) \otimes \left(\chi_{\text{smok}} = \chi_{\text{smok}_{\text{i}}}\right) \otimes \left(\chi_{\text{ap}} = \chi_{\text{ap}_{\text{i}}}\right) \tag{8}$$

Eq. (9) shows the situation when anyone sensor reading crosses the first threshold values. If temperature, smoke, vibration or noise little bit increases from the normal situation then ECR is notified.

$$\alpha \quad \leftarrow \alpha\, 2 \text{ if } \left(\chi_{\text{temp}} = \chi_{\text{temp}_{\text{i}}}\right) \odot \left(\chi_{\text{vib}} = \chi_{\text{vib}_{\text{i}}}\right) \odot \left(\chi_{\text{smok}} = \chi_{\text{smok}_{\text{i}}}\right) \odot \left(\chi_{\text{ap}} = \chi_{\text{ap}_{\text{i}}}\right) \tag{9}$$

Eq. (10) shows the situation when almost all sensors reading crosses the first threshold values. If temperature, smoke, vibration or noise all reading increases from the normal situation then ECR and CECC is notified.

$$\alpha \quad \leftarrow \alpha\, 3 \text{ if } \left(\chi_{\text{temp}} = \chi_{\text{temp}_{\text{ii}}}\right) \otimes \left(\chi_{\text{vib}} = \chi_{\text{vib}_{\text{ii}}}\right) \otimes \left(\chi_{\text{smok}} = \chi_{\text{smok}_{\text{ii}}}\right) \tag{10}$$

Eq. (11) shows the situation when sensors reading crosses the second threshold values. If temperature, smoke, vibration or noise increases from the second threshold value then ECR as well as CECC is notified.

$$\alpha \quad \leftarrow \alpha\, 4 \text{ if } \left(\chi_{\text{temp}} = \chi_{\text{temp}_{\text{ii}}}\right) \odot \left(\chi_{\text{vib}} = \chi_{\text{vib}_{\text{ii}}}\right) \odot \left(\chi_{\text{smok}} = \chi_{\text{smok}_{\text{ii}}}\right) \tag{11}$$

Eq. (12) shows the situation when almost all sensors reading crosses the second threshold values. If temperature, smoke, vibration or noise increases from the second threshold values then CECC is notified.

$$\alpha \quad \leftarrow \alpha\, 5 \text{ if } (\alpha_{\text{v}} = \gamma) \odot (\alpha_{\text{v}} = \lambda) \odot (\alpha_{\text{v}} = \varphi) \tag{12}$$

Eq. (13) shows abnormal attacked position in the institutions. CECC is informed in such like situations.

$$\text{Cat(x)} = \begin{cases} \text{x} = 1 & \text{if } \alpha == \alpha_1 \\ \text{x} = 2 & \text{if } \alpha == \alpha_2 \\ \text{x} = 3 & \text{if } \alpha == \alpha_3 \\ \text{x} = 4 & \text{if } \alpha == \alpha_4 \\ \text{x} = 5 & \text{if } \alpha == \alpha_5 \\ \text{x} = 6 & \text{if Layer 1 or 2 fails} \end{cases} \tag{13}$$

3.2.1 Smart watch

A panic button is installed on the smart watch. It is a traditional button which can be pressed easily, instead of a touch sensor. It has all the smartphone sensors and Wi-Fi connection. When the panic button is pressed, all the smart watch sensors are activated and data is automatically streamed to the ECR and CECC. More than one person has the smart watch button due to security issues.

3.2.2 Smart phone

The ECR applications are also run on several smartphones to instantly generate an alert. Smartphones are popularly used devices today. In the proposed scenario they are connected with the ECR. All sensors can be accessed on a smartphone. In case of an emergency, its application opens automatically to categorize the threat. If the user fails to respond, the system automatically categorizes the threat.

3.2.3 Laptop

The smart home gateway is used to integrate all the smart devices. This gateway is connected to the laptop to monitor the system. LCD monitor may also be used to monitor the system. The laptop is used to *make changes in connections, functions or algorithms.*

3.2.4 Security cameras

Smart security cameras are the most important part of the security systems. The modern Digital Video Recorder (DVR) has advance types of software which help in threat detection. Smart cameras are used to record the videos, detect any motions, detect faces and also for voice alerts. In educational institutions, because there are too many students, so we are not going to use its voice and face recognition functionality for threat detection. In case of any alert, cameras streaming is directed to the CECC. In normal situations, video streaming is not forwarded to the CECC to save the cost and traffic load. Security cameras existing functionality may be used to get alert at ECR.

$$\text{LiveStreaming(x)} = \begin{cases} \Pi & \text{round the clock} \\ \Xi & \text{On } \Xi \text{ request} \\ \Xi & \text{if threat detected} \end{cases} \tag{14}$$

3.2.5 Emergency gate

Every organization has emergency doors and gates for emergency exit. In an emergency, it is not possible to manually open these doors for the exit. We have proposed to attach these doors and gates with SSF. In SSF, as the alert is notified, all the connected emergency doors get open automatically.

$$\text{EmerDoors(x)} = \begin{cases} \text{Close} & \text{No alert detected} \\ \text{Open} & \text{Alert detected} \end{cases} \tag{15}$$

3.3 Cloud server

The IoT and cloud, both services work together. IoT has billion of devices and produces massive data. Cloud computing provides the infrastructure to process and store this large amount of data. In an emergency call, the cloud server starts to receive live streaming from different sensors. With the help of different algorithms, the nature of the attack is categorized. Notifications are sent to concern departments. Incoming streaming is directed toward CECC.

3.4 Central emergency control center

CECC is a building or room where all emergency alerts are received from the region. Every district has its own CECC. CECC guarantees a 24/7 service through a complex communications' system. It also uses the emergency numbers to receive emergency phone calls. CECC permits the police, the armed forces, civil protection department and the rescue department to take urgent action. Initially, CECC is monitored by an operator. In case of an emergency, stockholders officer take the control of CECC. CECC has the representatives of police, the ambulance services, the fire brigade, and rescue services. Live streaming of all the sensors are shown in CECC. All concern stack holders monitor the issue. They manage the response to the alert. Hospitals are updated according to the situations.

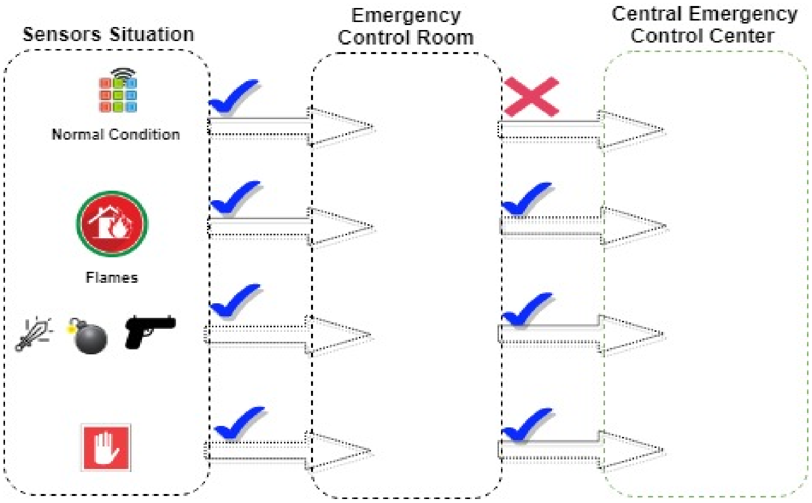


Figure 3: Conditional data flow of smart security system

4 Proposed algorithms

The proposed system notifies the concerns in case of an emergency. Fig. 3 shows the conditional flow of the proposed framework. In the normal situation, data is only streamed to the ECR situated within the organization to save the network cost. Although, CECC may get the live streaming of sensors any time. In case of an alert detection, all sensors data is directed to the CECC. Fig. 3 shows the conditional data flow of Smart Security Framework

An Algorithm 1 is embedded in smart-board and ECR. It reads temperature, pressure, smoke, motion and sounds etc. If the values increase from the threshold values, emergency notification is sent to the ECR and CECC and the smart emergency alarm starts ringing.

Algorithm 1 Initialization of Smart Security System

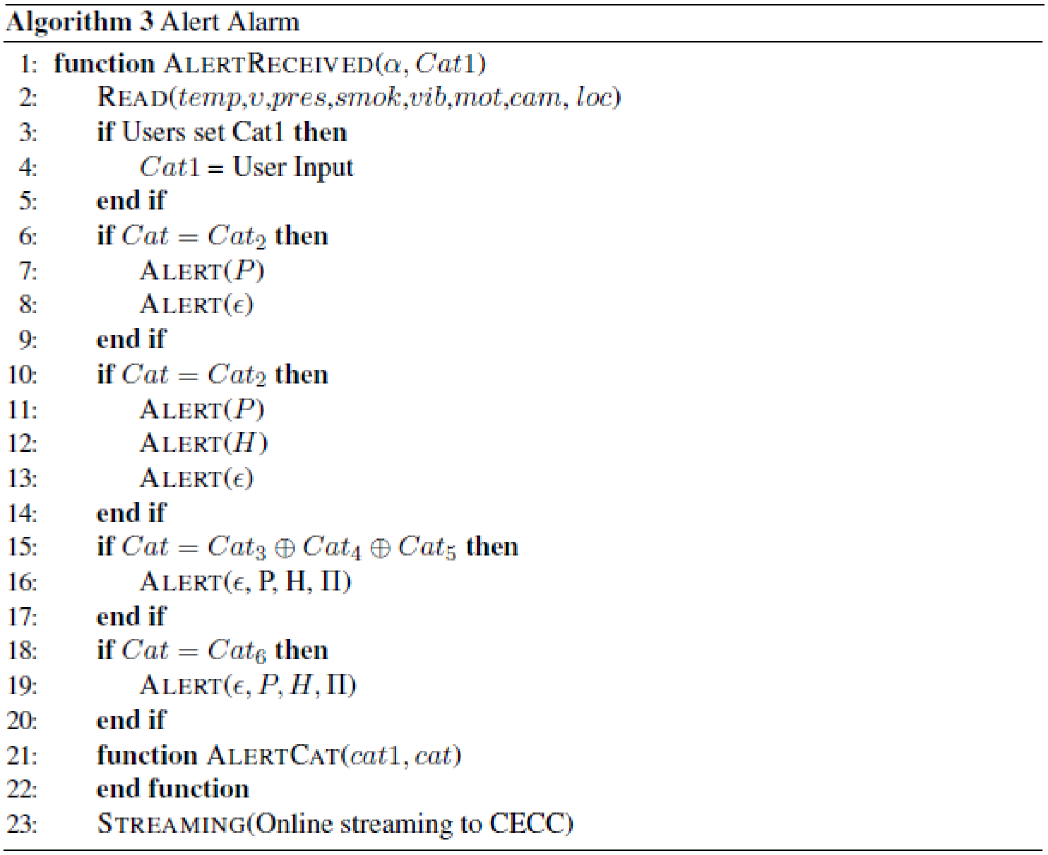
```
SwitchedOn
SETUP(Setup of Analog and Digital Pins)
READ($\chi_{temp}$,$\chi_p$,$\chi_{smok}$,$\chi_{vib}$,$\chi_{mot}$, $\chi_{cam}$,$\chi_{loc}$)
if $Cat(x) == 1, 2$ then
    Issued Emergency Notification to ECR
    EMERGALRAM(=yes)
end if
if $Cat(x) == 3, 4, 5$ then
    EMERGENCYCALL(yes)
    EMERGALRAM(yes)
    EMERGDOOR(Open)
    STREAMOUT($\chi_{temp}$, $\chi_p$, $\chi_{smok}$, $\chi_{vib}$, $\chi_{mot}$, $\chi_{cam}$, $\chi_{loc}$)
end if
if $Cat(x) == 6$ then
    EMERGENCYCALL(yes)
    EMERGALRAM(yes)
    SECONDARYHUB(yes)
end if
if ActionButton == yes then
    EMERGENCYBUTTON(yes)
    EMERGALARM(yes)
    EMERGDOOR(Open)
    STREAMOUT($\chi_{temp}$,$\chi_p$,$\chi_{smok}$,$\chi_{vib}$,$\chi_{mot}$, $\chi_{cam}$,$\chi_{loc}$)
end if
```

Algorithm 2 works in Emergency Control Room and in home-gateway. As emergency accrues, alert categorization application automatically opens on smartphones and ECR alarm starts ringing to categorize the alert. If the user fails to respond to the application, It automatically sends the alert to CECC.

Algorithm 2 Emergency Control Room

```
function ALERTRECEIVED($\alpha$)
    READ($\chi_{temp}$, $\chi_p$, $\chi_{smok}$, $\chi_{vib}$, $\chi_{mot}$, $\chi_{cam}$, $\chi_{loc}$)
    RISKCATEGORIZATION(Automatically open the application on smart phones)
    RINGING(ECR alarm)
    AUTOMATICCATEGORIZATION(Automatically categorize the risk)
    SENDING(Continue streaming all sensor data to the CECC)
    EMERGALARM(yes)
    EMERGDOORS(yes)
end function
```

Algorithm 3 is used in CECC. As the alert is received, CECC starts to get data from all the sensors placed in different locations. According to the data, the nature of alert is categorized. Notification and live streaming are issued to the concern departments.



Algorithm 3 Alert Alarm

```
function ALERTRECEIVED($\alpha$, $Cat1$)
    READ($temp$,$v$,$pres$,$smok$,$vib$,$mot$,$cam$, $loc$)
    if Users set Cat1 then
        $Cat1$ = User Input
    end if
    if $Cat = Cat_2$ then
        ALERT($P$)
        ALERT($\epsilon$)
    end if
    if $Cat = Cat_2$ then
        ALERT($P$)
        ALERT($H$)
        ALERT($\epsilon$)
    end if
    if $Cat = Cat_3 \oplus Cat_4 \oplus Cat_5$ then
        ALERT($\epsilon$, P, H, $\Pi$)
    end if
    if $Cat = Cat_6$ then
        ALERT($\epsilon, P, H, \Pi$)
    end if
    function ALERTCAT($cat1$, $cat$)
    end function
    STREAMING(Online streaming to CECC)
```

5 Experimental setup and evaluation

This section first describes the experimental setup and then presents the performance evaluation of the proposed framework. We used Cisco Packet Tracer 7 and Java, which is popularly used simulation tool for IoT network simulation. Cisco Packet Tracer 7 is specially designed to simulate IoT applications. This package includes different IoT devices, sensors, gateways and IoT servers for simulation.

5.1 Experimental setup

In the laboratory setup, we distributed the work into three layers. In the first layer, all sensors read the environment. On the second layer, fog computing technologies are utilized to analyze these data and send an alarm to the ECR & CECC. On the third layer, all the concern departments and CECC works. All the sensors are remotely monitored and controlled and smart decisions are made. Fig. 4 shows the simulation structure of Smart Security Framework.

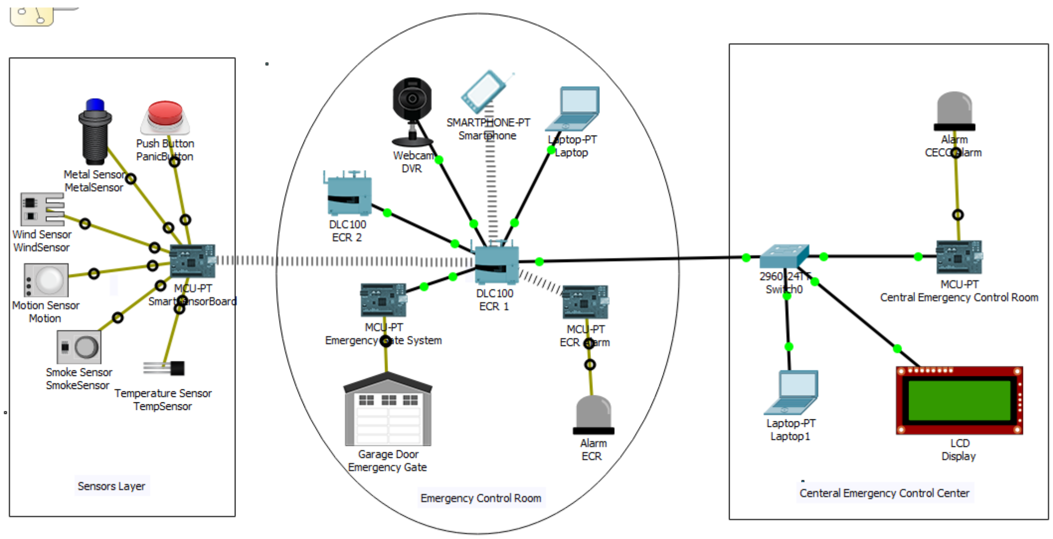


Figure 4: Simulation structure of smart security framework

5.1.1 Sensor board

Several types of sensors are connected to Microprocessor Control Unit (MCU). MCU is a small circuit board, which have links to install sensors on it. Using IoT cable, we connected temperature, motion, smoke, sound sensors and also the panic button to it. We programmed the MCU using java language to read data from all the connected sensors and transmit it to the ECR. To make the sensor board remote connection with the home gateway, IP address is assigned to the home gateway and set the MCU default gateway as the home gateway. We programmed the MCU to transmit its reading toward the home gateway.

5.1.2 Emergency control room

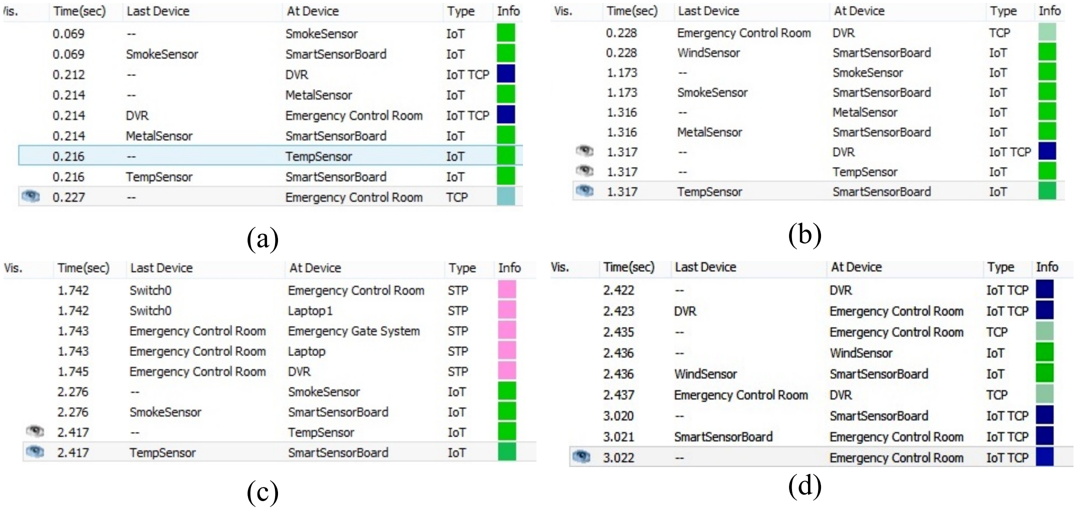
After making all connections, we connected the MCU board with home gateway. The home gateway is a wireless switch device, which can connect numbers of devices. It uses the fog computing concepts to process initial data on edge before sending it to the cloud. Digital Video Recorder (DVR), which has connections to numbers of cameras, are also connected to the home gateway. Home gateway has a wireless card to easily connect wireless devices to it. Laptop, smartphone, and smart watch are connected to the home gateway to get notifications from all sensor devices during on warning. Sirens installed in different locations of the institution are also connected to the home gateway. This emergency alarm ring during any alert. MCU circuit boards are used to connect emergency doors to the home gateway. In case of an emergency, all emergency doors open automatically. The laptop is used to get access to the home gateway and to implement programs on different sensor devices. It also facilitates to impose different types of conditions on the sensors and other connected IoT devices. To monitor SSF, we first converted the home gateway as IoT server. To implement the program, we opened the IoT monitor application, registered gateway as IoT server. The same application helps to program and executes the devices remotely. We wrote proposed algorithms here to get detail monitoring data from different sensors and to analyze that data. ECR and CECC are notified as any threat is detected. For example, when the panic button is pressed it instantly play the emergency alarm at ECR and CECC.

5.1.3 Central emergency control center

We used switches to create different departments. CECC is the central place where all the security devices are monitored. When a warning is identified, its emergency alarm starts ringing. The concern location is monitored online to get detail information about any warning. CECC has the authorization to access the local gateway. Alarm and the display screens are connected with the MCU board. Laptop and smartphone are also connected to the internal switch. MCU is programmed to receive notification from all over security devices. When an alert is received, the alarm system starts ringing.

5.2 Evaluation of proposed system

The proposed system is tested for different types of Alerts. We examined its functionality and performance. Average results of different tests are shown in below tables. Fig. 5 shows the snapshot of CISCO Packet Tracer results.



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.069	--	SmokeSensor	IoT	🟩
	0.069	SmokeSensor	SmartSensorBoard	IoT	🟩
	0.212	--	DVR	IoT TCP	🟦
	0.214	--	MetalSensor	IoT	🟩
	0.214	DVR	Emergency Control Room	IoT TCP	🟦
	0.214	MetalSensor	SmartSensorBoard	IoT	🟩
	0.216	--	TempSensor	IoT	🟩
	0.216	TempSensor	SmartSensorBoard	IoT	🟩
👁	0.227	--	Emergency Control Room	TCP	🟩

(a)

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.228	Emergency Control Room	DVR	TCP	🟩
	0.228	WindSensor	SmartSensorBoard	IoT	🟩
	1.173	--	SmokeSensor	IoT	🟩
	1.173	SmokeSensor	SmartSensorBoard	IoT	🟩
	1.316	--	MetalSensor	IoT	🟩
	1.316	MetalSensor	SmartSensorBoard	IoT	🟩
👁	1.317	--	DVR	IoT TCP	🟦
👁	1.317	--	TempSensor	IoT	🟩
👁	1.317	TempSensor	SmartSensorBoard	IoT	🟩

(b)

Vis.	Time(sec)	Last Device	At Device	Type	Info
	1.742	Switch0	Emergency Control Room	STP	🟪
	1.742	Switch0	Laptop1	STP	🟪
	1.743	Emergency Control Room	Emergency Gate System	STP	🟪
	1.743	Emergency Control Room	Laptop	STP	🟪
	1.745	Emergency Control Room	DVR	STP	🟪
	2.276	--	SmokeSensor	IoT	🟩
	2.276	SmokeSensor	SmartSensorBoard	IoT	🟩
👁	2.417	--	TempSensor	IoT	🟩
👁	2.417	TempSensor	SmartSensorBoard	IoT	🟩

(c)

Vis.	Time(sec)	Last Device	At Device	Type	Info
	2.422	--	DVR	IoT TCP	🟦
	2.423	DVR	Emergency Control Room	IoT TCP	🟦
	2.435	--	Emergency Control Room	TCP	🟩
	2.436	--	WindSensor	IoT	🟩
	2.436	WindSensor	SmartSensorBoard	IoT	🟩
	2.437	Emergency Control Room	DVR	TCP	🟩
	3.020	--	SmartSensorBoard	IoT TCP	🟦
	3.021	SmartSensorBoard	Emergency Control Room	IoT TCP	🟦
👁	3.022	--	Emergency Control Room	IoT TCP	🟦

(d)

Figure 5: Running time of IoT devices

Tab. 3 describes the test of a motion sensor. To check the operation of a motion sensor, we switched the Packet Tracer to simulation mode and brought the Alt+Mouse closer to it which is the default trigger of the motion sensor. As we brought it closer, the emergency alarm system of ECR started ringing. Same movement option is displayed on CECC. Packet Tracer result shows that the response time of the motion sensor is 0.01 seconds while the transfer time to the emergency alarm is 1.557 seconds.

Table 3: Motion sensor test

Type of Test	Checking working of motion sensor
Source Device	Motion Sensor
Target Device	To ring CECC Alarm
Expected Result	Alarming in CECC
Status	Successful
Response Time	0.01
Avg Execution Time	1.557

Tab. 4 explains the working of a metal detector. To evaluate the performance of the metal detector, we run the Packet Tracer in simulation mode and brought the metal closer to the metal detector which is its default trigger. As we brought it closer, the emergency alarm system of ECR started ringing. Packet Tracer results show that the response time of the metal sensor is 0.01 seconds. Transfer time of metal sensor signal to CECC is 2.19 seconds.

Table 4: Metal sensor

Type of Test	Checking working of metal detector
Source Device	Metal Detector
Target Device	To ring the CECC Alarm
Expected Result	Alarming in CECC
Status	Successful
Response Time	0.01
Avg Execution Time	2.19

Tab. 5 displays the functioning of a temperature sensor. Temperature sensor reads the temperature of the current environment and detail is sent to the ECR. A check has been placed on temperature to ring the alarm if the temperature passes by 50C. Temperature sensor was efficiently displaying results on ECR. Packet Tracer result shows that the transfer time of metal sensor signal to CECC is 1.226 seconds.

Table 5: Temperature reader

Type of Test	Checking working of temp sensor
Source Device	Temperature Sensor
Target Device	IoT or CECC Server
Expected Result	Displaying temp at ECR & CECC
Status	Successful
Response Time	0.01
Avg Transfer Time	1.226

Tab. 6 shows the working of a smoke sensor. The smoke sensor detects the smoke of current environment and detail is shown on ECR display. A check has been placed on smoke to ring the alarm if the smoke crosses 50 pp. The smoke sensor was efficiently displaying results on ECR. Packet Tracer result shows that the transfer time of the metal sensor signal to CECC is 1.524 seconds.

Table 6: Smoke sensor

Type of Test	Checking working of smoke sensor
Source Device	Smoke sensor
Target Device	IoT Server
Expected Result	Displaying reading on IoT server
Status	Successful
Response Time	0.01
Avg notification Time	1.524

Tab. 7 demonstrates the working of the panic button. To check the panic button, we run the Packet Tracer in simulation mode and pressed the panic button. As we pressed the button, the emergency alarm of ECR and CECC started ringing. Packet Tracer result shows that the response time of the panic button is 0.01 seconds and the transfer time of the emergency signal to CECC is 1.674 seconds.

Table 7: Panic button

Type of Test	Checking working of panic button
Source Device	Panic button
Target Device	Ringing ECR and CECC alarm
Expected Result	Alarming ECR and CECC
Status	Successful
Response Time	0.01
Avg Notification Time	1.674

Tab. 8 shows the operations of security cameras. Security cameras video is displayed 24/7 at ECR. The video is streamed to CECC only in emergency detection. However, CECC may watch this online streaming at any time. To assess the working of security cameras, we run the Packet Tracer in simulation mode and pressed the panic button. As we pressed the button, the security cameras video is directed toward the server. Packet Tracer result shows that the response time of security camera is 0.01 seconds and the transfer time of the emergency signal to CECC is 0.111 seconds.

Table 8: Security cameras

Type of Test	Checking working of security cameras
Source Device	Security cameras
Target Device	ECR & CECC
Expected Result	Displaying video at ECR and CECC
Status	Successful
Response Time	0.01
Avg. Transfer Time	0.111

Tab. 9 represents the working of emergency gates. We have connected one door to the Smart Security Framework to check it is working. Emergency gates are open only on an emergency call. To check the working of the emergency gate, we run the Packet Tracer in simulation mode and pressed the panic button. As we pressed the button, the gates open automatically. Packet Tracer result shows that the response time of gate is 0.01 seconds.

Table 9: Emergency doors

Type of Test	Checking working of emergency doors
Source Device	Panic button
Target Device	Emergency doors
Expected Result	Opening emergency doors
Status	Successful
Response Time	0.01
Avg. Execution Time	1.388

Tab. 10 shows the different protocols used by different devices during transmission. We used the ping command to note the protocol used and time taken in the transfer. Fig. 5(d) shows that when the IoT protocols and micro-controller are used the transfer time increases.

Table 10: Protocol used in simulation

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

Fig. 9 shows the results of Packet Tracer. We checked it only for the ping command to note down the total time taken in request transfer. Tab. 10 shows the protocol used in communication. The result shows that transfer time increases where MCU is used. It also uses the IoT protocol to communicate. In the proposed simulation, we are keeping the wire length constant. The result shows that the transfer time also increases if we increase intermediate communication nodes.

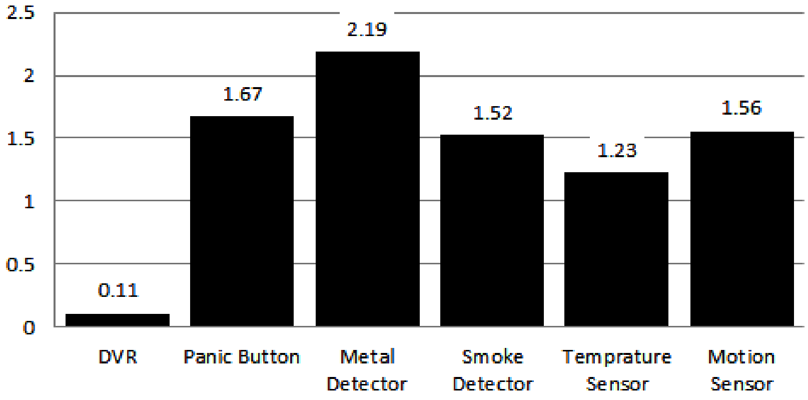


Figure 6: Packet Tracer simulation results

The above result and discussion shows that SSF is very good initiative towards instant notification about security issues. Security departments will be able to instantly move toward the threat direction. With this setup, control centers official will be able to properly guide the operation to minimize the losses.

6 Conclusion and future work

In this article, Smart Security Framework (SSF) has been introduced for educational institutions. The recent past massacres have taken many precious lives. This might be depreciated by adopting an efficient and smart alerting system. SSF is efficient and intelligent in alerting concerns in case of an emergency. Different types of sensors are placed in different locations of the building, reading environment 24/7. In case of any warning detection, an alert is sent to the Emergency Control Room (ECR) and also to Central Emergency Control Center (CECC). Smart emergency doors are connected with the proposed system which automatically opens in case of any alert detection. SSS is not confined only to the educational institutions, it may also be used in any other organizations for security objects. Our future plane is to extend this framework for the Smart Security Framework for the City (SSSC). In the SSSC, sensors will be placed in streets, public places and especially religion places to notify the concern on time.

References

Alharbi, R.; Aspinall, D. (2018): An IoT analysis framework: an investigation of IoT smart cameras' vulnerabilities. *Living in the Internet of Things, Cybersecurity of the IoT.*

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.

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

Baccarelli, E.; Vinueza Naranjo, P. G.; Scarpiniti, M.; Shojafar, M.; Jema, H. et al. (2017): Fog of everything: energy-efficient networked computing architectures, research challenges, and a case study. *IEEE Access*, vol. 75, no. 2, pp. 9882-9910.

Badshah, A.; Jalal, A.; Tauseef, U. R. (2014): Performance based service level agreement in cloud computing. *Research Journal of IT Management*, vol. 4, no. 3, pp. 19-30.

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.

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*.

Cho, Y.; Kim, H.; Sohn, Y.; Oh, J.; Song, M. (2016): Design of a variable resolution cmos image sensor for a smart security system. *12th Conference on Ph.D. Research in Microelectronics and Electronics*.

Deve, K. B.; Hanacke, G. P.; Silva, B. J. (2016): Design of a smart fire detection system. *42_{nd} Annual Conference of the IEEE Industrial Electronics Society.*

Emre, E.; Hasan, R.; Sab, Y. (2015): Designing a smart security camera system. *23rd Signal Processing and Communications Applications Conference.*

Hammoudi, S.; Benaouda, A.; Harous, S.; Aliouat, Z. (2016): Load balancing in the cloud using specialization. Ubiquitous Computing. *Electronics & Mobile Communication Conference.*

Lai, J.; Chen, G. (2016): Design of metal detector based on single chip microcomputer. *International Conference of Online Analysis and Computing Science.*

Lei, X.; Liao, X.; Huang, T.; Li, H. (2010): Development of smart security system. *6th International Conference-Cloud System and Big Data Engineering.*

Li, H.; Ota, K.; Dong, M. (2018): Learning iot in edge: deep learning for the internet of things with edge computing. *Edge Computing for the Internet of Things*, vol. 2, no. 2, pp. 96-101.

Li, W.; Logenthiran, T.; Phan, V. T.; Woo, W. L. (2019): A novel smart energy theft system (sets) for IoT-based smart home. *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531-5539.

List of School Massacres by Death Toll (2019): https://en.wikipedia.org/wiki/List_of_school_massacres_by_death_toll.

Madhav, M.; Seema, S.; Jayalekshmi, K. R.; Taskeen, N. (2017): Advance alert for ambulance pass by using iot for smart city. *International Journal of Engineering Science and Computing*, vol. 7, no. 6, pp. 13219-13221.

Marko, K.; Toivo, V.; Argo, R. (2016): Case study of smart city lighting system with motion detector and remote control. *IEEE International Energy Conference*.

Raghavan, N.; Ullas, S. (2107): Infant movement detection and constant monitoring using wireless sensors. *International Conference on Wireless Communications, Signal Processing and Networking*.

Ruinian, L.; Tianyi, S.; Nicholas, C.; Jiguo, Y.; Jason, C. (2017): IoT applications on secure smart shopping system. *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1945-1954.

Shoaib, M.; Hans, S.; Paul, H.; Ozlem, I. (2016): A hierarchical lazy smoking detection algorithm using smartwatch sensors. *18th International Conference on e-Health Networking, Applications and Services.*

Vermesan, O.; Friess, P. (2014): *Internet of Things from Research and Innovation to Market Development*. River Publisher Series in Communication.

Vijayalakshmi, M.; Padmashree, D.; Meenaxi, R. (2016): Packet tracer simulation tool as pedagogy to enhance learning of computer network concepts. *IEEE 4th International Conference on MOOCs, Innovation and Technology in Education.*

Yi, L.; Chao, Y.; Li, J.; Xie, S.; Yan, Z. (2019): Intelligent edge computing for IoT-based energy management in smart cities. *IEEE Network*, vol. 33, no. 2, pp. 111-117.