# Student Name

192002

**Securing Network Applications via embedded Security Model**

MSc Computer science with placement MSc Project Final Report

School of Computer Science and Technology Supervisor:

Block and Academic year: BLK1-6 & 2020/21

# Abstract

The adoption of Securing Network Applications via embedded Security Model s and services has resulted in a significant increase in interest in IoT. Institutions have started developing various embedded-based gadgets ranging from tiny personal devices like the smartwatch to a comprehensive network of intelligent grids, mining, manufacturing, and autonomous driver-less automobiles. The abundance and pervasiveness of data have attracted prospective hackers for cyber-attacks and data theft. One of the most significant concerns in embedded-system is security. The primary goal of this research is to offer a novel model based on a machine learning algorithm for detecting and mitigating botnet-based attacks in an embedded network system. Our proposed approach addresses the security challenges faced by bot attacks. Various machine learning techniques are used, such random forest and Decision tree algorithms. We used to developing a model where the BoT-IoT dataset trains data. A reference point selected the best algorithm based on accuracy percentage. .

# Acknowledgements

# Dedication

**This project is dedicated to my parents**

# Key words

**Cyber security, Network security, application security , embedded system**

# CONTENT LIST

**LIST OF TABLES**

# LIST OF FIGURES

**LIST OF SYMBOLS AND NOTATIONS**

# LIST OF ABBREVIATIONS

# Introduction

We live in a connected era. Organizations are more technologically savvy than before, and as technology advances, organizations' security postures must also evolve. Network security is a crucial subject to understand with so many devices talking with one another over-connected, wireless, or cell phones.

"Network Security is the process of taking hardware and virtual preventative precautions to protect the underlying network equipment from unauthorized users, abuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secured environment for computers, users, and programmers to perform their permitted critical functions within a secure environment," as according to SANS Institute.

**What exactly is network security?**

The practice of adopting preventative actions to safeguard the underlying networking infrastructure against illegal access, abuse, malfunction, alteration, destruction, or incorrect disclosure is known as network security.

The Internet has become an integral component of our daily lives without question. Many individuals in today's generation rely on the Internet for various professional, social, and personal purposes. But are you sure that your network is protected?

Many individuals seek to harm our Internet-connected machines, breach our privacy, and render Internet services inoperable. Given the frequency and diversity of present assaults and the danger of new and more devastating attacks in the future, network security has emerged as a critical subject in the field of cyber security. Implementing network security measures enables computers, users, and applications to carry out their official essential duties in a safe facility.

Now that we've defined network security let's look at the two basic types of network assaults.

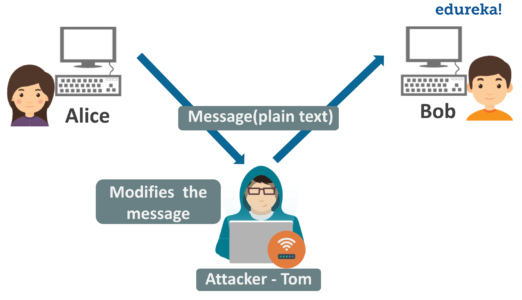
**What exactly is a embedded network security threat?**

A network attack is any technique, procedure, or means that is used maliciously to attempt to breach network security. Security is the process for avoiding network assaults across a particular network infrastructure, but the strategies and methods employed by the attacker further differentiate whether the attack is an active cyber attack, a passive type attack, or a mixture of the two.

To illustrate the distinction between aggressive and passive network attacks, examine a basic network assault scenario.

1. **Active Attacks**

An network device exploit is one in which the attacker attempts to alter data on the destination or data ready to travel to the target.



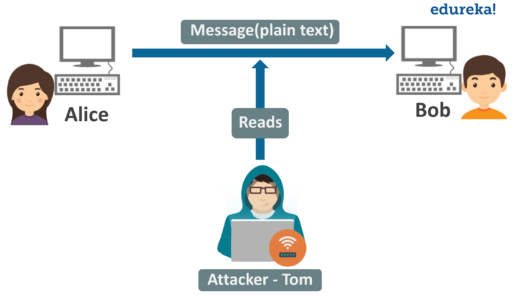
Let's meet Alice and Bob. Alice want to speak with Bob, but distance is an impediment. As a result, Alice sends an email to Bob through a network that is vulnerable to cyber threats. Tom, who is on the same network as Alice and Bob, is also present. Because the data flow is now available to everyone on the network, Tom modifies a piece of a permitted message to generate an unlawful impact. A notification that says "Allow BOB to view secret file X" is changed to "Allow Smith to read confidential file X."

Current network assaults are frequently forceful, obvious attacks that victims become aware of as soon as they occur. Active assaults are extremely harmful in nature, frequently locking out users, deleting memory or data, or obtaining unauthorized access to a targeted device or network.

1. **Passive Attacks**

A passive network assault is one in which a system is observed & occasionally searched for ports and services and weaknesses, but no system resources are affected.

Take a look at the previous example:



Alice sends emails to Bob through a network that is vulnerable to cyber assaults. Tom, and are on the same network as Alice and Bob, keeps an eye on the data transit between them. Assume Alice gives Bob some sensitive information, such as bank account information, in plain text. Tom has easy access to the data and can use it for nefarious reasons.

The goal of a passive assault is to obtain access to the computer and network and gather data without being detected.

As a result, network security entails integrating various hardware and software approaches required to protect the underlying network architecture. You can identify new risks before they reach your network and jeopardize your data if you have effective network security in place.

**Different types of network security**

A network security system is made up of numerous components that work together to improve your security posture. The following sections go through the most popular network security components.

1. **Control of Access**

You should be able to prevent unauthorized users and devices from accessing your network in order to keep prospective attackers out. Users having network access should only be able to access the resources for which they have been granted access.

1. **Application security**

Refers to the hardware, software, and processes that may be utilized to track and secure application vulnerabilities that attackers can use to access your network.

1. **Firewalls**

Devices or services that operate as gatekeepers, determining what enters and exits the network. To accept or deny traffic, they employ a set of predefined rules. A firewall can be either software or hardware.

1. **VPN**

A virtual private network (VPN) encrypts the connection between an endpoint and a network, often over the Internet. It authenticates communication between a device and a secure network in this manner, forming a secure, encrypted "tunnel" through the open internet.

1. **Analytics for Behavior**

You should understand regular network activity so that you may detect anomalies or network breaches as they occur. Behavioral analytics technologies detect actions that differ from the usual.

1. **Wireless Safety**

Wireless communication is less secure than conventional networks. Mobile devices and applications are increasingly being targeted by cybercriminals. As a result, you must restrict which devices may connect to our network.

1. **IPS**

Analyze network traffic to detect and prevent attacks, frequently by matching network activity fingerprints with databases of known attack strategies.

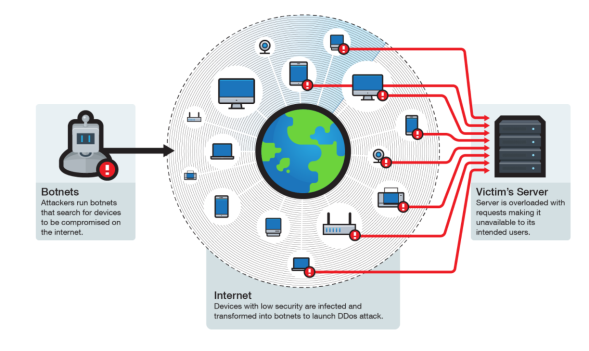
# Problem

Because of the increased use of digital communication in this digital era, cyber security is critical for maintaining a high degree of safety. Traditional security system firewalls and encryption are insufficient to prevent increasing cyber assaults. There is a demand for intrusion detection systems that can interface with existing systems and provide data security at a high level. Detecting unusual abnormalities is a practical approach to generate alarms for security managers to explore dangers and new zero-day attacks that typical security systems cannot detect. Embedded gadgets are widely utilized in modern houses and have permeated every aspect of our lives; nevertheless, they have become an easy target for cybercriminals because they are not very complex. IoT devices may be exploited as bots to perform a distributed denial of service (DDoS) assault.The increasing proliferation of IoT devices is more vulnerable to hacking than desktop computers. The proliferation of computers has increased the number of IoT-based botnet assaults. Attack using a botnet. It is a sort of DDOS assault in which the attacker takes advantage of many IoT devices to overrun a specified target in DOS. This form of assault is difficult to detect since the device works correctly. The user or owner of the device will not realize whether his gadget is a victim of an attack; in rare situations, the device's operation may be delayed.

# Aim and Objectives

The aim of this project is to provide different available security models, with their sole purposes to secure embedded applications. The project aims to use a secure network model to provide security to the embedded system applications using machine learning algorithm.

Here is the overview of the system.



# Aim

This project work aims to Securing Network Applications via embedded Security Model using machine learning. The aim is also confined to show the performance of the detection of Botnet attack on embedded system.

# Objectives

* + - * In order to gain sufficient insights on the problem associated with this research area, a detailed survey will be conducted from the recent and reputed international journals.
      * Preprocessing the dataset which we download from internet to implemented in this work.
      * Implement machine learning algorithm to identify botnet attack on embedded system.
      * Program will be written using python programming to implement machine learning models.

.

# Artefact

# Benefit

Network security is the process of safeguarding your network. Networks can be private, such as those within businesses, or public. The process of securing a network entails preventing any abuse or illegal devices connected to the internet or its resources. Here are the benefits of securing network application via embedded software.

* Protect data
* Prevents cyber attack
* Levels of access
* Centrally controlled

# Report organization

The rest of the report is organized as mentioned below. This section ‘Introduction’ is likely to help the readers to locate the concepts easily and reach the respective chapters as per the technical requirement of a reader. Chapter 2- ‘Literature survey’ is the essence from the plethora of literatures related to the secure network application in embedded system using machine learning. The strengths and weaknesses of recent literatures had been reported in this section. Clear understandings from the literature is highlighted in this section. Chapter 3 – Artefact design & Development and Testing contains the mathematical models and the detailed procedure to implement and test the models using the proposed architecture. Detailed explanation of feature extraction methods and finally the classification methods have been presented in this chapter. Chapter 4 – ‘Testing and evaluation’ holds the proof of analysis conducted in this research. Clear justifications of the work undertaken in this project is proved with the help of suitable metrics relevant to the research domain. Chapter 5 – ‘Conclusions & Future work’ declares the results obtained in the form of accuracy values and comparison of the outputs with recent literatures. This chapter also suggests few of the directions on which a future researcher in the same topic would be interested to extend. Chapter 6 – Reflection presents the experiences by looking back at the events since the start of this project. The chapter ‘References’ lists the literature that holds, title, author names, year of publishing, journal title etc. Ultimately, the section ‘Appendices’ contains the progress reports 1- 4, other valid supporting evidences and any other relevant contents related to this project.

# Literature search findings

This section outlines the previous work with regards to the request of various. The literature is reviewed with the focus on how Machine Learning has been applied and helped with the anomaly detection of Frauds in healthcare.

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **References** | **Year** | **Approach** |
| **1** | [1] | **2018** | Work on IoT home network wireless network gateway system based on predetermined setup |
| **2** | [2] | **2019** | Examines the student's performance using the provided questionnaires |
| **3** | [3] | **2017** | provide a flexible solution for detecting unusual behavior in network traffic using k-means clustering without deep packet inspection. |
| **4** | [4] | **2014** | Focuses on developing a quality model network that takes into account the link between the characteristics of the qualities. |
| **5** | [5] | **2021** | network forensics to find new threats and validates the results with recollection forensics |
| **6** | [6] | **2018** | Discusses various open research issues related to IoT cybersecurity. |
| **7** | [7] | **2020** | Improve wireless connection and life quality of smart cities using IoT |
| **8** | [8] | **2019** | Implement network security on university |
| **9** | [9] | **2019** | Implement and configure IPs on university network |

In this 2018, author used the clever house design is accomplished using the simulation concept, which involves testing the system, network configuration, and wireless home gateway computer network equipment required by an intelligent home network on a Cisco packet tracer with the Internet of Things (IoT) control. Multiple electrical items may be controlled and monitored through a Smartphone while testing the IoT home network wireless network gateway system based on predetermined setup criteria. The Smart Home can improve energy efficiency, lower energy costs, regulate gadgets and transform the role of occupants.

In this 2019, this author presents the simulation tool's capabilities and examines the student's performance using the provided questionnaires. This research describes data to support the educational efficacy of using a simulation software tool for teachers and students interested in networking principles.

In this 2017, this authors study investigates the feasibility of adopting dependable security measures by employing machine learning algorithms to conduct traffic categorization. The new framework, built on existing parallel hardware, seeks to provide a flexible solution for detecting unusual behavior in network traffic using k-means clustering without deep packet inspection. The metadata for trace analysis is retrieved by utilizing the PCA png file type characteristics. K-means clustering is implemented utilizing several parallel APIs, and comparative analysis and performance concerns are discussed.

In this 2014, authors attempts to address this problem by giving a quality model for a safe embedded device with a sensor network. Every characteristic again for a secure embedded system is built using DeLone and McLean's success information system, and each includes sub criteria based on its attributes. The current study also focuses on developing a quality model network that takes into account the link between the characteristics of the qualities.

In this 2021, authors provides a methodology for risk hunting, which uses security device logs and network forensics to find new threats and validates the results with recollection forensics. This revelation has resulted in new guidelines that will allow border protection to be more dynamic and effective in dealing with previously undiscovered security risks.

In this research conducts an exhaustive comparison of past surveys on the issue and demonstrates its uniqueness compared to previous studies. It discusses nine application domains in-depth and includes security needs, modeling techniques, types of threats, protocols, and technologies for those nine application domains. In addition, the study conducts a thorough assessment of specific existing methods and techniques described in the literature for protecting the security and privacy of IoT devices. Finally, it discusses various open research issues related to IoT cybersecurity.

In this , authors seeks to showcase a virtual network solution of 5G IoT smart cities in Cisco Packet Tracer visual simulation software. The rationale behind intelligent buildings is to improve wireless connection and life quality and safety in different facets of people's lives. For every smart building, the 5G IoT architecture addresses security, fire safety, energy management, and a wide range of intelligent devices such as RFID, lighting, and watering plants.

In this , the author's used university integrated network design has been presented. The architecture provides future development since institutions may join 3115 more hosts, allowing for per-host expenditures like cabling. The extra hosts can be added without using all the allocated IP addresses. Furthermore, if there is a large budget, the network system may be more powerful, have a high level of security, and numerous servers can be added to the network. Finally, while the approaches for establishing a network in this study are inexpensive and effective, they are not confined to impoverished nations.

In this , The authors research how to use the tool to create a simulation model for university network. The research delves into topics such as topology design, IP address setting, and how to convey information in the form of packets in a single network, and the usage of virtual Local Area Networks (VLANs) to isolate traffic generated by different departments.

# 2.1 Research gap

There has been a lot of study on botnet detection models, but very few use feature engineering to perform a comprehensive review to avoid difficulties. Duplication and multicollinearity are common problems with massive datasets. Simply Using a standard dataset without feature engineering may solve problems; however, it introduces over-fitting of the component.

Most research is conducted using traditional datasets that lack embedded system traces and are ineffective. Identify a current botnet issue in embedded system. Furthermore, the majority of Real-time research is being conducted in the botnet detection model datasets with a significant degree of imbalance Researchers concentrate their efforts on achieving great accuracy by employing several MLAs on those datasets that are skewed. They fail to consider the impact of the imbalanced dataset used in the training module. The precision offered by that An unbalanced dataset may be deceptive. In addition, researchers calculate accuracy after the Training algorithm for assessing the MLA performance. This gives the accuracy of the training dataset and does not provide information about the skill of the model on the unseen data

The accuracy % obtained from such a process may be deceptive, and there is a chance of data overfitting or under fitting. Furthermore, accuracy may be difficult because the class imbalance dataset model is skewed toward the dominant class. We used a combination of feature engineering and machine learning techniques.

# Artefact Design & Development and Testing

In the project, there will be the features of the artefact that will be utilized. The list of features of the artefact include:

1. To do the analysis of the embedded system network traffic gotten from the network applications to be used.
2. To implement the model by use of machine learning
3. To test the model in its efficiency to deal with attacks from various threats.
4. Do a series of analysis to know any issues that may arise concerning the model and the potential threats.

In as much as the features of the artefact have been discussed, it is crucial to analyze the added features that the artefact gives the project in analyzing the network applications and the use of the adopted model. They include:

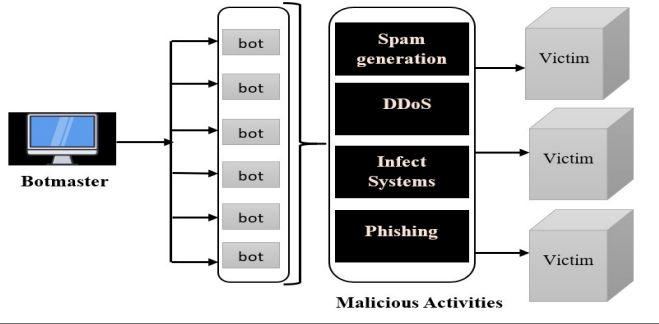
1. To do an analysis of the adopted model after implementation by use of machine learning. The analysis of model will add more value as it will show the efficiency of the model in dealing with embedded network security.
2. To undertake experiments that will show the different uses of the model and do the report and summary of the model.

# Methodology

This section provides a brief comprehensive overview of Botnet, embedded network security vulnerabilities, and machine learning algorithms employed in this project.

* **Botnet**

A botnet is a collection of multiple bots intended to undertake harmful actions on the targeted system and is managed by a single unit known as the botmaster using command and control protocol. Bots are infected computers automatically managed by the botnet and are used to undertake harmful actions. Botnet sizes range from a few hundred bots to 50,000 hosts in massive botnets. Attackers transmit botnet software, operate invisibly, with no visible trace of their existence, and remain practical and operational for years. The architecture of botnet show in below figure.



The essential component is the interaction between the botmaster and its connected bots. Communication with bots is required to provide orders to the bots to carry out destructive operations. Botmaster constantly stays hidden in the botnet network by utilizing minimal bandwidth and providing concealed services. Botmaster and bots constantly interact via the c&c server. Bots' primary purpose is to remain undetected until necessary to do given duties. Bots are challenging to recognize due to their concealed nature. They do not disturb regular host functions and remain silent until they receive a signal from the botmaster to undertake assigned operations.

* **Security vulnerabilities in IoT**

Intelligent technologies are being used in various public and private sectors, and they are rapidly becoming commonplace in everyday life. This resulted in a substantial danger to data privacy. In such a case, a computerized security system based on machine learning algorithms will be doomed.

Automated security systems based on machine learning are crucial for effectively preventing threats such as DDoS attacks, Man-in-the-middle attacks, botnet attacks, eavesdropping, and so on. Furthermore, most low-end IoT devices have a poor security system and are a target or even employed as a botnet for different security attacks.

* **Machine Learning**

2. **Implementation**

**Dataset**

Data was collected from nine business IoT devices infiltrated by legitimate botnets from two households. Mirai and BASHLITE are two of the most prevalent IoT-based botnets with previously proven destructive powers. The dataset is available for download from the internet.

1. **Data collection:** Using port mirroring on the switch via which the organizational traffic generally passes, record raw network traffic data (pcap format). To guarantee that the training data is free of harmful behaviors, IoT's typical traffic is gathered soon after being installed in the network.

**2. Feature extraction:** When a packet comes, we capture a behavioral picture of the hosts and protocols that sent it. The snapshot collects the packet's context by pulling 115 incoming traffic from many temporal frames to summarise all traffic that has occurred.

1. came from the same IP address in general.

2. came from the very same source MAC address and the same IP address.

3. transmitted between the source and destination IP addresses (channel), and 4. been transmitted between the source and destination TCP/UDP sockets (socket).

The dataset contains the following nine device normal & attack traffic.

● Danmini - Doorbell

● Ennio - Doorbell

● Ecobee - Thermostat

● Philips B120N/10 - Baby Monitor

● Provision PT-737E - Security Camera

● Provision PT-838 - Security Camera

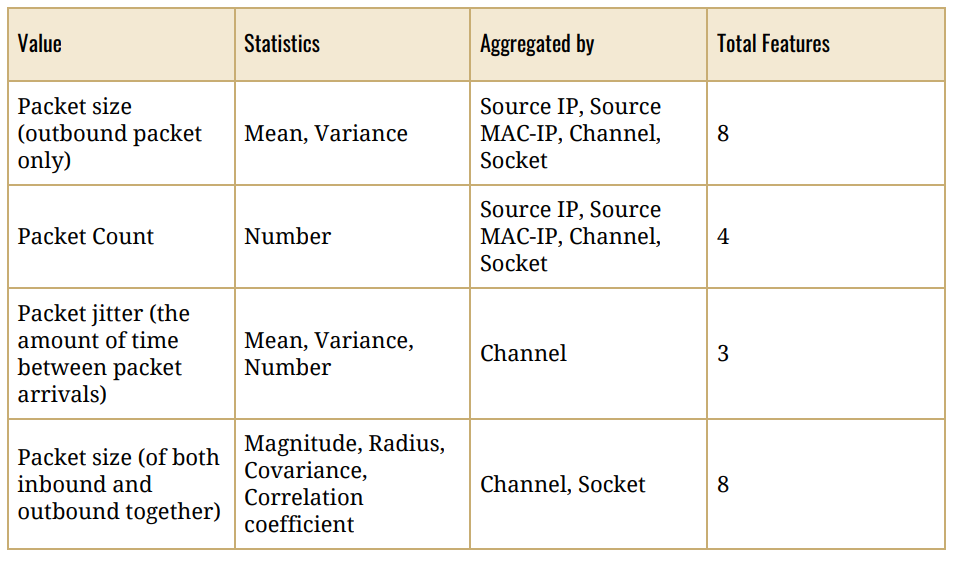
● Simple Home XCS7-1002-WHT - Security Camera

● Simple Home XCS7-1003-WHT - Security Camera

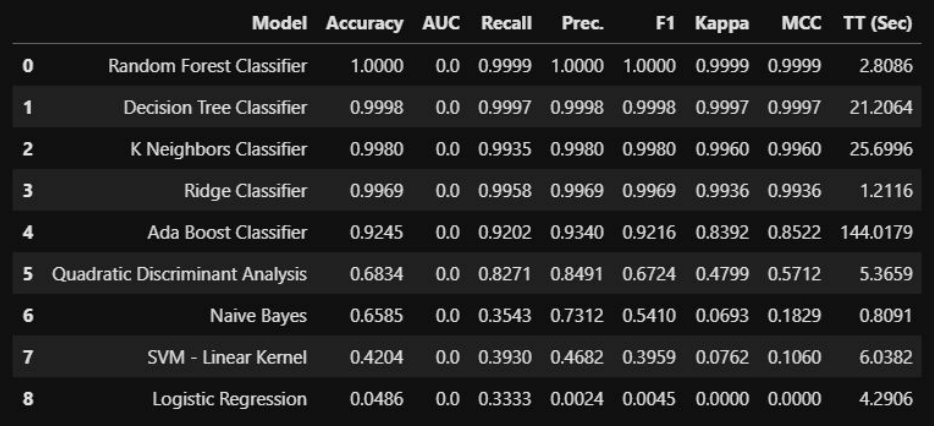
● Samsung SNH 1011 N - Web cam

The 115 characteristics listed above are taken from a collection of 23 features. the same set of 23 characteristics collected from the most recent 100ms, 500ms, 1.5sec, 10sec, and 1min time periods

These attributes may be calculated very quickly and gradually, allowing for real-time identification of malicious packets.



* **Training and testing**



.

# Evaluation

* 1. performance

.

* 1. Classification accuracy

# Conclusions & Further work

# Conclusions

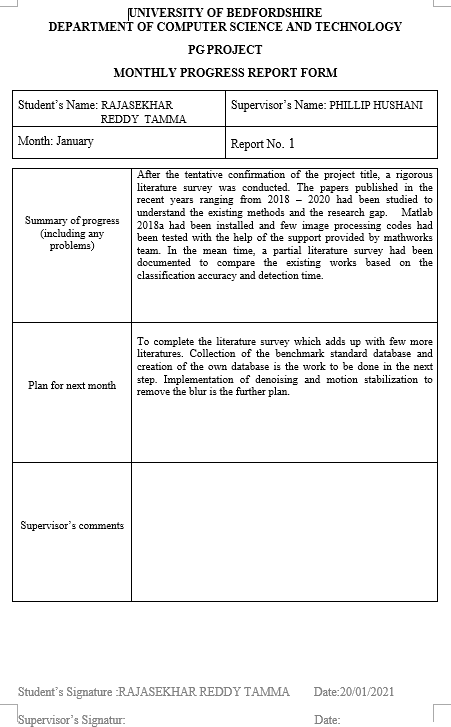
# Further work

The scope of this project is limited to identify

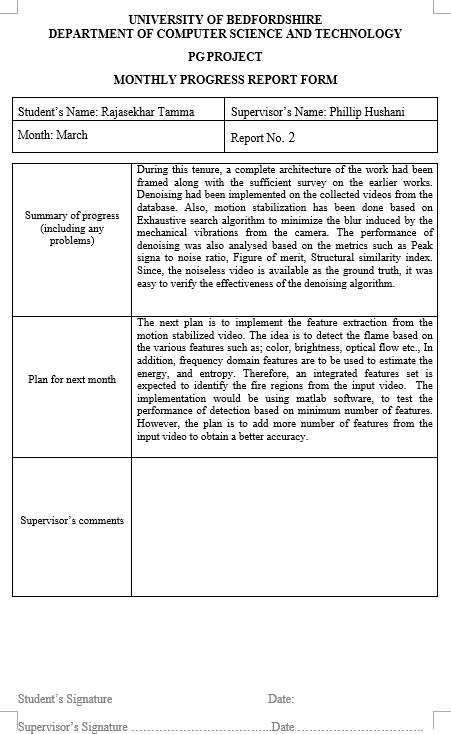
# References

# Appendices

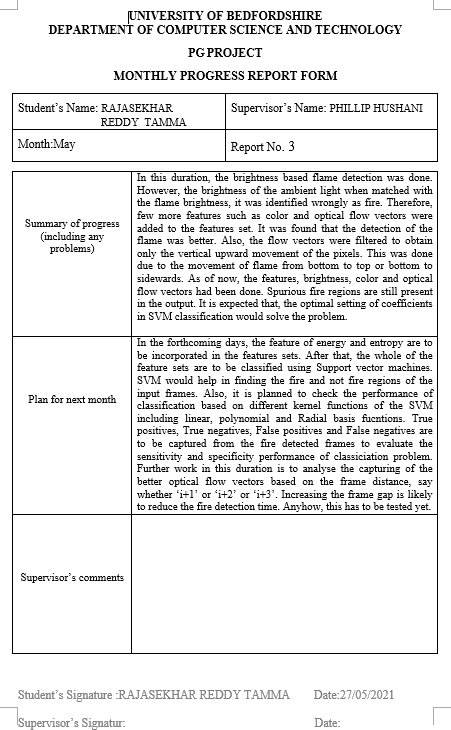
# Evidences of progress reports



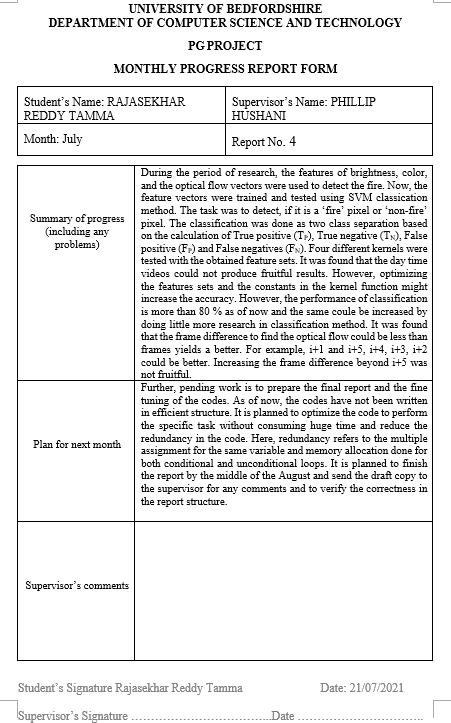
**Fig. A.1 Progress report 1**



# Fig. A.2 Progress report 2



**Fig. A.3 Progress report 3**



# Fig. A.4 Progress report 4