**INTRUSION DETECTION FRAMEWORK**

***A major project report submitted in partial fulfillment of the requirements***

***for the award of degree of***

**BACHELOR OF ENGINEERING**

# IN

**COMPUTER SCIENCE & ENGINEERING**

**SUBMITTED BY**

**Aadhaar Koul Cse - A1 (2020a1r040)**

**UNDER THE SUPERVISION OF**

**Mr. Saurabh Sharma**

**Assistant Professor, CSE**

****

**SUBMITTED TO**

**Department of Computer Science & Engineering**

**Model Institute of Engineering and Technology (Autonomous) Jammu, India**

**1 |** P a g e

**CANDIDATES DECLARATION**

I hereby declare that the work which is being presented in the major project report entitled, **“INTRUSION DETECTION FRAMEWORK”** in the partial fulfillment of requirement for the award of degree of B.E. (CSE) and submitted to the Department of Computer Science and Engineering, Model Institute of Engineering and Technology (Autonomous), Jammu, is an authentic record of our own work carried by us under the supervision of Mr. Saurabh Sharma , Asst. Prof. CSE Dept.. The matter presented in this report has not been submitted to any other University/Institute for the award of Batchelor of Engineering.

**Signature of the Student Dated: 30-05-2024**

**Aadhaar Koul Cse - A1 (2020a1r040)**

# Department of Computer Science & Engineering

# Model Institute of Engineering and Technology (Autonomous)

**Kot Bhalwal, Jammu, India (NAAC “A” Grade Accredited)**

## Ref. No.: MIET/CSE/2024/P10 Date:30/05/2024

## CERTIFICATE

Certified that this major project report entitled **“INTRUSION DETECTION FRAMEWORK”** is the bonafide work of **“Aadhaar Koul (2020a1r040), Computer Science Engineering, Model Institute of Engineering and Technology (Autonomous), Jammu”,** who carried out the major project work under my/our supervision during February 2024 - June 2024.

**Mr. Saurabh Sharma**

**Asst. Professor, CSE**

This is to certify that the above statement is correct to the best of my knowledge.

## Mr. Navin Mani Upadhyay

## Head CSE Department

**Model Institute of Engineering & Technology (Autonomous)**

# ACKNOWLEDGEMENTS

This Major Project opportunity was a great chance for learning and professional development. I would also like to express my deepest gratitude to **Mr. Saurabh Sharma**, Asst. Prof., CSE, for his precious guidance and knowledge which were extremely valuable for our study both theoretically and practically.

I must record my deep sense of gratitude to **Prof. (Dr.) Ankur Gupta (Director, MIET), Prof. (Dr.) Ashok Kumar (Dean Academics, MIET)**, and **Prof. Devanand Padha** for their guidance, constant inspiration, encouragement, and for their keen involvement throughout the course of present work.

Gratitude and thanks although mean a very small thing to convey my thanks to my parents who have always given me a parental source of love, motivation and strength right from the journey of my life.

Bearing in mind previous I am using this opportunity to express my deepest gratitude and special thanks to the faculty members who in spite of being extraordinarily busy with their duties, took time out to hear, guide and keep me on the correct path and allowing me to carry out my project at their esteemed organization and extending during the training.

We perceive this opportunity as a big milestone in our career development. We will strive to use gained skills and knowledge in the best possible way, and We will continue to work on their improvement, in order to attain desired career objectives. Hope to continue cooperation with all of you in the future.

**Aadhaar Koul Cse - A1 (2020a1r040)**

|  |  |  |
| --- | --- | --- |
|  | **CONTENTS** |  |
|  | Page No. |
| **ABOUT** | PREFACE | **3** |
|  | Acknowledgement | 4 |
|  | Abstract | 6 |
|  | Motivation | 7 |
|  | Background and Context | 8 |
|  | Problem Statement and Justification | 8 |
|  | Solution | 12 |
|  | Introduction | 13 |
| **CHAPTER 1** | **Theory** | **25** |
|  | 1.1 Technical Stack | 25 |
|  | 1.2 Languages | 25 |
|  | 1.3 Computer Vision Module | 26 |
|  | 1.4 Surveillance Module | 30 |
|  | 1.4.1 .1Fig : EP-32 Cam | 30 |
|  | 1.4.2 Features | 31 |
|  | 1.4.3 Circuit | 31 |
|  | 1.4.4 Video Streaming Server | 31 |
|  | 1.4.5 Install the ESP32 add-on | 31 |
|  | 1.4.6 Code | 32 |

|  |  |  |
| --- | --- | --- |
| **CHAPTER 2** | **IOT Module** | **36** |
|  | 2.1 Ultra sonic sensor | 40 |
|  | 2.2 Humidity and temperature sensor | 40 |
|  | 2.3 Esp8266 | 40 |
| **CHAPTER 3** | **Blynk Cloud Module** | **46** |
|  | 3.1 Components of the Blynk IoT Platform | 46 |
|  | \ 3.2 How Data Flows From Device to Blynk | 47 |
|  | 3.3 Send Data With Blynk Library Firmware API | 47 |
| **CHAPTER 4** | **Network Gateway Module** | 49 |
| **CHAPTER 5** | **Honeypot Module** | 54 |
| **CHAPTER 6** | **Features of ESP8266** | **54** |
| **CHAPTER 7** | **Flashing code to ESP8266** | **55** |
|  | 7.1 Installing ESP8266 Board in Arduino IDE | **55** |
|  | 7.2 Flashing Steps | **57** |
|  | 7.3 Developing the Honeypot Script | **58** |
| **CHAPTER 8** | **One Stop Solution Framework** | **63** |
|  | 8.1 Admin Control Application | **65** |
|  | 8.2 Implementation | **69** |
|  | 8.3 Libraries Used | **69** |
|  | 8.4 Use | **69** |
|  | 8.5 Module Code snippets | **72** |
|  | 8.6 Login Page | **72** |
|  | 8.7 Code | **72** |
|  | 8.8 Dashboard Page | **73** |
|  | 8.9 Code | **73** |
| **CHAPTER 9** | **Proposed Framework** | **78** |
|  | 9.1 Initialization | **80** |
|  | 9.2 Activity Detection | **81** |
|  | 9.3 Intrusion Detection | **81** |
|  | 9.4 Honeypot Trigger | **81** |
|  | 9.5 Admin's Actions | **81** |
|  | 9.6 Final State - Keep True | **81** |
| **CHAPTER 9** | **Estimations and Expectations** | **82** |
|  | 9.1 Results | **83** |
|  | 9.2 Future Scope | **84** |

|  |  |  |
| --- | --- | --- |
| **REFERENCES** |  | **85** |
| **APPENDIX** |  | **86** |

# LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| **Fig No.** | **Figure** | **Page No.** |
| Figure1 | Data Breach Statistics | 9 |
| Figure2 | Data Breach Statistics 2 | 10 |
| Figure3 | Global cyber Study | 11 |
| Figure 4 | Firewall | 13 |
| Figure 5 | IOT Enablers | 22 |
| Figure 6 | YOLO Python Implementation | 29 |
| Figure 7 | YOLO Working | 29 |
| Figure 8 | ESP32 CAM Circuit | 31 |
| Figure 9 | ESP CAM Code Implementation | 32 |
| Figure 10 | Surveillance Module Working | 34 |
| Figure 11 | Blynk Cloud Dashboard | 46 |
| Figure 12 | Network Dashboard | 53 |
| Figure 13 | Honeypot Script | 59 |
| Figure 14 | Honeypot Dashboard | 62 |
| Figure 15 | OSS Code Implementation | 63 |
| Figure 16 | OSS Working | 64 |
| Figure 17 | Android App Dashboard | 68 |
| Figure 18 | Android App Java Code | 72 |
| Figure 19 | Proposed Framework | 78 |
| Figure 20 | Proposed Workflow | 80 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Preface

In this document, we explore a comprehensive approach to developing a sophisticated Intrusion Detection Fgramework (IDF). The journey begins with the motivation and context that led to this project and traverses through the technical aspects, including computer vision, surveillance modules, IoT integration, and network security frameworks. Each section is meticulously crafted to provide clear insights and practical solutions for implementing a robust surveillance system. Our goal is to bridge theoretical knowledge with practical applications, thereby providing a valuable resource for professionals and enthusiasts in the field

3.