

**University Institute of Information Technology,**

**PMAS-Arid Agriculture University,**

**Rawalpindi Pakistan**

**MACHINE LEARNING USING**

**HIDS**

***By***

**Student Name 1 MUHAMMAD Ishfaq 17-ARID-1520**

**Student Name 2 MUHAMMAD ALI ARIF 17-ARID-1499**

**Student Name 3 MUHAMMAD WAQAS 17-ARID-1550**

***Supervisor*Dr./ ZEESHAN**

***Bachelor of Science in Computer Science (2020-2021)***

**The candidate confirms that the work submitted is their own and appropriate  
 credit hasbeen given where reference has been made to the work of others**.

**DECLARATION**

We hereby declare that this software, neither whole nor as a part has been copied out from any source. It is further declared that we have developed this software documentation and accompanied report entirely on the basis of our personal efforts. If any part of this project is proved to be copied out from any source or found to be reproduction of some other. We will stand by the consequences. No Portion of the work presented has been submitted of any application for any other degree or qualification of this or any other university or institute of learning.

Student Name 1 Student Name 2 Student Name 3

Muhammad Ishfaq Muhammad ali arif Muhammadwaqas

--------------------------- --------------------------- ---------------------------

**CERTIFICATE OF APPROVAL**

It is to certify that the final year project of BS (CS/IT/SE)“Project title” was developed by“Student **Name, Registration #”**, “Student **Name, Registration #”**and “**Student Name, Registration #”**under the supervision of“Supervisor Name” and that in their opinion; it is fully adequate, in scope and quality for the degree of Bachelors of Science in Computer Science/Information Technology/Software Engineering.

SIR ZEESHAN

---------------------------------------

**Supervisor**

---------------------------------------

**External Examiner (If any)**

---------------------------------------

**Administrator UIIT**

**Executive Summary**

In public places, there is often a need for monitoring people and different activities going on, which can be referred later for many reasons including security. Appointing humans for this task involves many problems such as increased employee hiring, accuracy problem, trust, no proof for later use, and also the fact that a human can remember things till a certain time limit. Talking about the current security system, they use dumb still cameras with a continuous recording facility ir-respective of the fact that any event may happen or not. Moreover they are usually pointing at a specific user defined locations so more than one cameras are required to cover the entire region.

To prevent all these problems from prevailing, the CSCS is developed. It is a surveillance system, which provides solution to many of these problems. It is a stand-alone application which doesn’t require any computer to operate. It monitors different situations using a camera which is able to rotate intelligently based on sensor messages and captures the scene in the form of video or photos later reference as well.

**C**ustomizable **S**urveillance **C**ontrol **S**ystem**(CSCS)** is a surveillance system that can be assigned a sensor type as in our case a heat sensor is used, it works accordingly, rotates the camera upon event detection and perform user defined actions like capturing video and stores them, for the future use.

It is an embedded system consisting of Linux fox kit with embedded a running server application also a camera, USB storage device and a sensor node base station is attached with fox kit. LAN communication is used by user to download the videos and to operate the system manually.

**Acknowledgement**

All praise is to Almighty Allah who bestowed upon us a minute portion of His boundless knowledge by virtue of which we were able to accomplish this challenging task.

We are greatly indebted to our project supervisor “Dr. Kashif Sattar” and ourCo-Supervisor “Dr. Tariq Ali” for personal supervision, advice, valuable guidance and completion of this project. We are deeply indebted to them for encouragement and continual help during this work.

And we are also thankful to our parents and family who have been a constant source of encouragement for us and brought us the values of honesty & hard work.

Student Name 1 Student Name 2 Student Name 3

Muhammad Ishfaq Muhammad ali arif Muhammad waqas

--------------------------- --------------------------- ---------------------------

**Abbreviations**

|  |  |
| --- | --- |
| **SRS** | Software Requirement Specification |
| **PC** | Personal Computer |
|  |  |
|  |  |
|  |  |

**Table of Contents**

**Introduction 1**

[1.1 Brief](#_Toc268523777) 2

[1.2 Relevance to Course Modules](#_Toc268523779) 2

[1.3 Project Background](#_Toc268523780) 3

[1.4 Literature Review](#_Toc268523780) 3

[1.5 Methodology and Software Life Cycle](#_Toc268523782) 5

**Problem Definition** 6

[2.1 Purpose](#_Toc268523795) 7

[2.2 Product Functions](#_Toc268523796) 7

[2.3 Proposed Architecture](#_Toc268523804) 7

[2.4 Project Deliverables](#_Toc268523806) 8

[2.5 Operating Environment](#_Toc268523807) 8

[2.6 Assumptions and Dependencies](#_Toc268523808) 8

**Requirement Analysis** 9

[3.1 Functional Requirments](#_Toc268523823) 10

[3.2 Non – Functional Requirments](#_Toc268523825) 11

[3.2.1 Usability](#_Toc268523787) 11

[3.2.2 Reliability](#_Toc268523787) 11

[3.2.3 Performance](#_Toc268523787) 11

[3.2.4 Supportability](#_Toc268523787) 11

[3.2.5 Design Constraints](#_Toc268523787) 11

[3.2.6 Licensing Requirements](#_Toc268523787) 11

[3.3 Use case Model](#_Toc268523823) 12

[3.3.1 Use Case Diagarm](#_Toc268523787) 12

[3.3.2 Actors Discription](#_Toc268523787) 16

[3.3.3 Use Case Discription](#_Toc268523787) 17

**The Design** 21

[4.1 UML Structural Diagrams](#_Toc268523830) 22

[4.1.1 Component Diagram](#_Toc268523787) 22

[4.1.2 System Component Diagram](#_Toc268523787) 24

[4.1.3 Package Diagram](#_Toc268523787) 25

[4.1.4 Deployment Diagram](#_Toc268523787) 26

[4.2 UML Behavioral Diagrams](#_Toc268523830) 27

[4.2.1 Activity Diagrams](#_Toc268523787) 27

[4.2.2 State Machine Diagrams](#_Toc268523787) 29

[4.3 UML Interaction Diagrams](#_Toc268523830) 30

[4.3.1 Sequence Diagrams](#_Toc268523787) 30

[4.4 Node Structure](#_Toc268523830) 31

[4.5 Communication Design Protocol](#_Toc268523830) 32

**Implementation** 33

[5.1 Communication Protocol Implementation](#_Toc268523830) 34

[5.2 PC Application Implementation](#_Toc268523830) 36

[5.3 Embedded Application Implementation](#_Toc268523830) 38

[5.4 Wireless Sensor Application Implementation](#_Toc268523830) 51

**Testing and Evaluation** 52

[6.1 Verification](#_Toc268523830) 53

[6.1.1 Functional Testing](#_Toc268523787) 53

[6.1.2 Static Testing](#_Toc268523787) 57

[6.2 Validation](#_Toc268523830) 57

[6.3 Usability Testing](#_Toc268523830) 57

[6.4 Unit Testing](#_Toc268523830) 57

* 1. [Integration Testing](#_Toc268523830) 57

6.6 [System Testing](#_Toc268523830) 57

**GUI** 58

**Future Work** 70

**References** 72

**List of Figures**

Fig 1.1 Block Diagram 8

Fig 2.1 Use Case Diagram 9

# Chapter 1: Introduction

This chapter provides the overview of the project. The first paragraph of every chapter should provide the chapter summary.

# Brief

COMPUTER Security is the main problem of today’s world as every thing is becoming digitalized. Today there is a vast data war going on .EVERY one is afraid of there data loss. WE are developing a system that will provide extra security to the system. OUR project will provide the users with a next level security. For example our project will provide log analysis, integrity checking, Windows registry monitor, Time based alerting system and active response. [5]. Our project title is Machine learning based on HOST INTRUSION DETECTION SYSTEM. THIS project has been chosen by learning about the system security. We will use c+ , java and python languages for coding and modifying the open source software .We are going to use open source software ossec and wazu . we have seen task bar .IN task bar there is a detail of system ongoing programs.

# Relevance to Course Modules

IN previous semesters we have studied different programming languages like C,C++,JAVA etc. NOW using these languages we are going to build our project .WE have also studied about database and we are going to use the MYSQL and postgresql database systems. Our project will be using open source ossec database as it contains a lot of information about different types of attacks and viruses.

# Project Background

It includes explanation of the idea behind the project. For example if the project is related to VoIP then this section describes that what is voice over IP & how it works.

Today everyone is busy in protecting their data. With advanced protection system the first line of defense is still the password authentication. A lot of people only use this authentication method to protect here data .BUT if any one can by-pass this authentication and if someone loses his password then he might never know when his data have been modified and he/she has lost his data. JUST to overcome this security issue we are going to develop this project .THUS this project will help us know the user about when was system logged in and what changes have been made.

# Literature Review

This section describes current trends/ research/ products etc. related to your project.

COMPUTER security is deﬁned as the protection of computing systems against threats to conﬁdentiality, integrity, and availability**.**[6].Confidentiality means that information is disclosed only according to policy. INTEGRITY means that information is corrupted and system performs correctly.[6].Security threats come from different sources **,** such as natural sources, accidents, Failure of services ,intruders etc.THERE are two types of intruders

* + 1. Internals: user having legal authorization to the system
    2. Externals: users having no authorization to the system

Techniques such as firewalls user authentication and data encryption are used as first line of defense against any intruder**.** If this first line of defense fails then the average users have no any other option.

OSSEC have developed an option for this purpose**. THE** option is HOST BASED INTRUSION DETECTION SYSTEM**. HIDS**  are applications that operate on information collected from individual computer system**. This property** allows it to analyze activities on host it monitors o high level of details which determine which processes or users are involved in malicious activities[7]**.**

1. The first intrusion detection model was proposed in 1987.since then three techniques have been used misuse detection or signature based detection
2. anomaly detection
3. hybrid detection

to detect attacks on the system.[8]

**AGENTS**: These are programs **/** coded software that are designed to perform a task. IT’s main purpose is to analyze whether anything or anyone has tried to access someone pc and tried to modify there data.[9]

CURRENTLY IDS are being used are of two types

**1.** NIDS: Network based intrusion detection system

**2.** HIDS: HOST BASED INTRUSION DETECTION SYSTEM

Today a lot of research is being made on IDS .RESEARCH started from 1980’s and still going on. OSSEC was developed in 2000 and has been open source for everyone. ALOT of products have also been developed LIKE wazuh , tripwire , HIDS cloud fare etc.

# Analysis from Literature Review (in the context of your project)

THUS it is very important for us to have a system that can work as second part of defense against intruders.THUS our project will help everyone to protect there data.

# Methodology and Software Lifecycle for This Piroject

WE are going to use AGILE MODEL for the development of our project.THE main reason to choose this methodology is because AT each stage we will be responsible to deleiver the product as it is being used.THUS it will enable us to save time and we will also be able to change any programming which has been done before .THUS it will help us understand and modify our project.[10]

We are also using object oriented concept as we will creating classes in different languages and understanding the open source code for any further editing.

METHODOLOGY which we will use will be the combination of structural object oriented programming .AS both will help us define what we are goping to do and how will we do it.

* + 1. Rationale behind Selected Methodology

Why you selected above methodology (such as structural and Object Oriented) and software life cycle for this project?

WE have selected these methodologies because we have studied the initial steps of these methodologies in our previous semesters and we have some understandings of these methodologies. THEY are also easy to understand and to do work with them is fun. SDLC we choose because our project is concerned with the system security and we will have to modify our project until or unless all the security conditions are not full met . FOR example Agile method help us modify any data at any iteration so we are going to use it. We can modify any part of our project at any time.

**Chapter 2: Problem Definition**

This chapter discusses the precise problem to be solved. It should extend to include the outcome.

# Problem Statement

# There is Lot of Software available on Google and different online store but some of these are paid or have limited trial. And free software sends a lot of alert popups and notification and to the user. Same system exist but And some user doesn’t like it. Thus the user sometimes ignores these alerts and simply becomes a victim.

We are hoping to learn software development , DATABASE , machine learning , python and other languages from this project.

# Deliverables and Development Requirements

Deliverables are following.

* Our system is free and easy to use.
* It will help the user to Protect private information
* Our system will notify user in case of Cyber Attack or any malware attack.
* No one will be able to change the data after our system installation except administrator
* Our System will notify the administrator if anyone want to change the data.

# Chapter 3: Requirement Analysis

Software Requirements Specification (SRS) report should be included in this chapter.

# Use Cases

|  |  |
| --- | --- |
| Use Case ID: | 1 |
| Use Case Name: | View intruders detected |
| Actors: | User |
| Description: | The admin will view the attacks made by any itruders. |
| Trigger: | Intruder alert notification |
| Preconditions: | 1.user must be an administrater  2.user must know about hids |
| Postconditions: | 1.user will know who trieed to attack the system  2.user will have the option to change system password |
| Normal Flow: | 1. User will login as an administrator 2. User will open hids 3. User will see the buttton for intders 4. User will view threats 5. User will take action on threats |
| Alternative Flows:  [Alternative Flow 1 – Not in Network] | 1. If user is not logged in as an administrator hids will not show any thing and will exit |
| Exceptions: | If user will not logg in as an administrator then hids will not show any record .And if user will enter will administrator priviliges he will see normal flow |
| Includes: |  |
| Special Requirements: |  |
| Assumptions: |  |
| Notes and Issues: |  |

|  |  |
| --- | --- |
| Use Case ID: | 2 |
| Use Case Name: | Log analysis |
| Actors: | User |
| Description: | The user will see who and when loged in |
| Trigger: | If user forgot password and enters wrong it will show as someone trieed to logged in with different password. |
| Preconditions: | User must know his password. |
| Postconditions: | User can see when someone tried to logged in as administrator.  User will also know if any guest account was used for entering the system. |
| Normal Flow: | 1.user must loggin as administrator  2.user must start hids  3.user can view log details by clicking on the log analysis button  4.user will see who and when his system was logged in |
| Alternative Flows:  [Alternative Flow 1 – Not in Network] | 1.If user log in as guest user then he will not see hids button and hids will stop and exit.  2.To view records hids must be started by administrator |
| Exceptions: | If user will not logg in as an administrator then hids will not show any record .And if user will enter will administrator priviliges he will see normal flow |
| Includes: |  |
| Special Requirements: |  |
| Assumptions: |  |
| Notes and Issues: |  |

|  |  |
| --- | --- |
| Use Case ID: | 3 |
| Use Case Name: | Threat found |
| Actors: | User |
| Description: | Admin will see the Threat found in the system |
| Trigger: | users Personel files have been tempered with. |
| Preconditions: | USER MUST BE LOGGED IN AS AN ADMINSTRATOR. |
| Postconditions: | User will see when his personel data was tempered with .  2.which data was tempered.  3.If user wants to save the tempered data or the origional file. |
| Normal Flow: | 1.user must loggin as administrator  2.user must start hids  3.user can view threats by clicking on the threats found button  4.user will see when and which file was tempered with.  5.user will have the option to save the original file or tempered file |
| Alternative Flows:  [Alternative Flow 1 – Not in Network] | .If user log in as guest user then he will not see hids button and hids will stop and exit.  2.To view records hids must be started by administrator |
| Exceptions: | If user will not logg in as an administrator then hids will not show any record .And if user will enter will administrator priviliges he will see normal flow |
| Includes: |  |
| Special Requirements: |  |
| Assumptions: |  |
| Notes and Issues: |  |

|  |  |
| --- | --- |
| Use Case ID: | 4 |
| Use Case Name: | Issues resolved |
| Actors: | User |
| Description: | All the actions done by the user to save his data using hids |
| Trigger: | If user want to know when he changed anything using hids |
| Preconditions: | User will have full record of when and what changes were made by the user |
| Postconditions: | IF user wants to know when he changed his data using hids |
| Normal Flow: | 1.user must loggin as administrator  2.user must start hids  3.user can view resolved issues by clicking on the issues resoled button  4.user will see when and which file was changed by him using hids. |
| Alternative Flows:  [Alternative Flow 1 – Not in Network] | 1. If user log in as guest user then he will not see hids button and hids will stop and exit.  2.To view records hids must be started by administrator |
| Exceptions: |  |
| Includes: | UC-1,UC-2,UC-3 |
| Special Requirements: |  |
| Assumptions: |  |
| Notes and Issues: |  |

# Functional Requirements

The functional requirements of “HIDS(host based intrusion detection system)“ are as following:

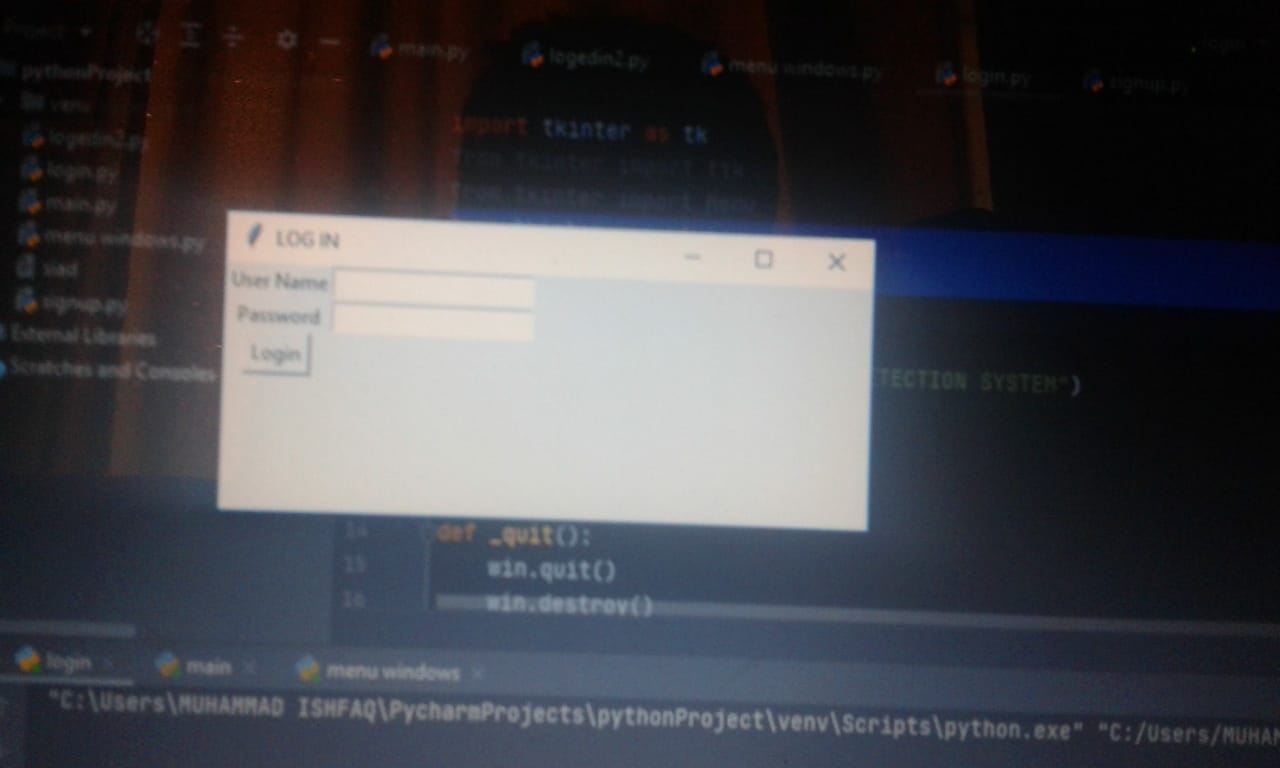
* User Module
* Login Module
* Logout Module
* Signup Module
* View log analysis Module
* Check intruders detected Module
* Threats found Module
* Issues resolved Module

# Non-Functional Requirements

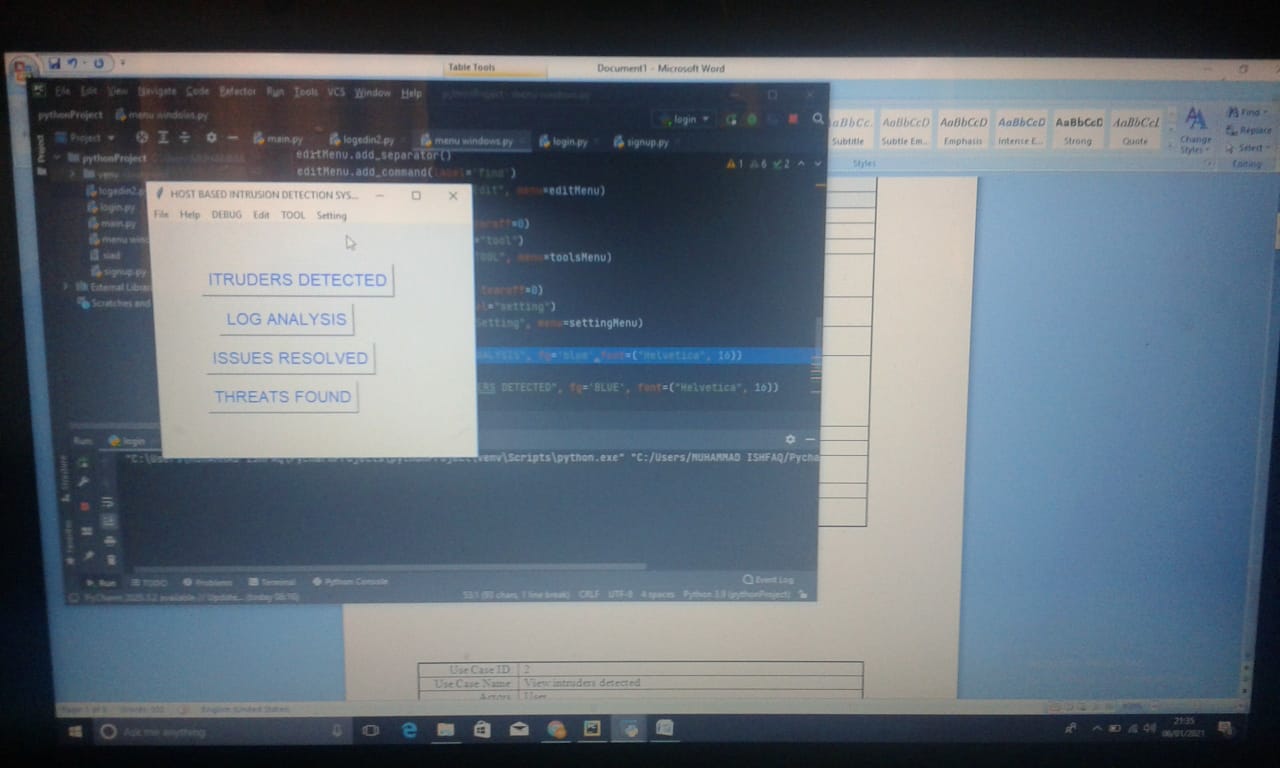
### Security Constraints

When user install system. He/she will create a user name and password, and He/She can only login in He/She enter correct password. If a unknown Person try to login administrative will be informed.

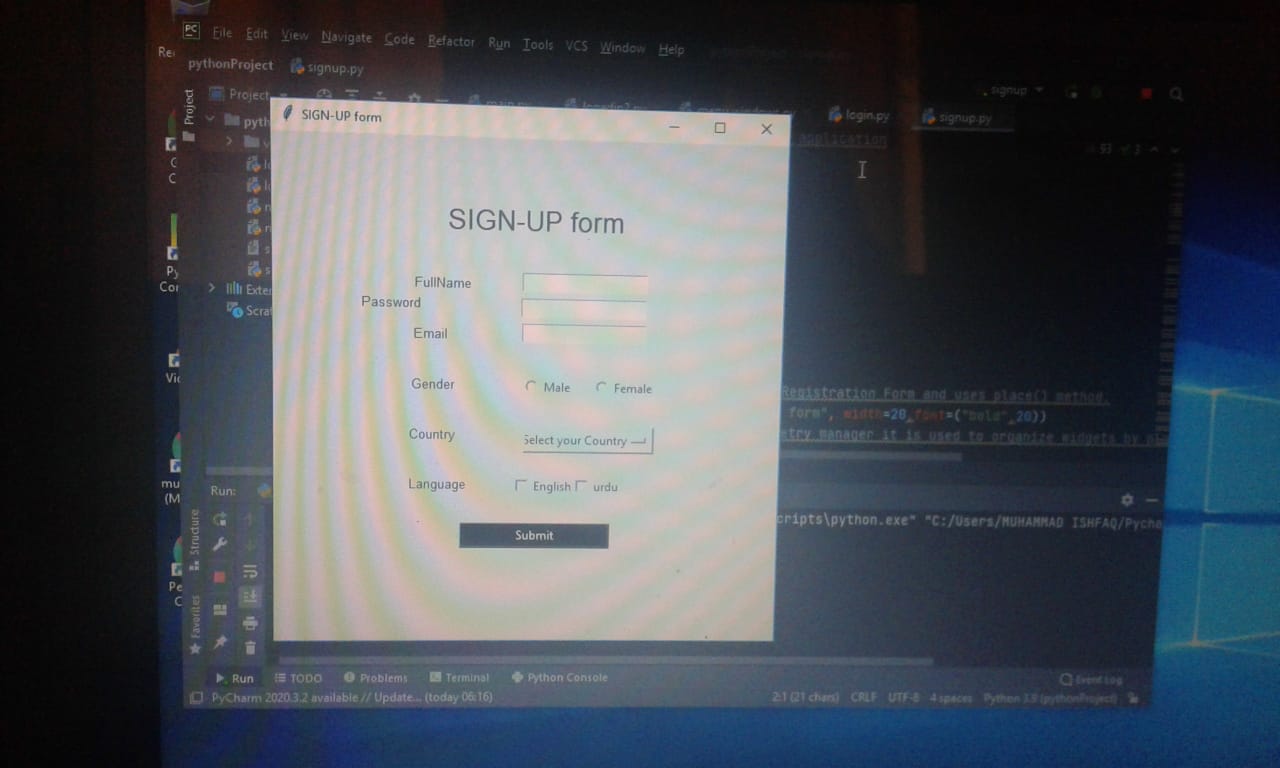
SCREEN SHOTS OF GUI



LOGIN window.



MAIN WINDOW.



SIGNUP FORM.

# Chapter 4: Design and Architecture

This chapter will discuss the design and architecture of your system.

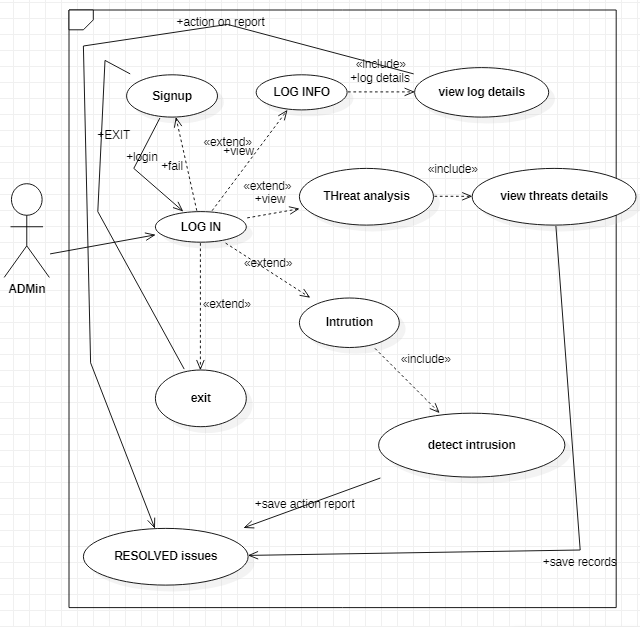
# System Architecture

Explain and justify the choice of system architecture for your project.

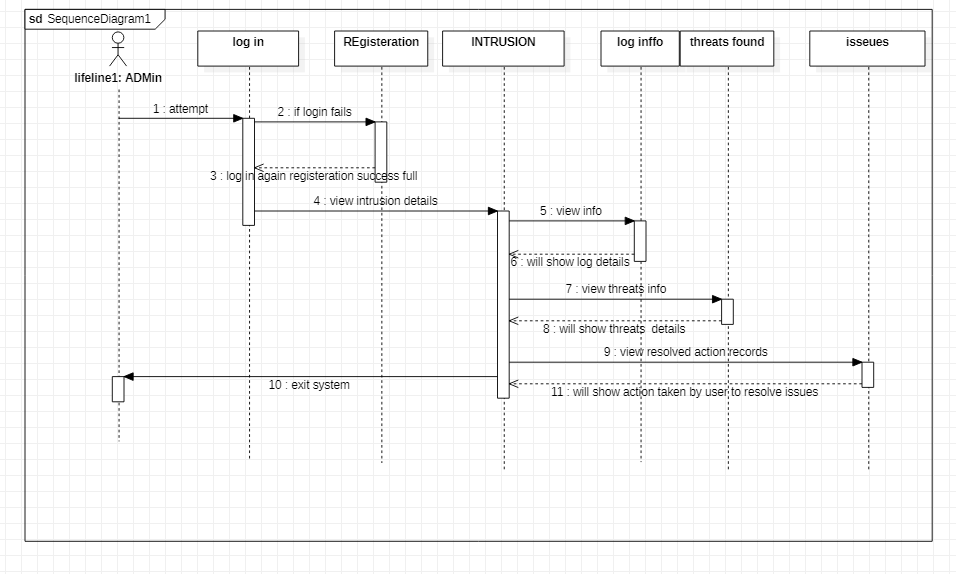
# System Design

As system design varies from system to system, therefore you are required to explore which design pattern is suitable for your system. For guidelines an IEEE Recommended Practice for Software Design Descriptions (section 5 and 6) is provided with this template.

**USE CASE DIAGRAM:**



**SEQUENCE DIAGRAM:**



# Chapter 5: Implementation

This chapter will discuss implementation details supported by UML diagrams (if applicable). You will not put your source code here.Any of the following sections may be included based on your project.

# Component Diagram

Present and explain component diagrams of your project.

# Network and Protocol Choice

It goes here.

# Choice of Object Middleware

RMI vs.CORBA vs. DCOM etc.

# User Interface

Details about user interface. (must enter user interfaces here )

# Chapter 6: Testing and Evaluation

This chapter may include the following sections.

# Verification

Verification section.

# Validation

Validation section.

# Usability Testing

Usability testing section.

# Module / Unit Testing

Unit testing.

# Integration Testing

Integration testing.

# System Testing

System testing.

# Acceptance Testing

Acceptance testing.

# Stress Testing

Stress testing.

# Hardware Configuration for Testing

Hardware configuration.

# Evaluation

Evaluation section.

# Deployment

Evaluation section.

# Maintenance

Evaluation section.

# Chapter 7: Conclusion and Future Work

This chapter concludes the project and highlights future work.

# Conclusion

Conclusion section.

# Future Work

Future work section.

# References

References to any book, journal paper or website should properly be acknowledged. Please consistently follow the style. The following are few examples of different resources i.e. journal article, book, and website.

1 Lyda M.S. Lau, Jayne Curson, Richard Drew, Peter Dew and Christine Leigh, (1999), Use Of VSP Resource Rooms to Support Group Work in a Learning Environment, ACM 99, pp-2. (Journal paper example)

2 Hideyuki Nakanishi, Chikara Yoshida, Toshikazu Nishmora and TuruIshada, (1996), FreeWalk: Supporting Casual Meetings in a Network, pp 308-314 (paper on web) http://www.acm.org/pubs/articles/proceedings/cscw/240080/p308-nakanishi.pdf

3 Ali Behforooz& Frederick J.Hudson, (1996), Software Engineering Fundamentals, Oxford University Press. Chapter 8, pp255-235. (book reference example)

4 Page Author, Page Title, http://www.bt.com/bttj/archive.htm, Last date accessed. (web site)