**SAVITRIBAI PHULE PUNE UNIVERSITY**

**A PRELIMINARY PROJECT REPORT ON**

**HOST INTRUSION DETECTION SYSTEM**

**FOR LOG FILES**

SUBMITTED TOWARDS THE

PARTIAL FULFILLMENT OF THE REQUIREMENTS OF

**BACHELOR OF ENGINEERING (Computer Engineering)**

**BY**

Shatruanjay Kumar Exam No: B120224245

Surjit Singh Exam No: B120224253

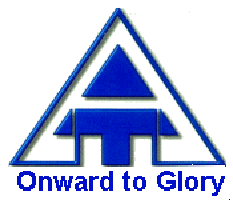
Sachin Yadav Exam No: B120224241

Yogesh Faguna Exam No: B120224260

Vikas Exam No: B120224257

**Under the Guidance of**

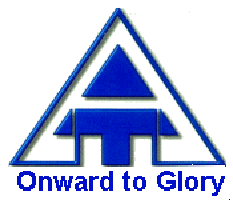
Prof. Sushma A Shirke



**DEPARTMENT OF COMPUTER ENGINEERING**

**ARMY INSTITUTE OF TECHNOLOGY**

**Dighi Hills, Pune – 411015**



**ARMY INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF COMPUTER ENGINEERING**

**CERTIFICATE**

This is to certify that the Project Entitled

**HOST INTRUSION DETECTION SYSTEM**

**FOR LOG FILES**

Submitted by

Shatruanjay Kumar Exam No: B120224245

Surjit Singh Exam No: B120224253

Sachin Yadav Exam No: B120224241

Yogesh Faguna Exam No: B120224260

Vikas Exam No: B120224257

is a bonafide work carried out by students under the supervision of Prof. Sushma A Shirke and it is submitted towards the partial fulfilment of the requirement of Bachelor of Engineering (Computer Engineering) Project.

|  |  |
| --- | --- |
| Prof. Sushma A Shirke | Prof. Dhore |
| Internal Guide | H.O. D |
| Dept. of Computer Eng. | Dept. of Computer Eng. |

**ACKNOWLEDGEMENT**

It gives us great pleasure in presenting the preliminary project report on **‘HOST INTRUSION DETECTION SYSTEM FOR LOG FILES’**.

I would like to take this opportunity to thank my internal guide **Prof. Sushma A Shirke** for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to **Prof. S.R. Dhore**, Head of Computer Engineering Department, Army Institute of Technology for his indispensable support, suggestions.

In the end our special thanks to **Library Staff, Lab attendants** for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

Shatruanjay Kumar

Surjit Singh

Vikas

Yogesh Faguna

Sachin Yadav

(B.E. Computer Eng.)

# INDEX

1. [Synopsis](#_bookmark0) 1

[1.1 Project Title](#_bookmark1) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

[1.2 Project Option](#_bookmark2) . . . . . . . . . . . . . . . . . . . . . . . . . . .. 2

[1.3 Internal Guide](#_bookmark3) . . . . . . . . . . . . . . . . . . . . . . . . . . . .. 2

* 1. [Technical Keywords (As per ACM Keywords)](#_bookmark5) . . . . . . . . . . .. 2

[1.5 Problem Statement](#_bookmark6) . . . . . . . . . . . . . . . . . . . . . . . . .. 2

[1.6 Abstract](#_bookmark7) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. 3

* 1. [Goals and Objectives](#_bookmark8) . . . . . . . . . . . . . . . . . . . . . . . .. 3
  2. [Names of Conferences / Journals where papers can be published](#_bookmark10) .. 3

**2** [**Technical Keywords**](#_bookmark13) 4

* 1. [Technical Keywords](#_bookmark15). . . . . . . . . . . . . . . . . . . . . . . . .. 5

3 [Introduction](#_bookmark16) 6

[3.1 Project Idea](#_bookmark17) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

[3.2 Motivation of the Project](#_bookmark18) . . . . . . . . . . . . . . . . . . . . . . 7

* 1. [Literature Survey](#_bookmark19) . . . . . . . . . . . . . . . . . . . . . . . . . . 7

4 [Problem Definition and scope](#_bookmark20) 9

* 1. [Problem Statement](#_bookmark21). . . . . . . . . . . . . . . . . . . . . . . . . .10
     1. [Goals and objectives](#_bookmark22) . . . . . . . . . . . . . . . . . . . . 10
     2. [Statement of scope](#_bookmark23). . . . . . . . . . . . . . . . . . . . . 10
  2. [Software context](#_bookmark24). . . . . . . . . . . . . . . . . . . . . . . . . . 11
  3. [Major Constraints](#_bookmark25). . . . . . . . . . . . . . . . . . . . . . . . . . 11
  4. [Methodologies of Problem solving and efficiency issues](#_bookmark26). . . . . . 12
  5. [Outcome](#_bookmark28) . . . . . . . . . . . . . . . . . . . . . . . . . . 13
  6. [Applications](#_bookmark29) . . . . . . . . . . . . . . . . . . . . . . . . . . 14
  7. [Software Resources Required](#_bookmark32). . . . . . . . . . . . . . . . . . . . 14

1. [Project Plan](#_bookmark33) 15
   1. [Project Estimates](#_bookmark34). . . . . . . . . . . . . . . . . . . .16
      1. [Reconciled Estimates](#_bookmark35) . . . . . . . . . . . . .16
      2. [Project Resources](#_bookmark36). . . . . . . . . . . . . . . 16
   2. [Risk Management w.r.t. NP Hard analysis](#_bookmark37) . . . . . . 17
      1. [Risk Identification](#_bookmark38). . . . . . . . . . . . . . ..17
      2. [Risk Analysis](#_bookmark39). . . . . . . . . . . . . . . . . .18
      3. [Overview of Risk Mitigation](#_bookmark43)  . ..19 [5.3 Project Schedule](#_bookmark44). . . . . . . . . . . . . . . . . . 21
      4. [Project task set](#_bookmark45). . . . . . . . . . . . . . . . .21
      5. [Task network](#_bookmark46). . . . . . . . . . . . . . . . . 22
   3. [Team Organization](#_bookmark48). . . . . . . . . . . . . . . . . . 22
      1. [Team structure](#_bookmark49). . . . . . . . . . . . . . . . . 23
2. [Software requirement specification](#_bookmark51). . . . . . . . . . . . 24

6.1 Introduction ……………………………………………25

6.1.1 Purpose and Scope of Document………… 25

6.1.2 Overview of responsibilities of Developer…...25

6.2 Usage Scenario………………………………………..25

6.2.1 User proﬁles …………………………………25

6.2.2 Use-cases …………………………………….25

6.2.3 Use Case View ………………………………26

6.3 Functional Model and Description ……………… …. 27

* + 1. Data Flow Diagram ……………………… 27

6.3.2 Activity Diagram: ……………………….… 31

7 [References](#_bookmark87) 32

**List of Tables**

1. [Software Resources Requirements](#_bookmark31) ………………………..16
2. [Risk Table](#_bookmark40) ………………………………………………….20
3. [Risk Probability definitions](#_bookmark41) ………………………………..20
4. [Risk Impact definitions](#_bookmark42) …………………………………… 20

CHAPTER 1

SYNOPSIS

### PROJECT TITLE

Intrusion Detection System

### 

### PROJECT OPTION

Internal project

### INTERNAL GUIDE

Prof. Sushma A Shirke

### TECHNICAL KEYWORDS (AS PER ACM KEYWORDS)

IDS

IPS

Firewall

Honeypot

DDoS

Anomaly

Shell

NID

HID

### PROBLEM STATEMENT

### We propose to build and demonstrate a novel system for rapid development and deployment of effective and cost-sensitive IDSs. We consider intrusion detection as a classification problem, that is, we wish to classify each audit record or log records into one of a discrete set of possible categories, normal or a particular kind of intrusion. However, before we can apply classification algorithms, we need to first select and construct the right set of system features that may contain evidence (indicators) of normal or intrusions. We will develop an automatic feature selection and construction system to systematically discover and construct predictive features that can be used to build effective misuse and anomaly detection models.

* 1. **ABSTRACT**

An Intrusion Detection System (IDS) is a software application or device that monitors the system or activities of network for policy violations or malicious activities and generates reports to the management system. A number of systems may try to prevent an intrusion attempt but this is neither required nor expected of a monitoring system. The main focus of Intrusion detection and prevention systems (IDPS) is to identify the possible incidents, logging information about them and in report attempts. In addition, organizations use IDPS for other purposes, like identifying problems with security policies, deterring individuals and documenting existing threats from infringing security policies. IDPS have become an essential addition to the security infrastructure of nearly every organization. Various methods can be used to detect intrusions but each one is specific to a specific method. The main goal of an intrusion detection system is to detect the attacks efficiently. Furthermore, it is equally important to detect attacks at a beginning stage in order to reduce their impacts. This research work proposed a new approach called outlier detection where, the anomaly dataset is measured by the Neighborhood Outlier Factor (NOF). Here, trained model consists of big datasets with distributed storage environment for improving the performance of Intrusion Detection system. The experimental results proved that the proposed approach identifies the anomalies very effectively than any other approaches.

### GOALS AND OBJECTIVES

The purpose of intrusion detections systems (IDSs) is to monitor networks or systems with the express purpose of identifying and responding to suspicious activity.

### NAMES OF CONFERENCES / JOURNALS WHERE PAPERS CAN BE PUBLISHED

* IEEE/ACM Conference/Journal 1
* Conferences/workshops in IITs
* Central Universities or SPPU Conferences
* IEEE/ACM Conference/Journal 2

## CHAPTER 2

## TECHNICAL KEYWORDS

### TECHNICAL KEYWORDS

IDS

IPS

Firewall

Honeypot

DDoS

Anomaly

Shell

Network based Intrusion Detection

Host based Intrusion Detection

Tunnel

Port Scanning

TCP

Attacks

Snort

Tiger

Trojans

Access Points

ADS Blocker

Logs

Client and Server

IP Address

Port and socket

HTTP , SYN , UDP

Ping

## 

## CHAPTER 3 INTRODUCTION

### PROJECT IDEA

Our project is about making a host based intrusion detection system which is compatible with any traditional security system. We just need to set up a system and then we can easily work on the host and the network. We want our project to be based on open source tools and no proprietary software.

### MOTIVATION OF THE PROJECT

* Most Common Attacks (source CSI/FBI)

In year 2014 most common attacks were:

*1. Virus (78%)*

*2. Insider Abuse of Net Access (78%)*

3. Laptop theft (55%)

*4. Denial of Service and System Penetration (40%)*

*5. Unauthorized Access by Insiders (38%)*

(Italic shows the items, which IDSs can decrease)

* Developing absolutely secure systems is not possible
* Most existing systems have security flaws
* Abuses by privileged insiders are possible
* Not all kinds of intrusions are known
* Quick detection of intrusions can help to identify intruders and limit damage
* IDS serves as a deterrent

### LITERATURE SURVEY

The aim of [1] is to address the issues of information security and describes the security needs of an organization to protect their critical information from attacks. A well trained staff and analysts are required to continuously monitor the system. But still a huge effort is required to construct new security strategies in this system which are discussed in [2], [9]. [2] Provides a multilayer approach in IDPS to monitor a single host. Multilayer approach consists of three layers. File Analyzer, System Resource Analyzer and Connection Analyzer. The advantage of this technique [2] is that it provides both signatures based and anomaly based detection and prevention. The drawback in Multilayer approach is that the IDPS require a large amount of memory to store the data of the system and network traffic.

Proventil desktop is software based solution [3] which detects and protects the system from network layer up to application layer by known and unknown attacks. This software has great flexibility to set

different type of filtering rules. The major drawback of HIPS is its high rate of false-positives. A lot of time and trained staff is required to monitor the IDPS [3]. The idea discussed in [4] helps an organization to take an informal decision in order to select the IDPS. The proposed model divides the IDPS into two types,in-source and out-source. Provide a security to an organization against attacks is a key business of Managed Security Services Provider (MSSP) [4]. MSSP spend most of the time to examine new technology to secure the information better than before. A risk is possible if MSSP do not exactly know the customer requirements of IDPS. According to [5], Snort and source fire are best IPSs for a multinational company. Snort [5] product provides high flexibility that allow to the user to self-configure and modify its source code by using source fire. The major drawback of Snort is that it uses only signature based technique to detect the intrusion but if anomaly behavior occur then it will not be possible for SNORT to detect that anomaly attack [5]. Harley [8] defines the difference between host based and network based intrusion detection and prevention system. This paper describes two types of network intrusion detection system: Promiscuous-mode and Network-node. The main disadvantage observed is that this IDS only responds to the signature based detected attacks but not to the anomaly based detected attacks. So still there is a need of human interaction who took real time action to resolve issue [8].

Novel string matching technique [9] is an optimization of other matching algorithms. Novel string matching algorithm breaks the string into small sets of state machines. Each state machine recognizes the subset of string. If any suspicious behavior occurs then the system broadcasts the information about intruder to every module (state machine) which holds the data base in order to define rules and compares the signatures of intruder with predefined detected signatures. This algorithm is most efficient and ten times faster than the other existing systems and it consumes less resources. The major issue is its practical implementation and it requires a large amount of memory. This algorithm is not capable to detect the anomaly behavior of the intrusion as in [7].

According to S. Mrdovi and E. Zajko [10], Distributed IDS is used to analyze the system in which multiple sensors are placed in selected network segments that observe the network traffic behavior. SNORT is used as an analysis engine. MySQL is used to log the events with the help of SNORT. Distributed IDS is managed by management console which monitors and configures the IDS. This IDS provides a greater protection against attacks because multiple computers are continuously monitoring and preventing the network from malicious attacks [7]. Large memory and well trained security analysts are required to implement and continuous management of the system [7].

This paper [11] describes the security of IDS. It highlights the two different techniques of IDS. Misuse detection and anomaly detection. Three different approaches data mining, data fusion and immunological based approach used in IDS. This paper provides brief information about existing intrusion detection technology. It evaluates the challenges and future directions of intrusion detection technology. The approaches that are discussed in [4], [9] are much sufficient for IDPS to detect and respond to anomalies in real time. This paper [10] proposed intrusion detection techniques by combining multiple hosts in order to detect multiple intrusions and to reduce false-positive rate. Hidden Markov Model (HMM) is a speech recognition technique that is used for modelling the system call events. Statistical technique gives the percentage of resource usages and system call events. Decision tree is used to model or classify the type intrusion to examine the future challenges. This technique [10] has advantage of less false-positive rate that increases performance of detection.

## 

## 

## CHAPTER 4

**PROBLEM DEFINITION AND SCOPE**

### PROBLEM STATEMENT

We propose to build and demonstrate a novel system for rapid development and deployment of effective and cost-sensitive IDSs. We consider intrusion detection as a classification problem, that is, we wish to classify each audit record or log records into one of a discrete set of possible categories, normal or a particular kind of intrusion. However, before we can apply classification algorithms, we need to first select and construct the right set of system features that may contain evidence (indicators) of normal or intrusions. We will develop an automatic feature selection and construction system to systematically discover and construct predictive features that can be used to build effective misuse and anomaly detection models.

### Goals and objectives

The purpose of intrusion detections systems (IDSs) is to monitor networks or systems with the express purpose of identifying and responding to suspicious activity.

### Statement of scope

* As we know IDS system are intrusion detection system and it can only detect the attack at real time so, as compare to 3rd party IDS software like SNORT & TIGER some new features are added to our IDS like :-
* **Trojans Scanner:** It check the active connection and find the possible Trojans plus report the administrator about it.
* **Shell Finder:** The program find the shell and back-connect backdoors in apache server and report it to the administrator.
* **PSAD:** Well known as "Port Scan Attack Detector". The concept of the PSAD is from well-known book called "The Art Of War" By Sun Tzuwhere he states "**If you know** **the enemy and know yourself, you need not fear the result of a hundred battles".** Similar port scanning is the first step of the hacking to know your enemy so, PSAD detect and alert the administrator.
* **Fake Access Point:** The fake access point is a honeypot which attract attacker and administrator can easily know about attacker and its capabilities.
* **ADS Blocker:** The program block ads and spam for user.
* The IDS CAN provide the following:
* CAN add a greater degree of integrity to the rest of you infrastructure
* CAN trace user activity from point of entry to point of impact
* CAN recognize and report alterations to data
* CAN automate a task of monitoring the Internet searching for the latest attacks
* CAN detect when your system is under attack
* CAN detect errors in your system configuration
* CAN guide system administrator in the vital step of establishing a policy for your computing assets
* CAN make the security management of your system possible by non-expert staff
* The IDS CAN NOT provide:
* CAN NOT compensate for a weak identification and authentication mechanisms
* CAN NOT conduct investigations of attacks without human intervention
* CAN NOT compensate for weaknesses in network protocols
* CAN NOT compensate for problems in the quality or integrity of information the system provides.
* CAN NOT analyze all the traffic on a busy network
* CAN NOT always deal with problems involving packet-level attacks
* CAN NOT deal with some of the modern network hardware and features.

### SOFTWARE CONTEXT

There are various factors and benchmarks which are to be kept in mind whilst we design and develop a IDS . This phase of the IDS project development process decides the actual outcome of the IDS . The environment and the IDS objects in the system must support the storyline and should be rendered in such way that they are a treat to the eyes of the hackers. At the same time we’’ll have to make sure that the IDS is light weight so as to run at an optimal pace with minimum system requirements. Hence it is important to know the problems in hand and also to grade them in the best possible so that it would help us in deciding up on the factors that is to be given a higher priority while designing and developing the IDS.

### MAJOR CONSTRAINTS

* [Noise](https://en.wikipedia.org/wiki/Noise_(signal_processing)) can severely limit an intrusion detection system's effectiveness. Bad packets generated from software bugs, corrupt [DNS](https://en.wikipedia.org/wiki/DNS) data, and local packets that escaped can create a significantly high false-alarm rate.
* It is not uncommon for the number of real attacks to be far below the number of false-alarms. Number of real attacks is often so far below the number of false-alarms that the real attacks are often missed and ignored.
* Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to newer strategies.
* For signature-based IDSes there will be lag between a new threat discovery and its signature being applied to the IDS. During this lag time the IDS will be unable to identify the threat.
* It cannot compensate for a weak identification and [authentication](https://en.wikipedia.org/wiki/Authentication) mechanisms or for weaknesses in [network protocols](https://en.wikipedia.org/wiki/Network_protocol). When an attacker gains access due to weak authentication mechanism then IDS cannot prevent the adversary from any malpractice.
* Encrypted packets are not processed by most intrusion detection devices. Therefore, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred.
* Intrusion detection software provides information based on the [network address](https://en.wikipedia.org/wiki/Network_address) that is associated with the IP packet that is sent into the network. This is beneficial if the network address contained in the IP packet is accurate. However, the address that is contained in the IP packet could be faked or scrambled.

### METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY IS- SUES

* **Feasibility Analysis**

It is an analysis of our idea related to the system and give a validity and make our idea important. It takes an effort and necessity of thinking ability about the system feasibility of a problem occurred. Feasibility is the study of a significant or strong influence, what occurs at the time of system development. The influence can be either positive or negative. The system is considered feasible when positivity entitles negativity. Feasibility study can be performed in various ways related to various fields, we are describing four important way of performing feasibility study which are described following:-

* **Technical Feasibility**: Technical feasibility of a system defines the compatibility, comfort, ability to achieve using current existing technology. It takes into attention weather the required technology is available or not and it also check for available resources like equipment’s and software tools for development of the system. We can say that our developed system is technically feasible because we are not getting any difficulty related to resource of development and maintenance of this project. Whatever software tools related to the development of system are commonly available and easy to get from internet and any other way like shop, friends etc.
* **Economical Feasibility**: This system is highly economic feasible because it is not taking any extra tools other than our required tools for development which are easily available and free to download and use for development of projects. We need not to spend more money for the development of the system. It is making an environment for the development with an effective manner. If we do as it than we can see the maximum usability of the related resources of system. After development of this system, we need not to be attentive for this system. Therefore we can say that, this system is economically feasible.
* **Schedule Feasibility:** It is defined as the state of being probable and completed within scheduled time. Our Project can be fail when it takes too long to be completed before it is used. It means estimating the project with respect of time that how long this system will take to develop. Schedule feasibility is a measurement of is timetable for project is reasonable. We discuss with our team and decide is the project deadline reasonable? Our project is initiated with specific deadline. We have determined whether the deadlines are mandatory or desirable.
* **Operational Feasibility**: It is related to the measurement of performance of system for which purpose it is developed. It relates to all the functions and features related to the system and look for speed of execution of requests came from users and effectiveness of response in well manner. It provides an advantage of the opportunities introduced at time of scope definition and its satisfaction of requirement identified. It also provide satisfaction for phase of system development. It ensures desired operational outputs which is the part of design and development. It includes design parameters like reliability, maintainability, supportability, usability of system for users. There all parameters are required for consideration of stages of design. A design and development of system requires appropriate and timely application software for development and provide efforts to meet the mentioned parameters which are defined previously. A system performs its planned purpose most effectively when its technical and operational characteristics are identifies into the design. So, we can say that operational feasibility is a critical aspect of systems engineering that needs to be an integral part of the early design phases.

### OUTCOME

* Monitors a network or systems for malicious activity or policy violations and after detection of these activities pop up alert messages to administrator for required actions.

### APPLICATIONS

* Monitor a mail server and other services
* monitors a network or systems for malicious activity or policy violations
* Digital Forensics
* Terminus Shock Detection Systems

### SOFTWARE RESOURCES REQUIRED

|  |  |  |
| --- | --- | --- |
| **SO.NO.** | **TOOL** | **USE** |
| **1.** | **Perl** | **Programming Language** |
| **2.** | **Wireshark** | **Packet Sniffing Tool** |
| **3.** | **Tshark** | **Command Line Packet Sniffing Tool** |
| **4.** | **TCP DUMP** | **TCP Traffic Intercepting Tool** |
| **5.** | **Apache Server** | **HTTPD Server to host Websites** |
| **6.** | **Airmon-ng** | **To Put wireless network card at monitor mode.** |
| **7.** | **Airodump-ng** | **To Dump All Wireless connection detail** |
| **8.** | **Airplay-ng** | **To do ARP Poisoning Attack on Base Stations** |
| **9.** | **Airbase-ng** | **To Create a New Base Station** |
| **10.** | **DHCP Server** | **To configure Networking such as IP-Address**  **Ranges** |
| **11.** | **BrupSute** | **To Intercept Session Of Users** |
| **12.** | **Driftnet** | **To Sniff Images form captured packets** |
| **13.** | **Hamster & Ferret** | **To Sniff Documents from captured packets** |

## 

## CHAPTER 5 PROJECT PLAN

### PROJECT ESTIMATES

5.1.1 Reconciled Estimates

5.1.1.1 Cost Estimates

All the software used are open source software’s.

Cost of router

5.1.1.2 Time Estimates

Estimated time of research is 8 months.

5.1.2 Project Resources

* System Requirements
* Linux OS
* Backtrack OS
* Kali OS
* Linux Distribution
* Fedora
* Ubuntu
* Redhat
* Software Installation Required
* Perl Programming
* Wireshark
* Apache Server
* Tcp-dump
* Tshark
* System Architecture
* System Hardware Architecture
* Linux compatible PC with OS architecture x86 or x64
* CPU
* Core 2 Duo
* RAM: 4 GB
* HDD : 320 GB
* Virtual Memory : 12,215 MB
* NIC
* System Software Architecture :
* Install Perl In UNIX Systems By Default Perl Package is installed test using " perl -v " Command.
* Install PerlX-Assert-0.900\_01
* Install TCP Dump Program
* Install Wireshark Program
* Install Tshark Program
* Install Apache Server
* Install airmon-ng Program
* Install airodump-ng Program
* Install airplay-ng Program
* Install airbase-ng Program
* Configure DHCP Server
* Install BrupSute Program
* Install Driftnet Program
* Install hamster & Ferret Program

### RISK MANAGEMENT W.R.T. NP HARD ANALYSIS

This section discusses Project risks and the approach to managing them.NP-hardness (non-deterministic polynomial-time hardness), in computational complexity theory, is the defining property of a class of problems that are, informally, "at least as hard as the hardest problems in NP".

**5.2.1 Risk Identification**

For risks identification, review of scope document, requirement specifications and schedule is done. Answers to questionnaire revealed some risks. Each risk is categorised as per the categories mentioned below. You can refer to following risk identification questionnaire:

1. Have top software and customer managers formally committed to support the project.

2. Are end-users enthusiastically committed to the project and the system/product to be built?

3. Are requirements fully understood by the software engineering team and its customers?

4. Have customers been involved fully in the definition of requirement?

5. Do end-users have realistic expectations?

6. Does the software engineering team has the right mix of skills?

7. Are project requirements stable?

8. Is the number of people on the project team adequate to do the job?

**5.2.2 Risk Analysis**

The risks for the Project can be analysed within the constraints of time and quality

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Probability | Impact | | |
| Schedule | Quality | Overall |
| 1 | Estimated Project Schedule | High | High | High | High |
| 2 | Project Scope Creep | Low | Low | Medium | Medium |
| 3 | Project Team Availability | Medium | Medium | High | High |
| 4 | Person Hours | High | High | High | High |
| 5 | Timeline Estimates Unrealistic | Medium | Medium | Medium | Medium |
| 6 | Poor Functional Match of Package to Initial System Requirements | Low | Low | Low | Low |

Table 5.2.1: Risk Table

|  |  |  |
| --- | --- | --- |
| Probability | Value | Description |
| High | Probability of occurrence is | >75% |
| Medium | Probability of occurrence is | 26-75% |
| Low | Probability of occurrence is | <25% |

Table 5.2.2: Risk Probability definitions

|  |  |  |
| --- | --- | --- |
| Impact | Value | Description |
| Very high | >10% | Schedule impact or Unacceptable quality |
| High | 5-10% | Schedule impact or Some parts of the project have low quality |
| Medium | <5% | Schedule impact or barely noticeable degradation in quality Low impact on schedule or Quality can be incorporated |

Table 5.2.3: Risk Impact definition

**5.2.3 Overview of Risk Mitigation, Monitoring, Management**

Following are the details for each risk.

|  |  |
| --- | --- |
| Risk ID | 1 |
| Risk Description | Estimated Project Schedule |
| Category | Development Environment |
| Source | Software requirement Specification document |
| Probability | High |
| Impact | High |
| Response | Mitigate |
| Strategy | Created comprehensive project timeline with frequent baseline reviews |
| Risk Status | Anticipated |

|  |  |
| --- | --- |
| Risk ID | 2 |
| Risk Description | Project Scope Creep |
| Category | Requirements |
| Source | Software Design Specification documentation review |
| Probability | Low |
| Impact | Medium |
| Response | Mitigate |
| Strategy | Scope initially defined in project plan,reviewed monthly by project guide |
| Risk Status | Identified |

|  |  |
| --- | --- |
| Risk ID | 3 |
| Risk Description | Project Team Availability |
| Category | Technology |
| Source | This was identified during early development and testing |
| Probability | Medium |
| Impact | Very High |
| Response | Accept |
| Strategy | Continuous review of project momentum by all levels.If necessary, increase committment by participation to full time status |
| Risk Status | Identified |

|  |  |
| --- | --- |
| Risk ID | 4 |
| Risk Description | Person Hours |
| Category | Requirements |
| Source | Software Design Specification documentation review |
| Probability | High |
| Impact | High |
| Response | Mitigate |
| Strategy | Comprehensive project management approach and communications plan |
| Risk Status | Identified |

|  |  |
| --- | --- |
| Risk ID | 5 |
| Risk Description | Timeline Estimates Unrealistic |
| Category | Requirements |
| Source | Software Design Specification documentation review |
| Probability | Medium |
| Impact | Medium |
| Response | Mitigate |
| Strategy | Timeline reviewed monthly by the members of the group and Project guide to prevent undetected timeline departures |
| Risk Status | Identified |

|  |  |
| --- | --- |
| Risk ID | 6 |
| Risk Description | Poor Functional Match of Package to Initial System Requirements |
| Category | Requirements |
| Source | Software Design Specification documentation review |
| Probability | Low |
| Impact | Low |
| Response | Mitigate |
| Strategy | Use of Intranet project website, comprehensive Communication plan |
| Risk Status | Identified |

**5.3 PROJECT SCHEDULE**

**5.3.1 Project task set**

Major Tasks in the Project stages are:

* Project Title Selection
* Discussion & Proposal
* Proposal submission
* Literature Survey
* Proposal Presentation
* Proposal Design
* Software Development
* Test Plan
* Testing and QA

5.3.2 Task network

Project Task

Selection

Discussion &

Proposal

Proposal

Submission

Literature

Survey

Proposal

Presentation

Proposal

Design

Test Plan &

Testing QA

Software

Development

Figure 5.1: Task Network

**5.4 TEAM ORGANISATION**

The team had three members under guidance of associated professors as follows:

* Project Guide: Prof. Sushma S Shirke
* Team Lead: Surjit Singh
* Lead Architecture: Shatruanjay Kumar
* Lead Test Engineer: Yogesh Faguna
* Lead Designer: Sachin Yadav and Vikas

5.4.1 Team structure

The team structure for the project is identified. Roles are defined.

Project Manager

Lead Architect

Team Lead

Lead Test Engineer

Testing/QA

Figure 5.4.1.1 Team Structure

## CHAPTER 6

**SOFTWARE REQUIREMENT SPECIFICATION**

**(SRS)**

**6.1 Introduction**

**6.1.1 Purpose and Scope of Document**

Nowadays the use of cloud usage has increased so much, that there is need for optimum usage of the rented resources. User feels a need to know the amount of resources used in the present as well as the predicted usage in the future.

**6.1.2 Overview of responsibilities of Developer**

Responsibilities of a developer include tracking of the current usage of the user and predicting the usage of resources in the future to the user in a graphical manner i.e. through graph ,pie charts etc.

**6.2 Usage Scenario**

Users’ needs an optimum limit of the usage of resources .For example: For an allocated limit of ram of 4 GB ,if user’s limit is at max 3 GB then extra cost of 1 GB can be reduced and proﬁted by user.

**6.2.1 User proﬁles**

A user proﬁle deﬁnes how client applications interact with one or more server components by a network connection. A server user proﬁle deﬁnes how resources on the server are aﬀected by parameters you specify.

**6.2.2 Use-cases**

All use-cases for the software are presented. Description of all main Use cases using use case template is to be provided.

**6.2.3 Use Case View**

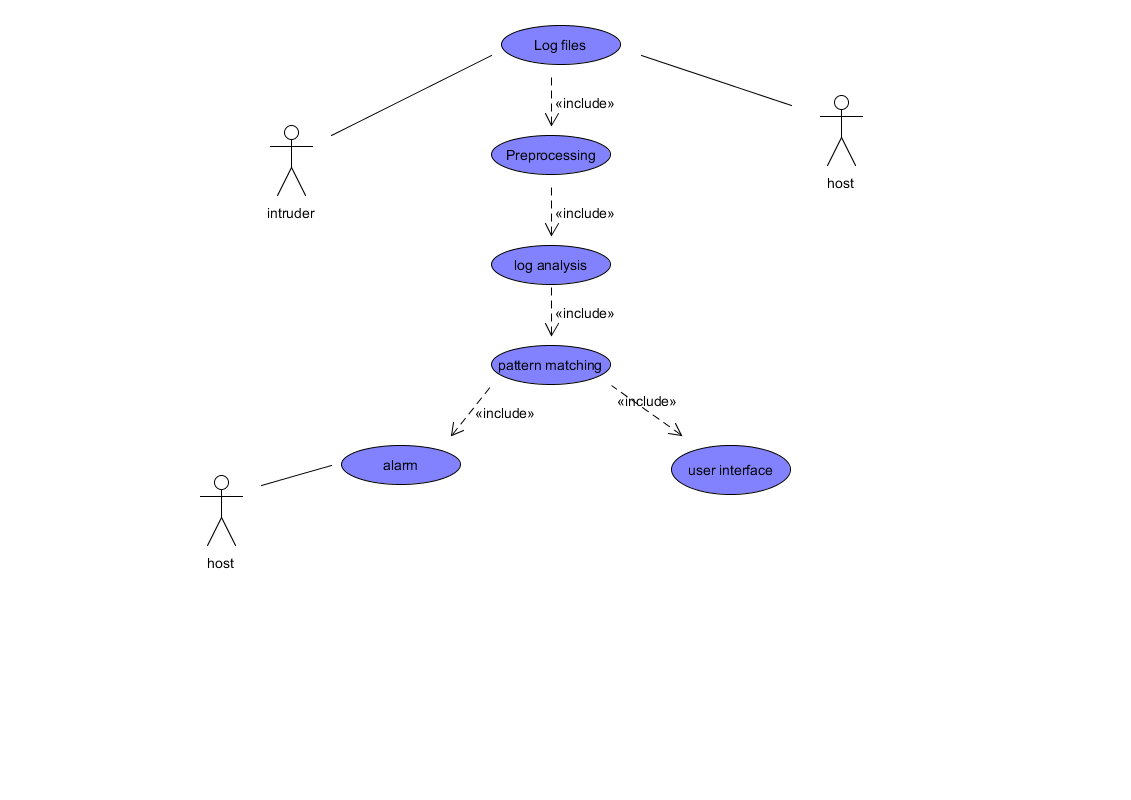


Fig 6.1 Use case diagram

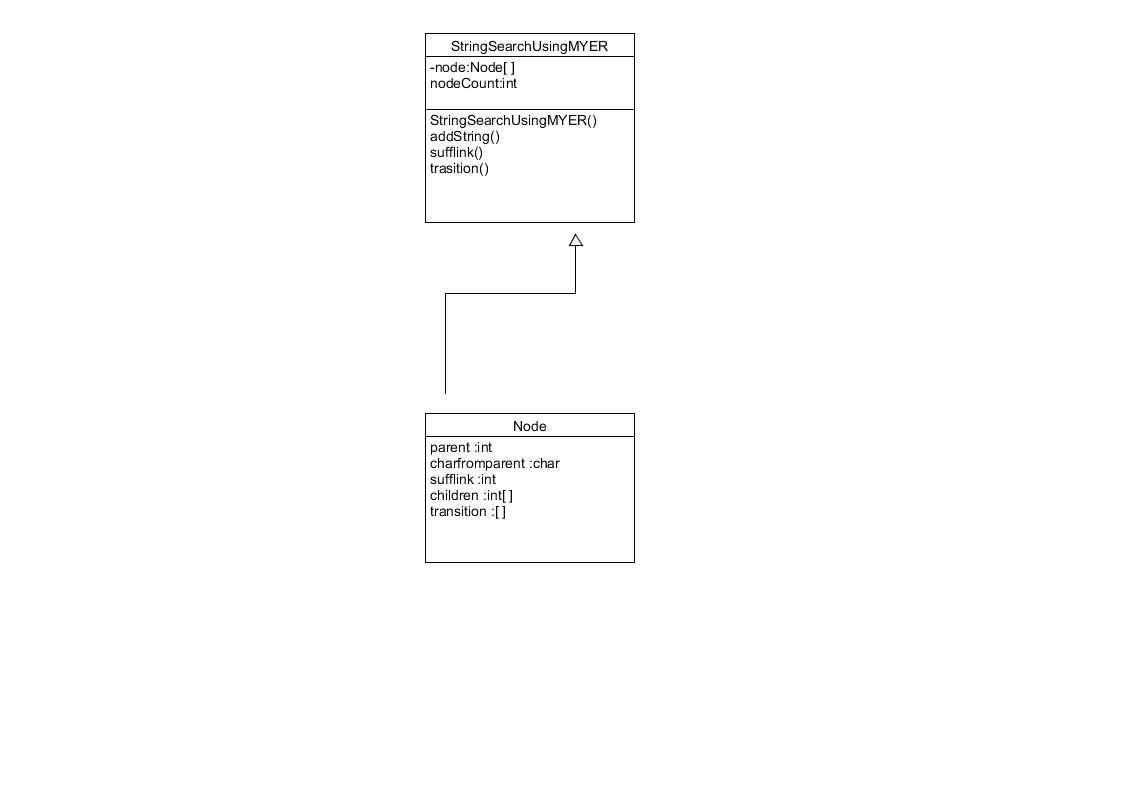


Figure 6.2 Class Diagram

**6.3 Functional Model and Description**

### 

### 6.3.1 Data Flow Diagram

**Flow Chart Firewall:**

**START**

**Main Menu**

Honeypot, Ddos protection, logs,

logout (1,2,3,4,5) respectively.

**Option : 1**

**Firewall**

1.

Block Ip

2.

Block Mac

3.

Packet Filtering

4.

Website block

5.

Go

Back

**GO TO**

**YES**

**NO**

**Run Successfully**

**End**

**Flow Chart**

**Honeypot:**

**START**

**Main Menu**

Honeypot, Ddos protection ,logs,

logout(1,2,3,4,5) respectively.

**Option : 2**

**Honeypot**

. Run Honeypot

1

. Port scan detect.

2

. Fake access point

3

honeypot

.

4

Go Back

**GO TO**

**YES**

**NO**

**Run Successfully**

**End**

**Flow Chart Dos/Ddos:**

**START**

**Main Menu**

Honeypot, Ddos protection, logs,

logout (1,2,3,4,5) respectively.

**Option : 3**

**Dos/Ddos**

1

. Anti ARP

2

. Anti Http flood

. Anti UDP flood

3

4

. Tcp/Ip flood

5

. Go back

**GO TO**

**YES**

**NO**

**Run Successfully**

**End**

6.3.2 Activity Diagram

Activity states represent the performance of a step within the workﬂow. Transitions allow transitions from one activity state to another. This is referred as completion transition. It diﬀers from a transition in that it does not require an explicit trigger event; it is triggered by the completion of the activity that the activity state represents. Decisions for which a set of guard conditions are deﬁned. These guard conditions control which transition of a set of alternative transitions follows once the activity has been completed. You may also use the decision icon to show where the threads merge again. Decisions and guard conditions allow you to show alternative threads in the workﬂow of a business use. There are actually 2 activity diagrams i.e. for admin and user.

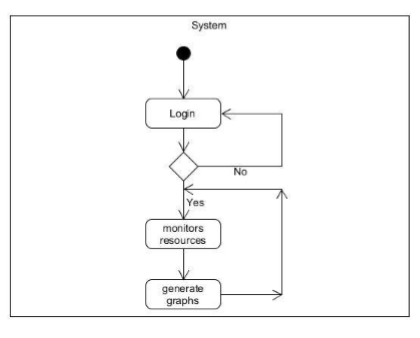


Fig No 6.4 Admin Activity Diagram

## CHAPTER 7

## REFERENCES

* + - 1. Ahmed Patel, Qais Qassim, Christopher Wills. *A survey of intrusion detection and prevention systems*, Information Management & Computer Security Journal (2010).
      2. Oludele Awodele, Sunday Idowu, Omotola Anjorin, and Vincent J. Joshua, *A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)*, Babcock University, (Volume 6, 2009).
      3. *Host Intrusion Prevention Systems and Beyond*, SANS Institute (2008).
      4. *Intrusion Detection and Prevention In-sourced or Out-sourced*, SANS Institute (2008).
      5. Mario Guimaraes, Meg Murray. *Overview of Intrusion Detection and Intrusion Prevention*, Information security curriculum development Conference by ACM (2008).
      6. Muhammad Awais Shibli, Sead Muftic. *Intrusion Detection and Prevention System using Secure Mobile Agents*,IEEE International Conference on Security & Cryptography (2008).
      7. David Wagner, Paolo Soto. *Mimicry Attacks on Host Based Intrusion Detection Systems*, 9th ACM Conference on Computer and Communications Security (2002).
      8. Harley Kozushko. *Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems*, (2003).
      9. Lin Tan, Timothy Sherwood. *A High Throughput String Matching Architecture for Intrusion Detection and Prevention*, Proceedings of the 32nd Annual International Symposium on Computer Architecture (ISCA 2005).
      10. S. Mrdovic, E. Zajko. *Secured Intrusion Detection System Infrastructure*, University of Sarajevo/Faculty of Electrical Engineering, Sarajevo, Bosnia and Herzegovina (ICAT 2005).
      11. Yeubin Bai, Hidetsune Kobayashi. *Intrusion Detection Systems: technology and Development*, 17th International Conference of Advanced Information Networking and Applications, (AINA 2003).