

IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

by

V.R.Madhiyazhakan (38110283)

S.Thiyagesh kanna (38110601)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

**SATHYABAMA INSTITUTE OF SCIENCE AND
TECHNOLOGY**

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600

119

MARCH - 2022



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **V.R.Madhiyazhakan (38110283), S.Thiyagesh kanna (38110601)**

who carried out the project entitled **"IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING"** under my supervision from November 2021 to March 2022

Internal Guide

Dr. A. Sivasangari ME. PhD

Head of the Department

Dr. L. Lakshmanan, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

We **V.R.Madhiyazhakan** and **S.Thiyagesh kanna** hereby declare that the Project Report entitled **IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING** done by us under the guidance of Dr./Prof./Mr./Ms. **Dr. A. Sivasangari ME. Ph.D.** (Internal) is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

V.R.Madhiyazhakan
S.Thiyagesh kanna

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D, Dean**, School of Computing **Dr. L. Lakshmanan M.E., Ph.D. ,** and **Dr.S.Vigneshwari M.E., Ph.D. Heads** of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide Dr./Mr./Ms for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT:

This aids in refining any organization's security policy due to identification of vulnerabilities, and guarantees that the security measures taken actually gives the protection that the organization expects and requires. Administrator needs to perform vulnerability which helps them to uncover shortcomings of network security that can lead to device or information being compromised or destroyed by exploits. These outputs are typically heterogeneous which makes the further analysis a challenging task. Normal user network may give the way to unauthorized people to access as a authorized agents. Whenever, users step into online networks, without knowing them third party or any other harmful person monitoring their behavior. Provide the protection from malicious activity, admin or authorized person also check the user networks such as IP address and email.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	5
	LIST OF ABBREVIATIONS	10
1.	CHAPTER 1 : INTRODUCTION 1.1 INTRODUCTION 1.2 EXISTING SYSTEM 1.2.1 DEMERITS 1.3 LITERATUTRE SURVEY 1.4.PROPOSED SYSTEM 1.4.1 ADVANTAGE	11
2.	CHAPTER 2 :PROJECT DESCRIPTION 2.1 METHODOLOGY 2.2 MODULES 2.3 MODULE EXPLANATION 2.4 MODULE DIAGRAM	19

3.	CHAPTER 3 : REQUIREMENTS ENGINEERING 3.1 GENERAL 3.2 HARDWARE REQUIREMENTS 3.3 SOFTWARE REQUIREMENTS	23
4.	CHAPTER 4 : SYSTEM DESIGN ENGINEERING 4.1 GENERAL 4.1.1 USE CASE DIAGRAM 4.1.2 ACTIVITY DIAGRAM 4.1.3 DATA FLOW DIAGRAM 4.1.4 ER- ARCHITECTURE 4.1.5 SYSTEM DIAGRAM	25

5.	CHAPTER 5 :DEVELOPMENT TOOLS 5.1 GENERAL FRONT END 5.2 FEATURES OF JAVA 5.2.1 THE JAVA FRAMEWORK 5.2.2 OBJECTIVE OF JAVA 5.2.3 JAVA SERVER PAGES-AN OVERVIEW 5.2.4 EVOLUTION OF WEB APPLICATIONS 5.2.5 BENEFITSO F JSP 5.3 SERVLETS 5.4 JAVA SERVLETS 5.5 CONCLUSION	32
7.	CHAPTER 6 : SNAPSHOTS 7.1 GENERAL 7.2 VARIOUS SNAPSHOTS	41

8	CHAPTER 7: APPLICATIONS AND FUTURE ENHANCEMENT 8.1 FUTURE ENHANCEMENT CONCLUSION REFERENCE	47
---	---	----

LIST OF ABBREVIATION

S.NO	ABBREVIATION	EXPANSION
1.	DB	DataBase
2.	SMC	Secure MultipartyComputation
3.	MDA	Medical Admin
4.	DBC	Data Base Confidentiality
10	JVM	Java Virtual Machine
11.	JSP	Java Server Page

CHAPTER 1

1.1 INTRODUCTION:

In this paper, we explore how a network can manipulate this information source-the peering link where traffic ingresses a network-to more precisely locate sources of spoofed traffic. Our key observation is that the routes are partially under an origin network's control, and so the network receiving the spoofed traffic has some ability to impact on which link it receives traffic, instead of relying on routers that are not under its control. We propose techniques that are fundamentally Different from existing trace back approaches and can be used today, requiring no changes to deployed equipment nor cooperation from other networks. Our techniques work best when the spoofed traffic originates from few sources, as is common in amplification DoS attacks.

1.2 EXISTING SYSTEM:

CONCEPT:

Network can use to systematically vary BGP announcement configurations to induce changes to Internet routes and to the set of sources routed to each peering link.

1.2.1 Disadvantage:

This scheme cannot be used to detect loops

1.3 LITERATURE SURVEY:

TITLE: LIFEGUARD: Practical Repair of Persistent Route Failures.

AUTHOR: Ethan Katz-Bassett, Colin Scott, David R. Choffnes

YEAR: 2012

PAPER EXPLANATION:

The Internet was designed to always find a route if there is a policy compliant path. However, in many cases, connectivity is disrupted despite the existence of an underlying valid path. The research community has focused on short-term outages that occur during route convergence. There has been less progress on addressing

Avoidable long-lasting outages. Our measurements show that long lasting events contribute significantly to overall unavailability. To address these problems, we develop LIFEGUARD, a system for automatic failure localization and remediation. LIFEGUARD uses active measurements and a historical path atlas to locate faults, even in the presence of asymmetric paths and failures. Given the ability to locate faults, we argue that the Internet protocols should allow edge ISPs to steer traffic to them around failures, without requiring the involvement of the network causing the failure. Although the Internet does not explicitly support this functionality today, we show how to approximate it using carefully crafted BGP messages. LIFEGUARD employs a set of techniques to reroute around failures with low

impact on working routes. Deploying LIFEGUARD on the Internet, we find that it can effectively route traffic around an AS without causing widespread disruption.

TITLE: A survey of distributed denial-of-service attack, prevention, and mitigation techniques

AUTHOR: Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang.

YEAR: 2017

PAPER EXPLANATION:

Distributed denial-of-service is one kind of the most highlighted and most important attacks of today's cyber world. With simple but extremely powerful attack mechanisms, it introduces an immense threat to current Internet community. In this article, we present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a systematic analysis of this type of attacks including motivations and evolution, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges of existing research. Finally, some important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks.

TITLE: Towards Measuring Global DDoS Attack Capacity

AUTHOR: T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky

YEAR: 2019

PAPER EXPLANATION:

In today's Internet, distributed denial-of-service (DDoS) attacks play an ever-increasing role and constitute a risk to any commercial, military or governmental

entity that has a presence on the Internet or simply has an Internet connection. To address this threat on all levels, decision-makers have to rely on trustworthy information regarding attack capacity, sources, and the largest contributors. The lack

of this information limits the ability of technicians, policymakers, and other relevant

decision-makers to remediate the issue as efficiently as possible. This research introduces a methodology for measuring the properties of individual devices participating in such attacks. These properties include rate limiting, amplification factor, and speed, which allows the calculation of each device's actual contribution to the attack capacity. This methodology was implemented as a proof of concept for the NTP protocol and the results indicate that it has promising potential.

Individual measurements aggregated together provide insights into particular abused protocols: all the protocols together could provide the global DDoS attack capacity.

TITLE: Single-Packet IP Traceback with Less Logging

AUTHOR: Wen-Chung Kuo; Yi-Lin Chen; Shuen-Chih Tsai; Jung-Shian Li

YEAR: 2011

PAPER EXPLANATION:

Currently, the main threats of network security are coming from hacker intrusion, deny of service (DoS), computer virus, worm, spam, malicious code and sniffer because there are many weaknesses in the original design of IPv4. One is that attackers could send IP spoofing packets which is he wants to attack. That is the attackers modify the IP from the true one to another on the IP field. However, it is hard to trace the source of attacks from victims. In this paper, we will propose a method that reduces the storage of the router and trace the attack source by a single packet. According to the experimental results, we can prove that it works well.

TITLE: Tracking Down Sources of Spoofed IP Packets

AUTHOR: Osvaldo Fonseca, Ítalo Cunha, Elverton Fazzion, Wagner Meira, Brivaldo Junior, Ronaldo A. Ferreira, Ethan Katz-Bassett

YEAR: 2020

PAPER EXPLANATION:

The lack of authentication in the Internet's data plane allows hosts to falsify (spoof) the source IP address in packet headers, which forms the basis for amplification denial-of-service (DoS) attacks. Current approaches to locate sources of spoofed traffic lack coverage or are not deployable today. We propose a mechanism that a network with multiple peering links can use to coarsely locate the sources of spoofed traffic in the Internet. More precisely, the network can monitor and map spoofed traffic arriving on a peering link to the set of sources routed toward that link. We propose mechanisms the network can use to systematically vary BGP announcement configurations to induce changes to Internet routes and to the set of sources routed to each peering link. A network using our technique can correlate observations over multiple configurations to more precisely delineate regions sending spoofed traffic. Evaluation of our techniques on the Internet shows that they can partition the Internet into small regions, allowing targeted intervention.

1.3 PROPOSED SYSTEM:

Concept:

Whenever step to the application, their IP address to be obtained by the authority person with valid request from the concern persons.

Technique:

AES algorithm

1.3.1 Advantage:

Reliable and effective method of safeguarding sensitive information.

CHAPTER 2

2.1 METHODOLOGY:

Methodologies is the process of analyzing the principles or procedure of a Progressive Anonymous Database management system.

2.2 MODULES:

- LOGIN
- ADD FILE
- VIEW
- REQUEST
- RESPONSE
- DOWNLOAD

2.3 MODULE EXPLANATION:

LOGIN:

This module gives the way to enter into main page after login with valid input such as username or email id and password.

ADD FILE:

This module is help us to the manager add the file or document to the database. To view the staffs.

VIEW:

This module to help us the staff view the file. But the staff cannot be open the file until the Head office accept the file. After response the head office the file can view by the staff with the help of secret key.

REQUEST:

This module to help to staff request the file to head office and the head office accept the request. And third party or hacker also request the file.

RESPONSE:

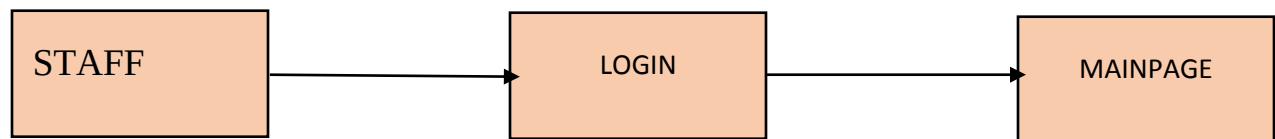
This module to help to staff requested file to head office accept the request. And the hacker or third party also request the file. But the hacker request doesn't Show the ip address of the hacker. Then the head office will identify the requested person is hacker or valid user.

DOWNLOAD:

This module is help to staff download the file after head office approve the request.

2.4 MODULE DIAGRAM:

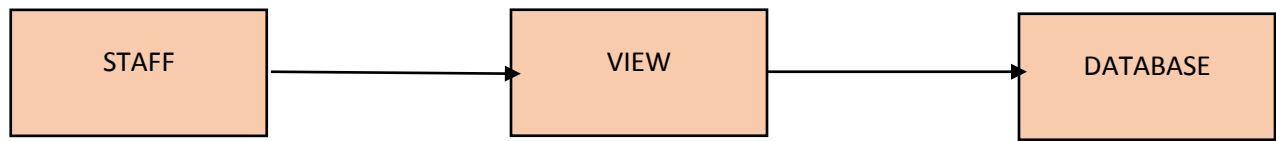
LOGIN:



ADD FILE:



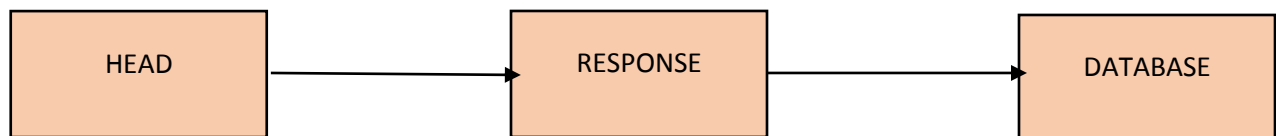
VIEW:



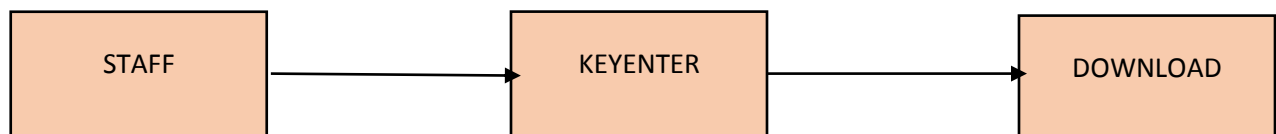
REQUEST:



RESPONSE:



DOWNLOAD:



CHAPTER 3

REQUIREMENTS ENGINEERING

3.1 GENERAL

These are the requirements for doing the project. Without using these tools and software's we can't do the project. So we have two requirements to do the project. They are

1. Hardware Requirements.
2. Software Requirements.

3.2 HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the

starting point for the system design. It shows what the system does and not how it should be implemented.

- PROCESSOR : DUAL CORE 2 DUOS
- RAM : 2 GB DD RAM
- HARD DISK : 250 GB

3.3 SOFTWARE REQUIREMENTS

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

- FRONT END : J2EE (JSP, SERVLET)
- BACK END : MY SQL 5.5
- OPERATING SYSTEM : WINDOWS 7
- IDE : ECLIPSE

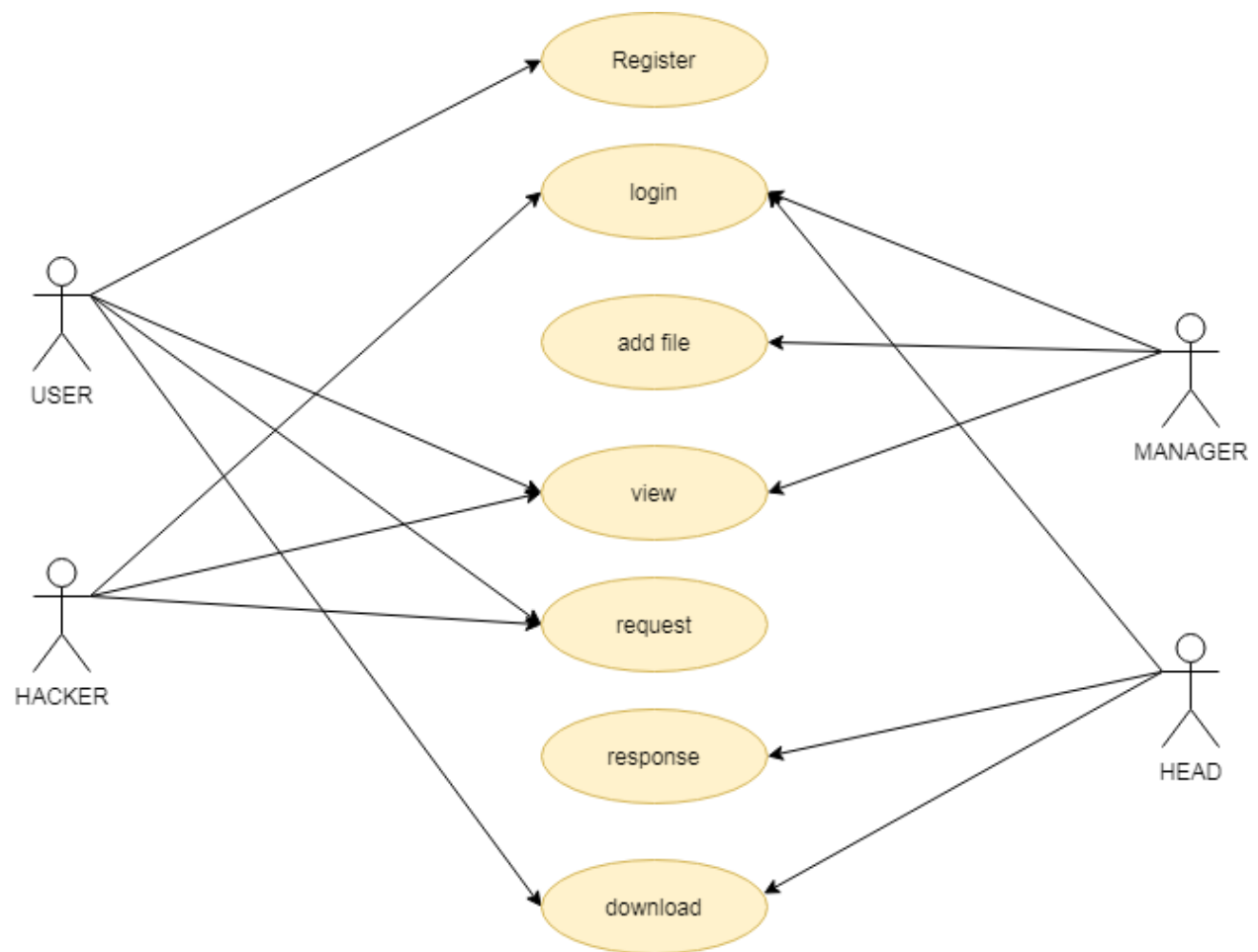
CHAPTER 4

DESIGN ENGINEERING

4.1 GENERAL

Design Engineering deals with the various UML [Unified Modeling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

4.1.1 USE CASE:

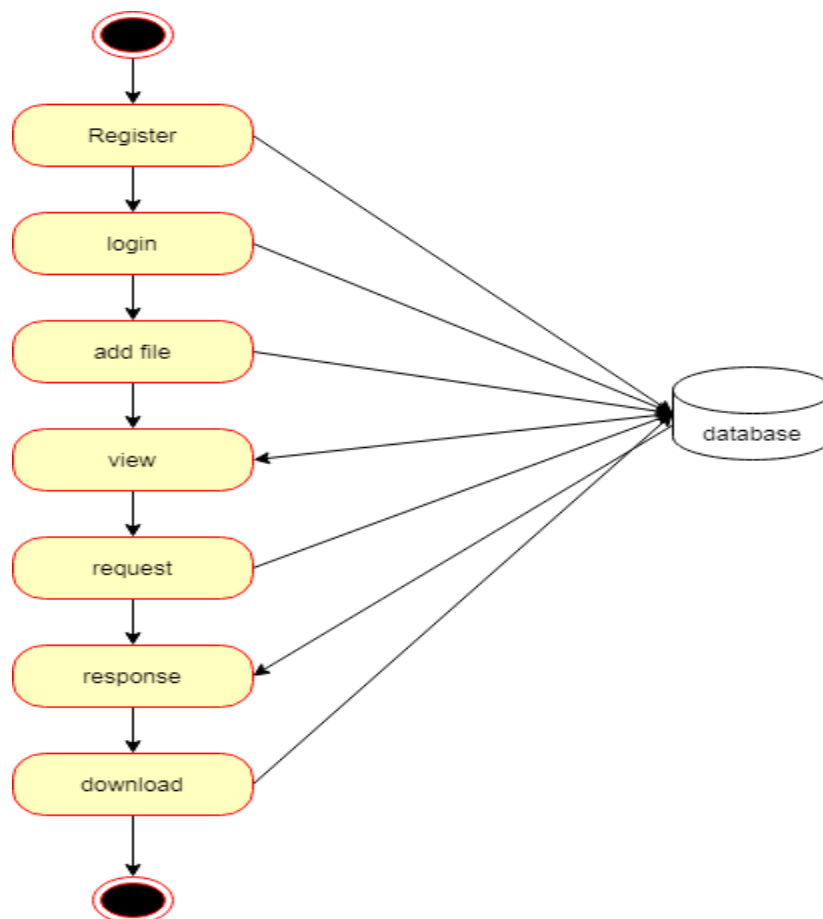


EXPLANATION:

The use case diagram is the main building block of object oriented modeling. It is used both for general conceptual modeling of the

systematic of the application, and for detailed modeling translating the models into programming code. For this in our component diagram first propose a data in this proposed method we are using Hash-Solomon Code Algorithm to encrypt the data.

4.1.3 ACTIVITY DIAGRAM:

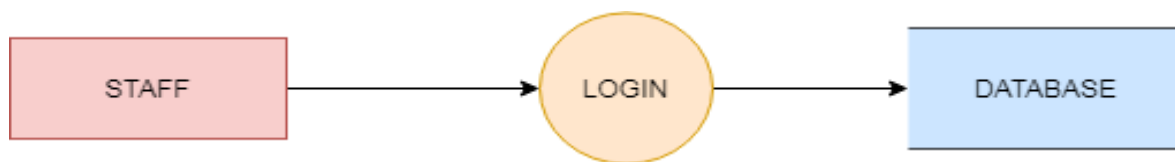


EXPLANATION:

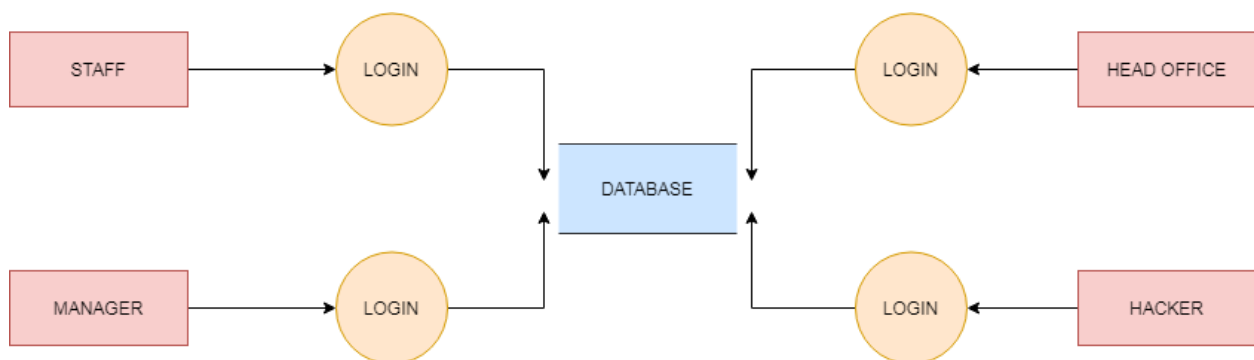
Activity diagram are a loosely defined diagram to show workflows of stepwise activities and actions, with support for choice, iteration and concurrency. UML, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. UML activity diagrams could potentially model the internal logic of a complex operation. In many ways UML activity diagrams are the object-oriented equivalent of flow charts and data flow diagrams (DFDs) from structural development.

4.1.6 DATA FLOW DIAGRAM:

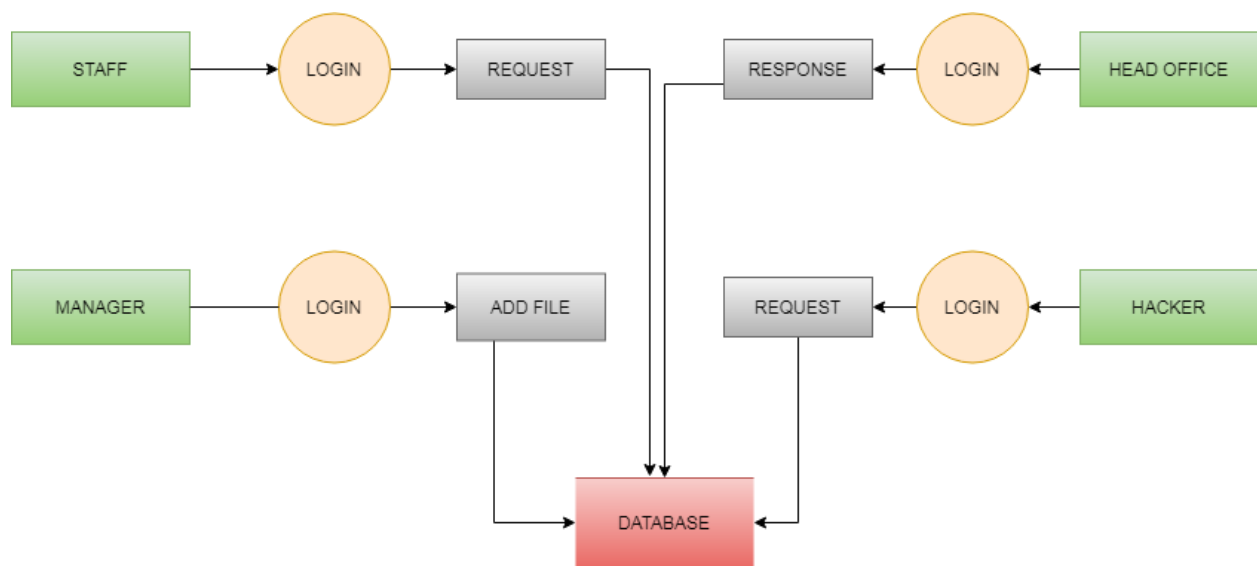
LEVEL 1:



LEVEL 2:



LEVEL 3:

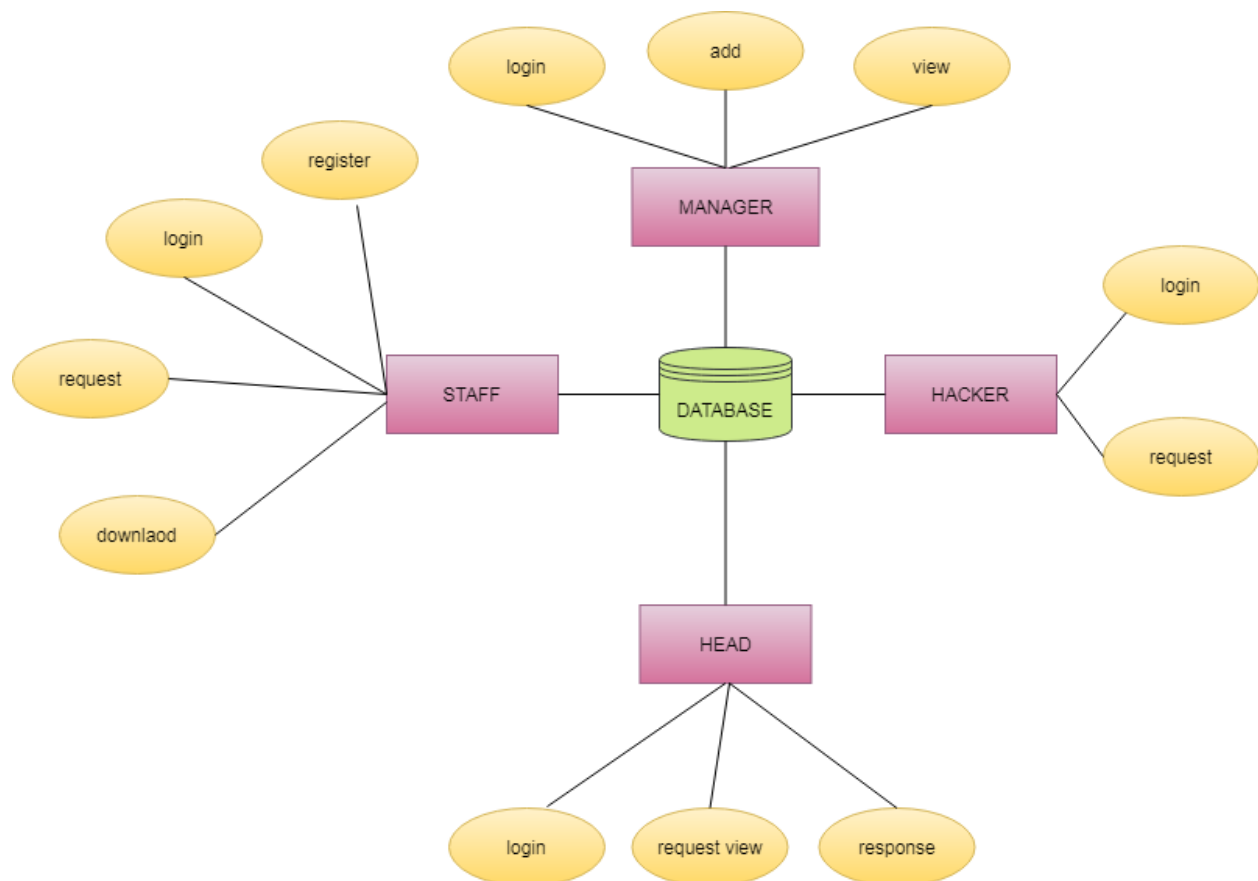


EXPLANATION:

A data flow diagram (DFD) is a graphical representation of the “flow” of data through an information system. It differs from the flowchart as it shows the

data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts.

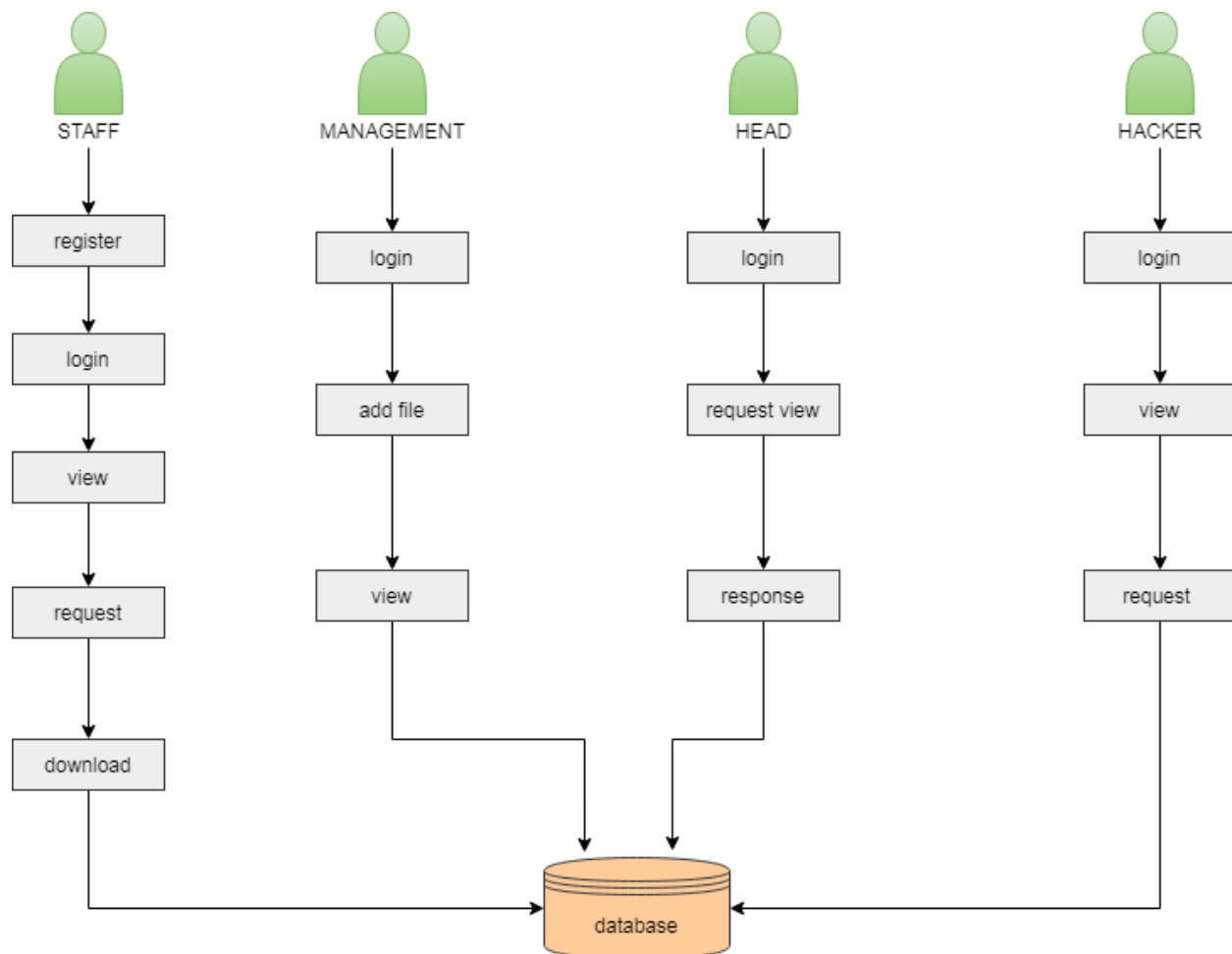
4.1.7 E-R DIAGRAM:



EXPLANATION:

An Entity Relationship (ER) Diagram is a type of flowchart that illustrates how “entities” such as people, objects or concepts relate to each other within a system. ER Diagrams are most often used to design or debug relational databases in the fields of software engineering, business information systems, education and research. Also known as ERDs or ER Models, they use a defined set of symbols such as rectangles, diamonds, ovals and connecting lines to depict the interconnectedness of entities, relationships and their attributes. They mirror grammatical structure, with entities as nouns and relationships as verbs.

4.1.8 SYSTEM ARCHITECTURE:



EXPLANATION:

The systems architect establishes the basic structure of the system, we propose a Hash code Solomon algorithm and we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.

CHAPTER 5

DEVELOPMENT TOOLS

5.1 GENERAL:

This chapter is about the software language and the tools used in the development of the project. The platform used here is JAVA. The Primary languages are JAVA,J2EE and J2ME. In this project J2EE is chosen for implementation.

5.2 FEATURES OF JAVA

5.2.1 THE JAVA FRAMEWORK

Java is a programming language originally developed by James Gosling at Sun Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation

dependencies as possible. It is intended to let application developers "write once, run anywhere".

Java is considered by many as one of the most influential programming languages of the 20th century, and is widely used from application software to web applications. The Java framework is a new platform independent that simplifies application development internet. Java technology's versatility, efficiency, platform portability, and security make it the ideal technology for network computing. From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere!

5.2.2 OBJECTIVES OF JAVA

To see places of Java in Action in our daily life, explore java.com.

WHY SOFTWARE DEVELOPERS CHOOSE JAVA:

Java has been tested, refined, extended, and proven by a dedicated community. And numbering more than 6.5 million developers, it's the largest and most active on the planet. With its versatility, efficiency, and portability, Java has become invaluable to developers by enabling them to:

- Write software on one platform and run it on virtually any other platform
- Create programs to run within a Web browser and Web services
- Develop server-side applications for online forums, stores, polls, HTML forms processing, and more
- Combine applications or services using the Java language to create highly customized applications or services

- Write powerful and efficient applications for mobile phones, remote processors, low-cost consumer products, and practically any other device with a digital heartbeat

Some Ways Software Developers Learn Java:

Today, many colleges and universities offer courses in programming for the Java platform. In addition, developers can also enhance their Java programming skills by reading Sun's java.sun.com Web site, subscribing to Java technology-focused newsletters, using the Java Tutorial and the New to Java Programming Center, and signing up for Web, virtual, or instructor-led courses.

Object Oriented:

To be an Object Oriented language, any language must follow at least the four characteristics.

1. Inheritance: It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding additional features as needed.
2. Encapsulation: It is the mechanism of combining the information and providing the abstraction.
3. Polymorphism: As the name suggests one name multiple form, Polymorphism is the way of providing the different functionality by the functions having the same name based on the signatures of the methods.
4. Dynamic binding: Sometimes we don't have the knowledge of objects about their specific types while writing our code. It is the way of providing the maximum functionality to a program about the specific type at runtime.

5.2.3 Java Server Pages - An Overview

Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. JSP provide excellent server side scripting support for creating database driven web applications. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy.

JSP pages are efficient, it loads into the web servers memory on receiving the request very first time and the subsequent calls are served within a very short period of time.

In today's environment most web sites servers dynamic pages based on user request. Database is very convenient way to store the data of users and other things. JDBC provide excellent database connectivity in heterogeneous database environment. Using JSP and JDBC its very cc easy to develop database driven web application.

Java is known for its characteristic of "write once, run anywhere." JSP pages are plat Java Server Pages

Java Server Pages (JSP) technology is the Java platform technology for delivering dynamic content to web clients in a portable, secure and well-defined way. The Java Server Pages specification extends the Java Servlet API to provide web application developers with a robust framework for creating dynamic web content on the server using HTML, and XML templates, and Java code, which is secure, fast, and independent of server platforms.

JSP has been built on top of the Servlet API and utilizes Servlet semantics. JSP has become the preferred request handler and response mechanism. Although

JSP technology is going to be a powerful successor to basic Servlets, they have an evolutionary relationship and can be used in a cooperative and complementary manner.

Servlets are powerful and sometimes they are a bit cumbersome when it comes to generating complex HTML. Most servlets contain a little code that handles application logic and a lot more code that handles output formatting. This can make it difficult to separate and reuse portions of the code when a different output format is needed. For these reasons, web application developers turn towards JSP as their preferred servlet environment.

5.2.4 Evolution of Web Applications:

Over the last few years, web server applications have evolved from static to dynamic applications. This evolution became necessary due to some deficiencies in earlier web site design. For example, to put more of business processes on the web, whether in business-to-consumer (B2C) or business-to-business (B2B) markets, conventional web site design technologies are not enough. The main issues, every developer faces when developing web applications, are:

1. Scalability - a successful site will have more users and as the number of users is increasing fastly, the web applications have to scale correspondingly.
2. Integration of data and business logic - the web is just another way to conduct business, and so it should be able to use the same middle-tier and data-access code.

3. Manageability - web sites just keep getting bigger and we need some viable mechanism to manage the ever-increasing content and its interaction with business systems.

4. Personalization - adding a personal touch to the web page becomes an essential factor to keep our customer coming back again. Knowing their preferences, allowing them to configure the information they view, remembering their past transactions or frequent search keywords are all important in providing feedback and interaction from what is otherwise a fairly one-sided conversation.

Apart from these general needs for a business-oriented web site, the necessity for new technologies to create robust, dynamic and compact server-side web applications has been realized. The main characteristics of today's dynamic web server applications are as follows:

1. Serve HTML and XML, and stream data to the web client
2. Separate presentation, logic and data
3. Interface to databases, other Java applications, and CORBA, directory and mail services
4. Make use of application server middleware to provide transactional support.
5. Track client sessions.

5.2.5 Benefits of JSP

One of the main reasons why the Java Server Pages technology has evolved into what it is today and it is still evolving is the overwhelming technical need to

simplify application design by separating dynamic content from static template display data. Another benefit of utilizing JSP is that it allows to more cleanly separate the roles of web application/HTML designer from a software developer. The JSP technology is blessed with a number of exciting benefits, which are chronicled as follows:

1. The JSP technology is platform independent, in its dynamic web pages, its web servers, and its underlying server components. That is, JSP pages perform perfectly without any hassle on any platform, run on any web server, and web-enabled application server. The JSP pages can be accessed from any web server.
2. The JSP technology emphasizes the use of reusable components. These components can be combined or manipulated towards developing more purposeful components and page design. This definitely reduces development time apart from the At development time, JSPs are very different from Servlets, however, they are precompiled into Servlets at run time and executed by a JSP engine which is installed on a Web-enabled application server such as BEA Web Logic and IBM Web Sphere.

5.3 Servlets:

Earlier in client- server computing, each application had its own client program and it worked as a user interface and need to be installed on each user's personal computer. Most web applications use HTML/XHTML that are mostly supported by all the browsers and web pages are displayed to the client as static documents.

A web page can merely displays static content and it also lets the user navigate through the content, but a web application provides a more interactive experience.

Any computer running Servlets or JSP needs to have a container. A container is nothing but a piece of software responsible for loading, executing and unloading the Servlets and JSP. While servlets can be used to extend the functionality of any Java- enabled server.

They are mostly used to extend web servers, and are efficient replacement for CGI scripts. CGI was one of the earliest and most prominent server side dynamic content solutions, so before going forward it is very important to know the difference between CGI and the Servlets.

5.4 Java Servlets

Java Servlet is a generic server extension that means a java class can be loaded dynamically to expand the functionality of a server. Servlets are used with web servers and run inside a Java Virtual Machine (JVM) on the server so these are safe and portable. Unlike applets they do not require support for java in the web browser. Unlike CGI, servlets don't use multiple processes to handle separate request. Servets can be handled by separate threads within the same process. Servlets are also portable and platform independent.

A web server is the combination of computer and the program installed on it. Web server interacts with the client through a web browser. It delivers the web pages to the client and to an application by using the web browser and the HTTP protocols respectively.

The define the web server as the package of large number of programs installed on a computer connected to Internet or intranet for downloading the requested files using File Transfer Protocol, serving e-mail and building and publishing web pages. A web server works on a client server model.

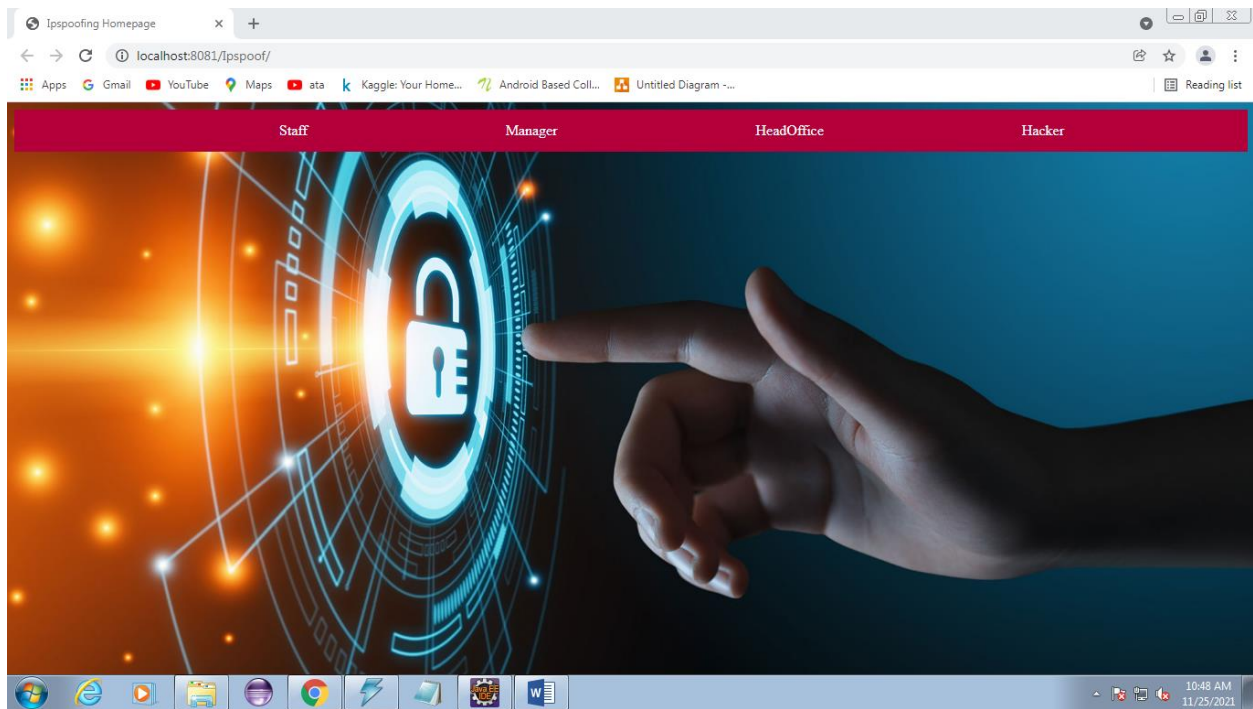
5.5 Conclusion

JSP and Servlets are gaining rapid acceptance as means to provide dynamic content on the Internet. With full access to the Java platform, running from the server in a secure manner, the application possibilities are almost limitless. When JSPs are used with Enterprise JavaBeans technology, e-commerce and database resources can be further enhanced to meet an enterprise's needs for web applications providing secure transactions in an open platform. J2EE technology as a whole makes it easy to develop, deploy and use web server applications instead of mingling with other technologies such as CGI and ASP. There are many tools for facilitating quick web software development and to easily convert existing server-side technologies to JSP and Servlets.

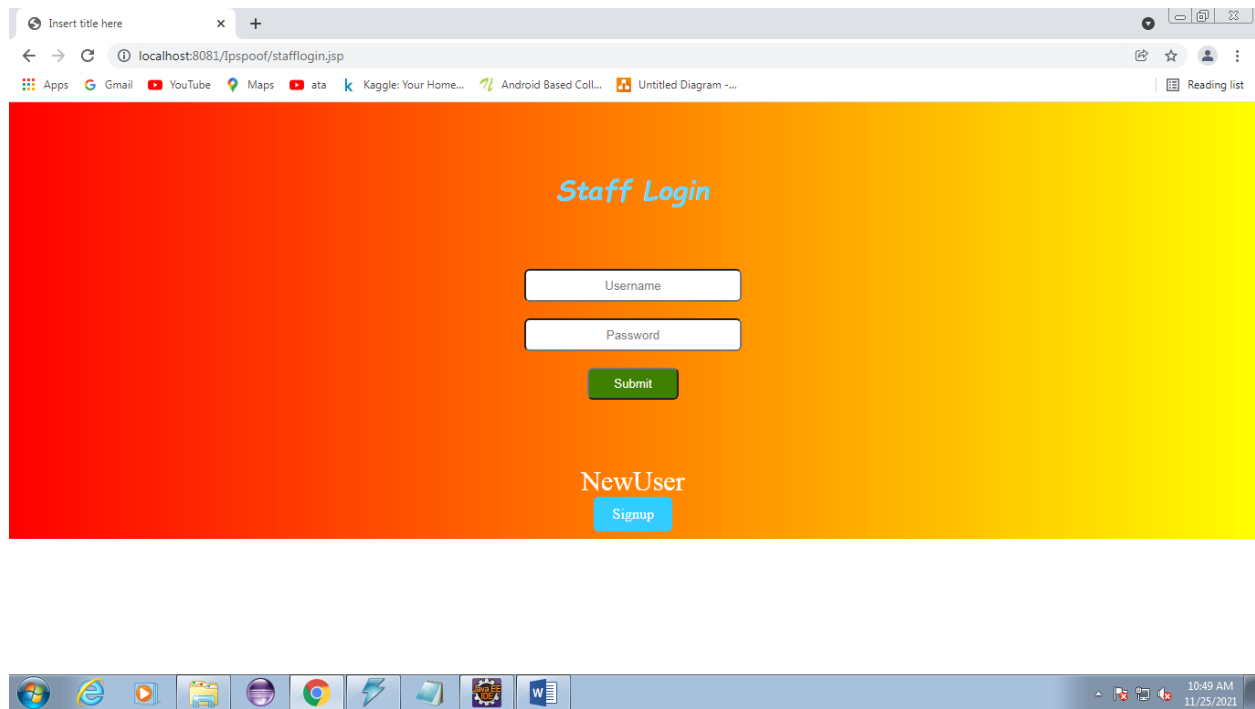
CHAPTER 6

SNAPSHOTS:

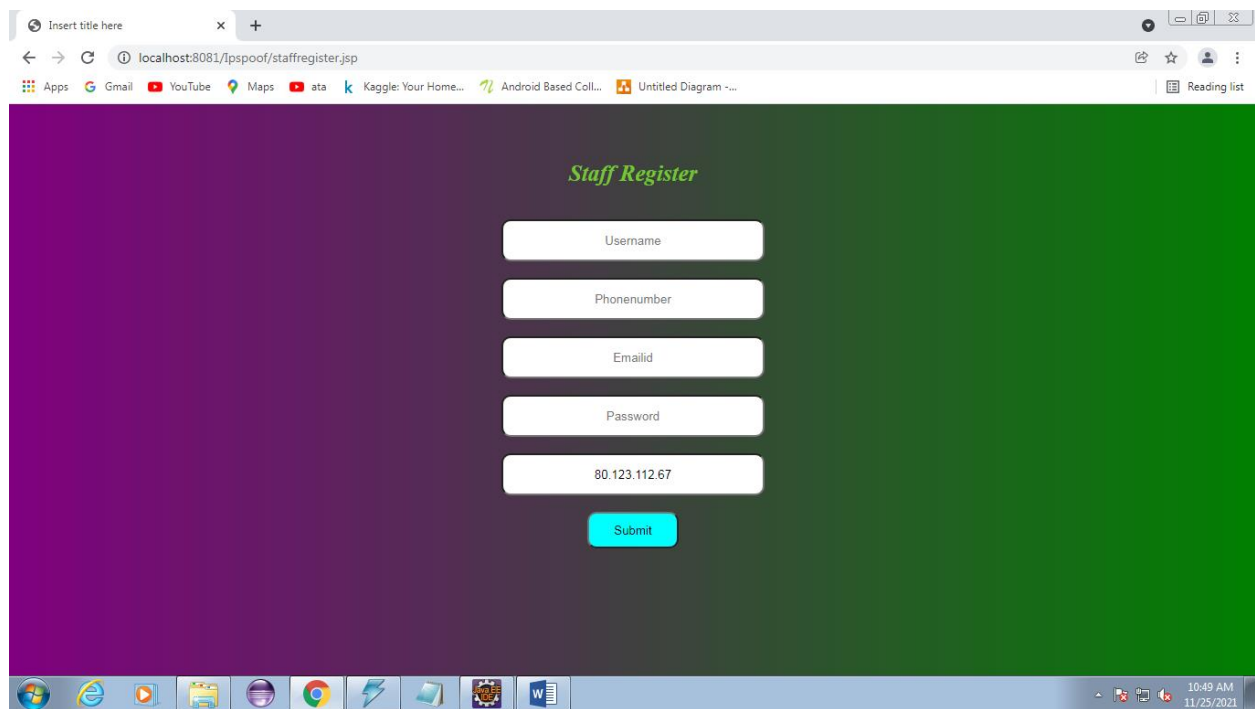
Homepage:



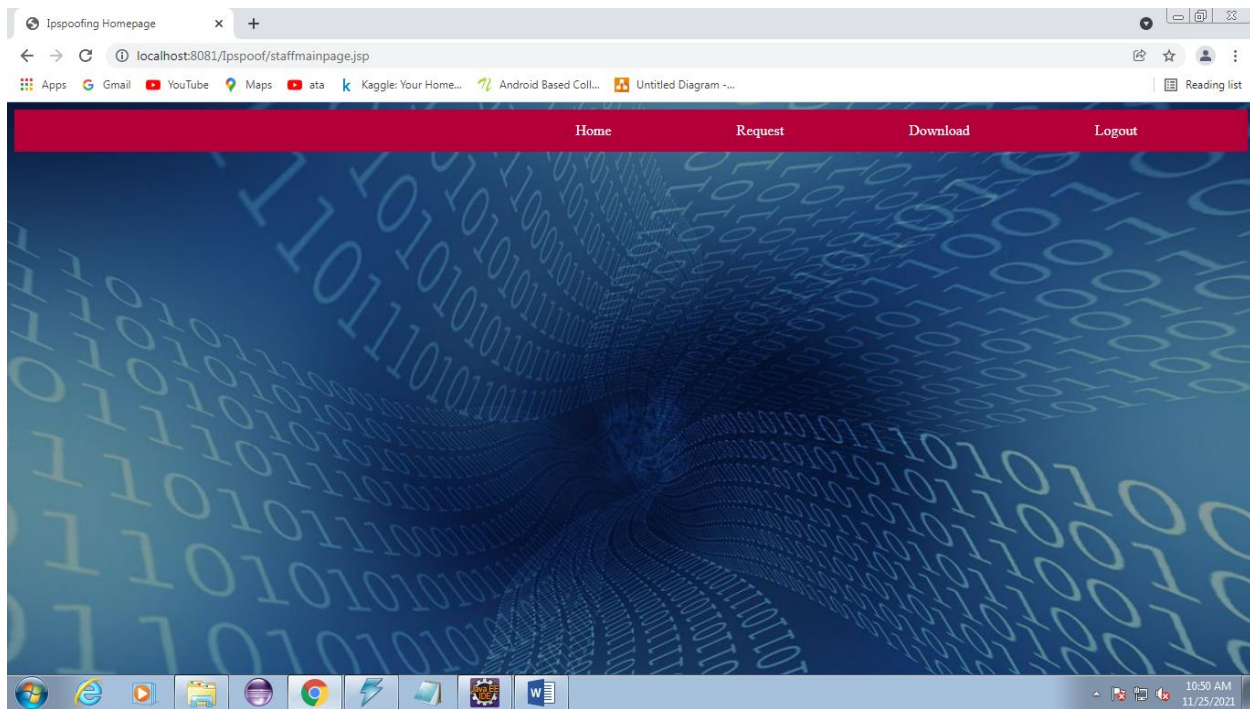
Stafflogin:



Staffregister page:



Staff homepage :



Request page:

Insert title here

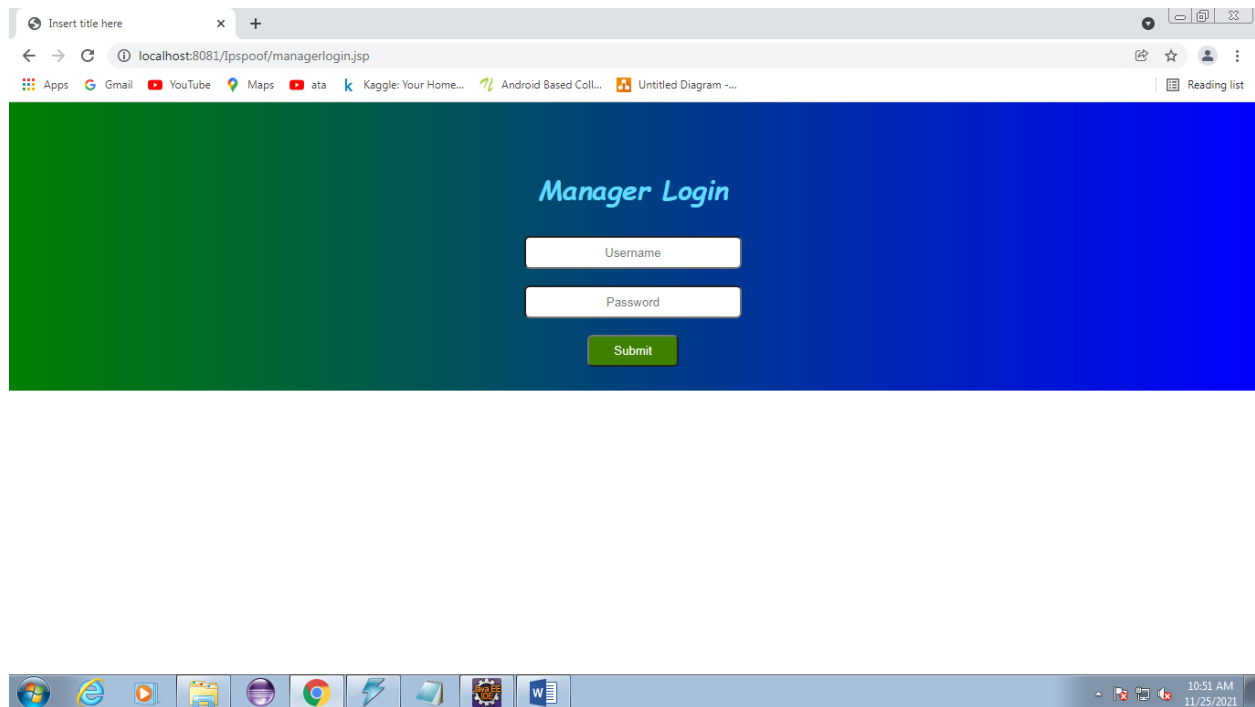
localhost:8081/ipspoof/userrequest.jsp

Staff Viewlist Back

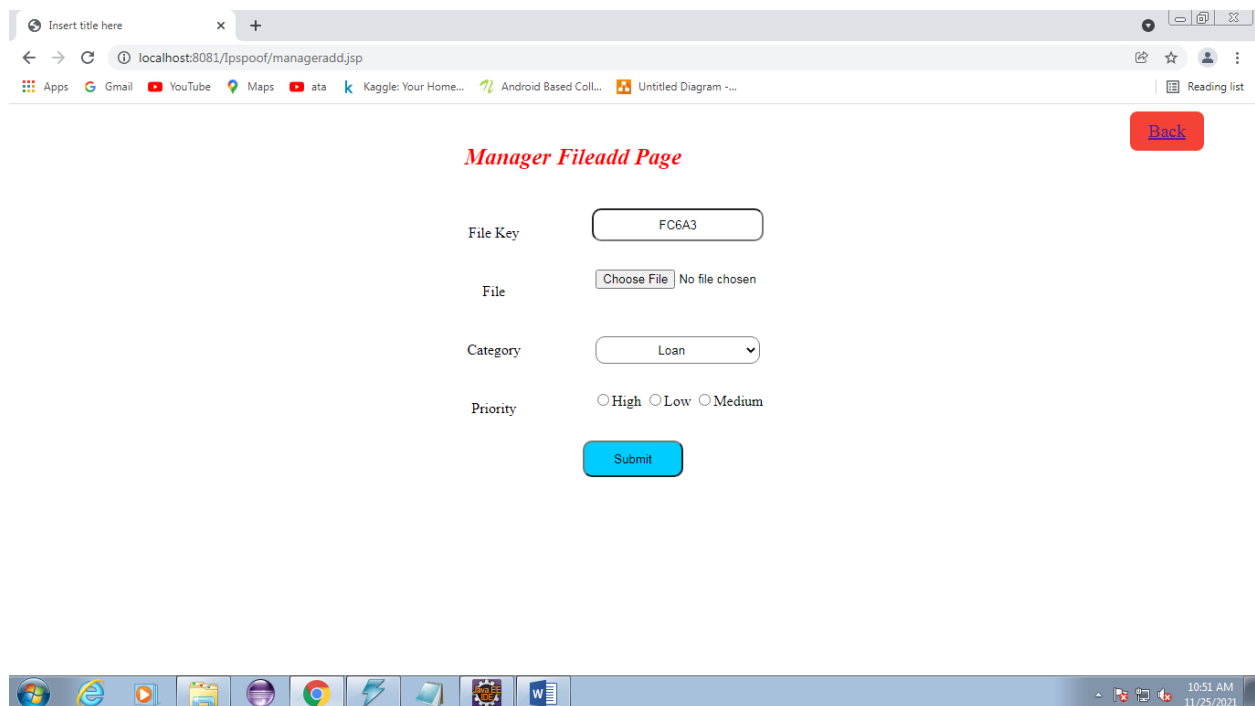
Username	Ippaddress	Filename	Filekey	Category	Priority	Remarks
sss@gmail.com	31.181.137.71	fifth.txt	1E66G	insurance	hight	Request
sss@gmail.com	31.181.137.71	first.txt	1A556	insurance	low	Request
sss@gmail.com	31.181.137.71	second.txt	87GF2	netbanking	high	Request
sss@gmail.com	31.181.137.71	third.txt	G2582	loan	low	Request
sss@gmail.com	31.181.137.71	fourth.txt	9BBF1	atmservice	medium	Request
sss@gmail.com	31.181.137.71	student.pdf.pdf	G9BE9	atmservice	high	Request
sss@gmail.com	31.181.137.71	daily statement.pdf	765C7	insurance	low	Request
sss@gmail.com	31.181.137.71	new.pdf	CEF71	atmservice	low	Request

Windows taskbar at the bottom shows application icons and the system clock indicating 10:50 AM on 11/25/2021.

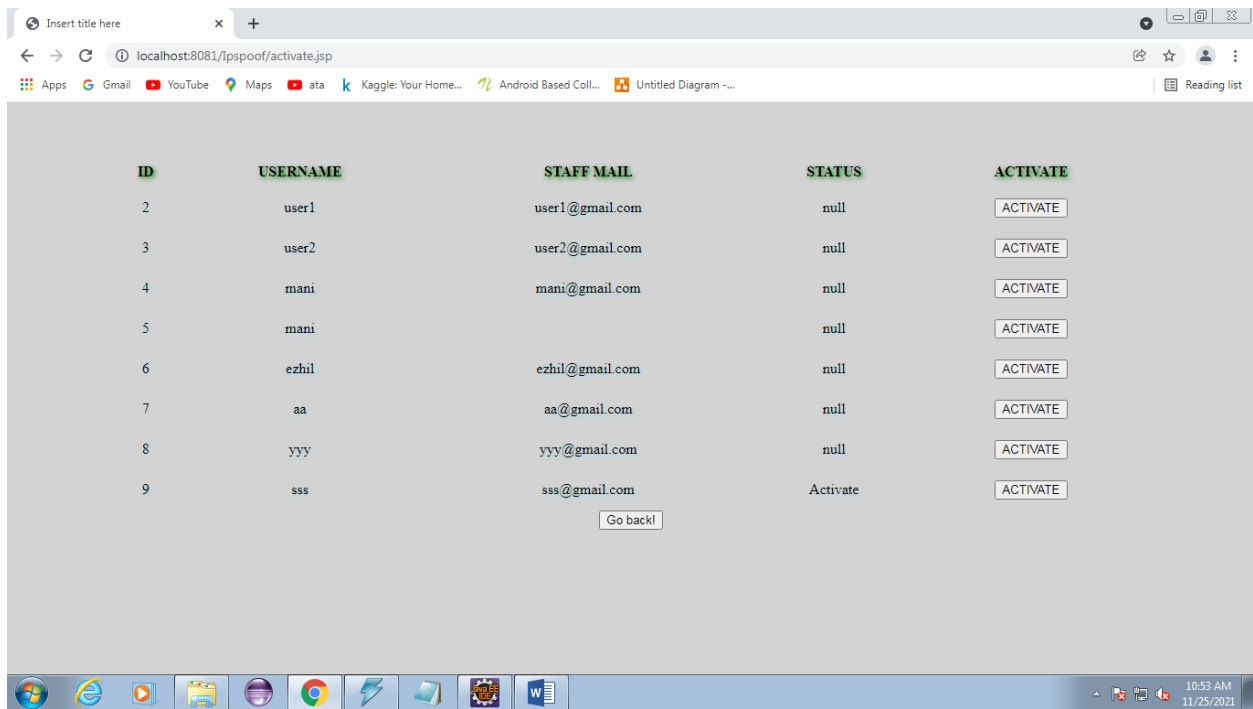
Manager login page:



File add page:



Head activate page:



Head response page:

Insert title here x +

localhost:8081/lpspoof/headrespons.jsp

Apps Gmail YouTube Maps ata Kaggle: Your Home... Android Based Coll... Untitled Diagram ~... Reading list

Head Office Response [Back](#)

Username	Ipaddress	Filename	Filekey	Category	Priority	Remarks
user1@gmail.com	null	first.txt	1A556	insurance	low	Accept
user1@gmail.com	null	second.txt	87GF2	netbanking	high	Accept
user1@gmail.com	167.111.72.34	third.txt	G2582	loan	low	Accept
user1@gmail.com	167.111.72.34					Accept
user1@gmail.com	167.111.72.34					Accept
user2@gmail.com	182.211.132.155					Accept
user1@gmail.com	167.111.72.34					Accept
ezhil@gmail.com	0.158.54.85	student.pdf.pdf	G9BE9	atmservice	high	Accept
user1@gmail.com	167.111.72.34	fifth.txt	1E66G	insurance	hight	Accept
user1@gmail.com	167.111.72.34	fifth.txt	1E66G	insurance	hight	Accept
aa@gmail.com	78.31.107.244	daily statement.pdf	765C7	insurance	low	Accept

10:53 AM 11/25/2021

CHAPTER 7

8.1 FUTURE ENHANCEMENTS:

1. Implementing a real-world anonymous database system.
2. Improving the efficiency of protocols, in terms of number of messages exchanged and in terms of their sizes, as well.
3. Implement using AES algorithm.
4. Manage will find the valid user or hacker for secure the data file.

CONCLUSION:

We envision two research fronts for future work. One is to expand our techniques to reduce cluster sizes even more, e.g., designing new algorithms for choosing targets for poisoning, and using BGP communities for controlling export policies (and influence routing decisions) on remote networks. Another is to expand the system to allow identification of sources of spoofed traffic during DDoS attacks, e.g., by jointly optimizing for cluster size and traffic volume, giving higher utility to reducing the size of clusters inferred to send more spoofed traffic; and (ii) improving existing catchment prediction technique to allow generation of announcement configurations without prior knowledge and reducing the need for measuring catchments in advance.

REFERENCE:

- [1] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, “Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks,” in Proc. ACM IMC, 2014.
- [2] M. Prince, “Technical Details Behind a 400Gbps NTP Amplification DDoS Attack,” Feb 2014. [Online]. Available: <https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack>
- [3] K. York, “Dyn Statement on 10/21/2016 DDoS Attack,” 2016, <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.
- [4] L. H. Newman, “Github Survived the Biggest DDoS Attack ever Recorded,” Wired, March 2018.
- [5] V. Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-service Attacks,” SIGCOMM Comput. Commun. Rev., vol. 31, no. 3, pp. 38–47, 2001.
- [6] “Akamai Q4 2016 State of the Internet – Security Report,” <https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/>.
- [7] E. Targett, “AWS Hit With a Record 2.3 Tbps DDoS Attack,” Jun 2020. [Online]. Available: <https://www.cbronline.com/news/record-ddos-attack-aws>
- [8] H. Burch and B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” in Proc. USENIX Conf. on System Admin., 2000.
- [9] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network Support for IP Traceback,” IEEE/ACM Trans. Netw., vol. 9, no. 3, pp. 226–237, 2001.
- [10] A. Belenky and N. Ansari, “On Deterministic Packet Marking,” Comput. Netw., vol. 51, no. 10, pp. 2677–2700, 2007.
- [11] Z. Gao and N. Ansari, “A Practical and Robust Inter-domain Marking Scheme for IP Traceback,” Comput. Netw., vol. 51, no. 3, pp. 732–750, 2007.
- [12] S. Bellovin, M. Leech, and T. Taylor, “ICMP Traceback Messages,” 2003, <https://tools.ietf.org/html/draft-ietf-itrace-04>.

- [13] M. Sung, J. Xu, J. Li, and L. Li, “Large-scale IP Traceback in Highspeed Internet: Practical Techniques and Information-theoretic Foundation,” IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1253–1266, 2008.
- [14] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, “Single-packet IP Traceback,” IEEE/ACM Trans. Netw., vol. 10, no. 6, pp. 721–734, 2002.
- [15] L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and C. Rossow, “AmpPot: Monitoring and Defending Against Amplification DDoS Attacks,” in Proc. Intl. Symp. on Research in Attacks, Intrusions and Defenses (RAID), 2015.