Discovering Suspicious File Migration With AWS Cloud

A PROJECT REPORT

Submitted by

KIRUBA SHANKAR AP – 312319104075

KESAVAN PR - 312319104072

in partial fulfilment for the award of the Degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

St. JOSEPH'S COLLEGE OF ENGINEERING

(An Autonomous Institution)

St. Joseph's Group of Institutions

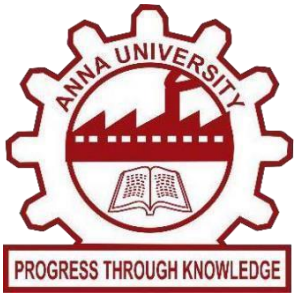
Jeppiaar Educational Trust

OMR, Chennai 600 119

ANNA UNIVERSITY:: CHENNAI 600 025

APRIL 2023

ANNA UNIVERSITY



BONAFIDE CERTIFICATE

Certified that this project report on ***Discovering Suspicious File Migration With AWS Cloud*** *is the bonafide work of* ***KESAVAN PR (312319104072)*** *and* ***KIRUBA SHANKAR AP(312319104075)*** *who carried out the project under mysupervision during the academic year 2022 - 2023.*

Signature of the
Head of the Department

Dr. R. Pugalendhi M.E., Ph. D HOD – Lab Affairs
Department of Computer Science and Engineering
St. Joseph's College of Engineering
OMR, Chennai- 600119.

Signature of the Supervisor

Dr. C. Pandeeswaran M.Tech,Ph.D
SUPERVISOR
Assistant Professor
Department of Computer Science and Engineering
St. Joseph's College of Engineering
OMR, Chennai- 600119

CERTIFICATE OF EVALUATION

COLLEGE NAME **:** St. Joseph's College of Engineering,

BRANCH **:** B.E. - Computer Science and Engineering

SEMESTER VIII

S. No	Name of the Student	Title of The Project	Name of the Supervisor with Designation
1.	KESAVAN.PR (312319104072)	**Discovering Suspicious File Migration With AWS Cloud**	**Dr. C. Pandeeswaran M.Tech,Ph.D.** Assistant Professor
2.	KIRUBA SHANKAR AP. (312319104075)		

The report of the project work submitted by the above students in partial fulfilment for the award of the Degree of Bachelor of Engineering in Computer Science and Engineering at Anna University is confirmed to be a report of the work done by the above students and thenevaluated.

Submitted to Project and Viva Examination held on_____.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

At the outset, we would like to express our sincere gratitude to the **ALMIGHTY** and our beloved ***Chairman, Dr. B. Babu Manoharan M.A., M.B.A., Ph.DSt. Joseph's Group of Institutions*** for his constant guidance and support to the student community and the Society.We would like to express our hearty thanks to our respected ***Managing Director, Mrs. S. Jessie Priya M.Com. St. Joseph's Group of Institutions*** for her kind encouragement and blessings. We wish to express our sincere thanks to our ***Executive Director Mr. B. Shashi Sekar, M.Sc. St. Joseph's Group of Institutions*** for providing ample facilities in the institution.

We would like to express sincere gratitude to our beloved and highly respected ***Principal Dr. Vaddi Seshagiri Rao M.E., M.B.A., Ph.D., F.I.E.*** for his inspirational ideas during the course of the project. We would like to express sincere gratitude and our utmost respect to our beloved ***Dr. B. Parvathavarthini M.E., M.B.A., Ph.D.,Dean (Research)*** for her inspirational ideas during the course of the project.

I also express my sincere thanks and most heartfelt sense of gratitude to **Dr. A.Chandrasekar, M.E., Ph.D., Head of theDepartment of Computer Science and Engineering** for his dedication, commendable support and encouragement for the completion of project work with perfection.

We would like to acknowledge our gratitude to our supervisor **Dr.C. Pandeeswaran M.E., Ph.D** for her excellent guidance and connoisseur's suggestion throughout the study carried out successfully.

Finally, we thank the **Faculty Members** and **our Family**, who helped and encouraged us constantly to complete the project successfully

ABSTRACT

This guides in refining any association's security strategy because of identification of weaknesses, and ensures that the safety efforts were taken and give the assurance that the association expects and requires. Chairman necessities to perform weakness which assists them with uncovering deficiencies of organization security that can prompt gadgets or data to be compromised or obliterated by taking advantage. These results are commonly heterogeneous which makes further examination a difficult errand. Ordinary client organizations might give the way to unapproved individuals access like approved specialists. Whenever, clients step into online organizations, without realizing them outsiders or some other unsafe individuals check their way of behaving. Give security from malevolent movements, administrators or approved individuals likewise check the client organizations, for example, IP address and email. then storing details of the users, files, their encryption, and decryption data in the best type of storage in AWS Cloud by using RDS.

TABLE OF CONTENTS

`

LIST OF FIGURES

` b

` b

LIST OF ABBREVIATIONS

ACRONYM	DESCRIPTION
HDFS	Apache Hadoop Distributed File System
SAN	Storage Area Network
CDR	Call Detail Record
IDS	Intrusion Detection System
LSA	Licensed Service Area
KMS	Key Management System
RDS	Relational Database Service
JVM	Java Virtual Machine
JSP	Java Server Page
DB	DataBase

CHAPTER 1

INTRODUCTION

In this project, we investigate how an organization can control this data source and the looking connection where traffic entrances an organization to all the more unequivocally find wellsprings of ridiculed traffic. Our key perception is that the courses are somewhat under a beginning organization's control, Thus the organization getting the caricature traffic affects which connect it gets traffic, rather than depending on switches that are not influenced quite a bit. We propose procedures that are essentially not the same as existing follow-back draws near and can be utilized today, requiring no progressions to conveyed hardware nor participation from different organizations. Our methods work best when the caricature traffic begins from not many sources, as is normal in enhancement DoS assaults. It is also used for governing file migration with the most enhanced secure algorithm and using the best way to store data and retrieve it.

CHAPTER 2

LITERATURE SURVEY

Systems analysis is the process by which an individual (s) studies a work such that an information system and their work can be analyzed, modeled, and a logical alternative can be chosen.

2.1 EXISTING SYSTEM

In the previously proposed existing work, There is a chance to make the login process by unknown users with valid user mail ids. It may lead to making malicious activities in various ways such as data will be known by unknown users, data or files may be lost, and so on. The users are unable to control the actual locations of their data and the security of the data. This affects users' confidence and trust in the storage provider. To address this issue, They proposed a system which is known as LAST-HDFS, that integrates Location-Aware Storage Technique (LAST) into the (HDFS). The LAST-HDFS system has enforced location-aware file allocations and then it continuously monitors file transfers to detect potentially illegal transfers in the system, and also they implemented a framework and carried out an extensive experimental evaluation, In this work, they use one of the most used cloud storage systems–Hadoop Distributed File System (HDFS), and they design an enhanced HDFS system, it is called as LAST-HDFS. The LAST-HDFS extends HDFS capabilities to achieve location-aware file allocations and file transfer monitoring, and this is one of the least cost models with moderate security methods implemented to protect files from unauthorized users or unauthenticated users.

Technique Involved

HDFS System

Concept:

There is a chance to make the login process by unknown users with valid user's mail ids. It may lead to make the malicious activities in various ways such data will be known by unknown users, data or file may be lost and so on.

Disadvantage:

It keeps different procedures to share the data in different ways. So the probability of suspicious file migration is possible and there is no enhanced security method to allow and deny user activities and to track the records. There is no secure encryption and decryption of Files in the system they store the file as it gets, locate, and distribute it among the users without knowing their privilege. The system interface and HDFS are not easy to use.

2.2 RELATED WORKS

The author Miriam Allalouf, Itai Segall, Muli Ben- Yehuda, and Julian Satran [1] discussed the Block storage listener for detecting train-position intrusions, An intrusion discovery system(IDS) is generally located and operated at the host, where it captures the original suspicious events, or at an appliance that listens to the network exertion. furnishing an online IDS to the storehouse regulator is essential for dealing with compromised hosts or coordinated attacks by multiple hosts. SAN block storehouse regulators are connected to the world via block-position protocols, similar to iSCSI and Fibre Channel. generally, block-position storehouse systems don't maintain information specific to the train system using them. The range of pitfalls that can be handled at the block position is limited. A train system view at the regulator and the knowledge of which arriving block belongs to which train or inode will enable the discovery of train-position pitfalls. In this paper, we

present IDStor, an IDS for block-grounded storehouses. IDStor acts as a listener to storehouse business, out of the regulator's I/ O path, and is thus seductive for integration into being SAN- grounded storehouse results. IDStor maintains a block-to-train mapping that's streamlined online. Using this mapping, IDStor infers the semantics of train-position commands from the interdicted block-position operations, thereby detecting train-position intrusions by simply observing the block read and write commands passing between the hosts and the regulator.

The author Nassir Abuhamoud; Ibrahim Alsadi; Salwa Ali [2] discussed Detecting SIMBox Fraud Using CDR lines And Neo4j Technology, Voice business termination fraud; frequently appertained to as Subscriber Identity Module box(SIMBox) fraud, is a common illegal practice mobile networks, in which cellular drivers around the world dodge billions loss annually. Fraudulent SIMBoxes seize transnational voice calls to be transferred over the Internet to a cellular device network, where it's-injected into the cellular network. thus, calls don't appear original at the destination network, and cellular drivers of intermediate and destination networks don't admit payments for routing and terminating calls. lately, data mining ways have gained great fashionability as a robust and ineluctable fashion among fraud forestallment approaches. This exploration’s end is to describe sim box fraud using CDR lines related to the Almadar Aljadid driver. The CDR line analysis was performed over four months using the Neo4j technology to discover SIM cards used in SIMBox bias. We examine druggies' natural geste to define any suspicious geste to descry fraudulent cards. The data medication process was performed using Python language to be ready for the analysis using Neo4j technology, where Cypher queries for Neo4j technology was written grounded on four features druggies' figures making calls without

entering any, those who entered textbook dispatches without transferring any, figures related to druggies making calls from a fixed position and figures that their calls exceeded the predefined duration. A graphical stoner interface was designed to grease the operation of the practical side of the study. Our result confirms the effectiveness of the neo4j technology to dissect the CDR and therefore fete SIM box frauds.

The author Ethan Katz- Bassett, Colin Scott, and David R. Choffnes [3] discussed the LIFEGUARD Practical form of Persistent Route Failures. The Internet was designed to always find a route if there's a policy biddable path. still, in numerous cases, connectivity is disintegrated despite the actuality of an underpinning valid path. The exploration community has concentrated on short-term outages that do during route confluence. There have been lower progress on addressing avoidable long-lasting outages. Our measures show that long continuing events contribute significantly to overall attainability. We develop LIFEGUARD, an automatic failure localization and remediation system to address these problems. LIFEGUARD uses active measures and a literal path atlas to detect faults in the presence of asymmetric paths and failures. Given the capability to detect faults, we argue that the Internet protocols should allow edge ISPs to steer businesses to them around failures, without taking the involvement of the network causing the failure. Although the Internet doesn't explicitly support this functionality moment, we show how to compare it using precisely drafted BGP dispatches. LIFEGUARD employs a set of ways to reroute around failures with low impact on working routes. Planting LIFEGUARD on the Internet, we find that it can effectively route business around an AS without causing wide dislocation.

The author Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang[4] describes Combating Ransomware using Content Analysis and Complex train Events that, ransomware is a program that scrambles records and requests investiture for their delivery or decoding. A typical strategy to battle ransomware is proved to observe for dubious changes and rehabilitation from(accordingly kept up with) mounts. We offer two styles to work on the cutting edge the study of the document lifecycle and the application of content disquisition. We consider the record lifecycle exercising complex occasions that permit us to all the more likely glass the customer's cerebral model(what the customer thinks he's doing), egging further shrewd document occasion running. Content examination exercising Apache Tika permits us to distinguish assaults by looking for dubious substance-type changes. We execute the two styles in a device(ARW) and demonstrate its viability against the$ ucyLocker ransomware. The two styles ought to be considered for mixing into a living adversary of ransomware instruments to work on their acceptability.

The author Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Vicky [5] discussed distance- predicated system to descry anomalous attributes in log lines that, Nowadays working or accessing a large amount of data logs is like to be trouble in a haystack problem. Changing applicable or existing events can be associated with an incident or real-time analysis of the functional records is delicate, when the underlying data volume is large and no more unambiguous abuse model exists. Certain knowledge may be useful in logging data, but an automated approach for detecting anomalies and for tracking down incidents are the only doable results when defining large volumes of data. So, this paper addresses the issue of automated log analysis and ISP-handed firewall logs. Their work approaches statistical process control and information proposition to track implicit incidents and

then describe suspicious networks.

2.3 MOTIVATION

The main motivation behind aws cloud computing is to enable businesses to get access to data centers and manage tasks from a remote location and t enables organizations to gain additional training and resources (technical, business, sales, and marketing) that will better serve their customers using AWS services and AES encryption uses a “symmetric block cipher” or encryption algorithm developed by the National Institute of Standards and Technology (NIST) in 1997 to make government data less susceptible to brute force attacks and AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

2.4 PROPOSED SYSTEM

We have proposed a system that is used to track the authorized user’s IP address by checking the IP address manually and then giving authorization and privileges based on their need and role, Then the authorized users request the uploaded encrypted file which is uploaded by the managers, Then the requests are received by the managers and after reviewing the IP address, role and their access and privilege to the file, they accept the request and users can access the file and decrypt the file using private and public file key which decrypts the encrypted file, we use QRcode scanner for getting the key. This encryption and decryption technique is based on one of the most secured algorithms called the AES-Algorithm, Then we use AWS Cloud Storage for storing the data and files, We use a Service called RDS from AWS Cloud Which is used as a database.

Outline of Work Design-

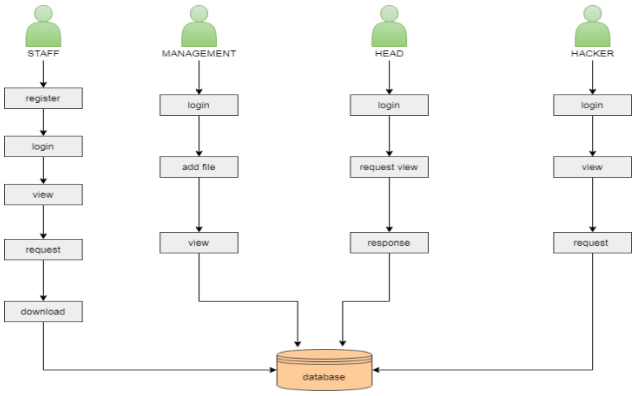


Figure 2.4.1: Outline of the proposed system.

AES-Algorithm

It is known as Advanced Encryption Standard, It is generally employed crucial encryption

computation securing data transfer done in multiple ways. But utmost experts relate to data encryption as a stylish system and presently, Java AES is an advanced result available for calculating. New algorithms are replacing the old values of DES with AES. It has a better heritage of non-public parcels, data authentication, and high situations of integrity. It's a huge advantage over other styles to secure sensitive information. It's a stylish result for government agencies and financial institutions which bear guarding sensitive information. As cybersecurity enterprises arise, the use of AES as an advanced system strikes as stylish volition as it has 3 blocks cipher. Both the sender and receiver retain the same key to keep information classified and uncommunicative. This makes it a flexible and safe tool. It works in a block mode, fixed or sluice mode that uses bits of data. presently, the operations are common for dispatch dispatches, TLS, and also instant messaging. It allows the data to remain secure until it's revealed by a secret key. numerous

enterprises can now use it to keep hackers down from scrabbling information. For agencies that bear data in an unbreakable format announcement also transmitted safely, it's the most flexible and feasible option.

```
public class AES_ENCRYPTION {
    private SecretKey key;
    private final int KEY_SIZE    128;
    private final int DATA_LENGTH = 128;
    private Cipher encryptionCipher;

    public void init() throws Exception {
        KeyGenerator keyGenerator =
KeyGenerator.getInstance("AES");
        keyGenerator.init(KEY_SIZE);
        key = keyGenerator.generateKey();
    }
public String encrypt(String data) throws Exception {
        byte[] dataInBytes = data.getBytes();
        encryptionCipher =
Cipher.getInstance("AES/GCM/NoPadding");
        encryptionCipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] encryptedBytes =
encryptionCipher.doFinal(dataInBytes);
        return encode(encryptedBytes);
    }
```

Figure 2.4.2: Encryption:

```
public String decrypt(String encryptedData) throws Exception {
        byte[] dataInBytes = decode(encryptedData);
        Cipher decryptionCipher =
Cipher.getInstance("AES/GCM/NoPadding");
        GCMParameterSpec spec = new
GCMParameterSpec(DATA_LENGTH, encryptionCipher.getIV());
        decryptionCipher.init(Cipher.DECRYPT_MODE, key, spec);
        byte[] decryptedBytes =
decryptionCipher.doFinal(dataInBytes);
        return new String(decryptedBytes);
    }
```

Figure 2.4.3: Decryption:

The code is a Java class that implements the AES algorithm. The law starts by declaring

variables for the key and the cipher. It also creates an instance of Cipher applying those two variables. Next, it sets up a crucial object with its SecretKeySpec object applied to cipher data in this program. Eventually, it uses the Cipher's doFinal() method to cipher some textbook and save it as a" translated textbook". The code declares three private static final String constants" algorithm"," keyValue" and" encryptText". The first constant is set equal to" AES"; this tells us what encryption algorithm we use(in case we need to change latterly). The alternate constant holds a byte array containing all our keys; these keys will be used throughout this program when demanded. Incipiently, the third constant holds our translated text string; formerly again, this string will be used throughout our program but not outside of it because

there would be no way for someone different to know what value was stored in that variable without knowing how we created it or where we saved it! The code is a simple Java program that encrypts a key using the AES algorithm. The law above begins by declaring a String variable named" algorithm" with the value of" AES". Next, it declares an array named" keyValue" and initializes it to contain the string value" A, S, e, c, u, r, eS, e, c, r, e tK." The ensuing line of code creates a byte() object called" keyValue" and assigns it the values in this array. The final line of code creates a case of java. crypto. Cipher class with the name Cipher and assigns its constructor argument to be equal to the algorithm(the value of String variable The code begins by generating a key. This is done using the induce crucial() method, which returns a crucial object that can be used to cipher and decipher data. Next, the Cipher class is expressed with an algorithm of" AES". The cipher's init() system takes two parameters: the mode in which encryption will take place(in this case, it's set toEncrypt_Mode) and the alternative being the crucial generated before. The coming step in this code block is to initialize the cipher with these values using its init() method. After initialization, we call doFinal(), passing in our plain text as input and entering back translated text as output.

We also render this value into base64 format before returning it for use away within our program or operation. The code is a method that encrypts and decrypts strings. The first line of the code creates a crucial object and uses it to initialize the cipher object with the encryption algorithm. Next, the plain text is translated using Cipher's doFinal() method which returns an array of bytes representing the translated string. Eventually, this new byte array is decoded into base64 garbling format before being returned as a result of this method call. The code performs decryption by initializing with Cipher's init() system and calling doFinal() to recoup the original string from its translated

form.

Shared Key and Public Key Encryption

SKIP uses a combination of shared key cryptography and public key cryptography to protect messages sent between hosts. SKIP hosts use shared traffic keys that change frequently to encrypt data sent from one host to another. To protect these shared traffic keys, SKIP hosts use the public key to calculate an implicit shared secret, which they use to encrypt the shared traffic keys, keeping network communication secure.

Shared Key Encryption

Shared key encryption uses one key to encrypt and decrypt messages. For shared key cryptography to work, the sender and the recipient of a message must both have the same key, which they must keep secret from everybodyelse. The sender uses the shared key to encrypt a message, shown in the following figure, and then sends the ciphertext message to the recipient.

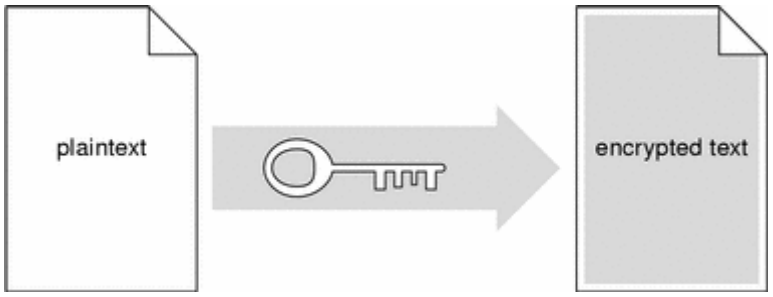


Figure 2.4.4 Sender Uses Key to Encrypt Plaintext to Ciphertext

When the ciphertext message arrives, the recipient uses the identical shared key to decrypt the message, shown in the following figure.

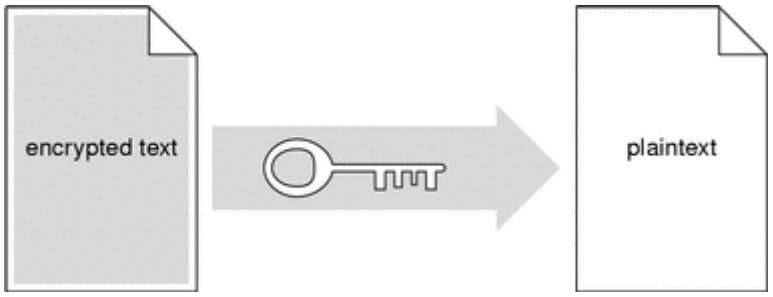


Figure 2.4.5 Recipient Uses Key to Decrypt Ciphertext to Plaintext

Shared key encryption/decryption is relatively fast. However, since anyone with a shared key can decrypt the information, shared key encryption requires that only the sender and recipient have access to the shared key. SunScreen SKIP uses shared key algorithms to encrypt packets sent between hosts. SunScreen SKIP protects the security of encrypted information by generating new traffic keys frequently during a communication session, making the acquisition of any one traffic key useless

Amazon RDS

Amazon RDS is a Relational Database Service, a web service provided by AWS. It is used to set up, operate, scale, and relate databases in AWS Cloud. It also allows us to encrypt our database by using keys and the keys are managed by the AWS Key Management Service (KMS), It stores and manages the keys. And main features of RDS are to keep databases encrypted, automate backups, read replicas, take snapshots automatically, and can make them available globally if needed.

CHAPTER - 3

SYSTEM REQUIREMENTS

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

1. Hardware Requirements.
2. Software Requirements.

3.1 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
- RAM : 2 GB DD RAM
- HARD DISK : 250 GB

3.2 SOFTWARE REQUIREMENTS

Operating system	:	Windows 7, Windows 8, Windows 10 ,
Windows 11 .Language		: Python .
Documentation tool	:	Microsoft word 2007 and Above
Versions .Back end	:	JavaScript .
Simulation Tool	:	Visual Studio Code and Chrome .
Software Needed	:	Visual Studio Code , Python , Tensorflow , Youtube .

3.3 SOFTWARE FEATURES

JAVA

*Java is a **programming language** and a **platform**.* Java is a high-level, robust, Object-oriented and secure programming language. Java was developed by *Sun Microsystems* (which is now a subsidiary of Oracle) in the year 1995. *James Gosling* is known as the father of Java. Before Java, its name was *Oak*. Since Oak was already a registered company, so James Gosling and his team changed the name from Oak to Java.

Platform: Any hardware or software environment in which a program runs, is known as a platform. Since Java has a runtime environment (JRE) and API, it is called a platform.

EASY TO CODE

Java was designed to be easy to use and is therefore easy to write, compile, debug, and learn than other programming languages. Java is object-oriented. This allows you to create modular programs and reusable code. Java is platform-independent.

OPEN SOURCE AND FREE

OpenJDK (Open Java Development Kit) is a free and open-source implementation of Java SE. It is an alternative that allows more than 70% of Java developers to continue stabilizing their Java application environments while remaining within the open-source ecosystem. OpenJDK is primarily licensed under the GNU GPLv2. The freedoms guaranteed by this distribution strategy have made OpenJDK the default choice for Java developers to build desktop applications that are compatible with Java SE.Visual Studio Code

ECLIPSE

Eclipse is an excellent platform for building integrated development environments, it is far more general than that; Eclipse is used as a platform for tools that are not specifically related to software development.

HTML

HyperText Markup Language (HTML) is a simple markup system used to create hypertext documents that are portable from one platform to another. HTML documents are SGML documents with generic semantics that are appropriate for representing information from a wide range of applications.

HTML is a file extension used interchangeably with HTM. ... The HTML tags can be used to define headings,paragraphs, lists, links, quotes, and interactive forms. It can also be used to embed Javascript, and CSS (cascading style sheets).

CSS

CSS stands for Cascading Style Sheets. It is the language for describing the presentation of Web pages, including colours, layout, and fonts, thus making our web pages presentable to the users.

CHAPTER 4

SYSTEM DESIGN

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 SYSTEM ARCHITECTURE DIAGRAM

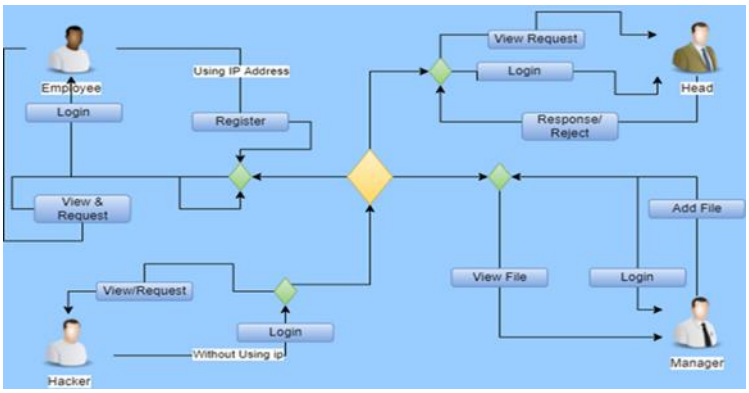


Figure 4.1: System Architecture Diagram

The system's workflow establishes the basic structure and control flow of the system, we propose an algorithm and by that, we can put a small part of data in the local machine and fog server to protect privacy. Moreover, It is based on computational intelligence, this algorithm can compute the distribution proportion stored in the cloud, fog, and local machines, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is a powerful supplement to the existing cloud storage scheme.

4.2 DATA FLOW DIAGRAM

DFD are used to Specify Functions of the Information System and how data flow from functionto function. A data flow diagram has no control flow, there are no decision rules and no loops.Specific operations based on the data can be represented by a flowchart. The data flow diagramis part of the structured analysis modeling tools.

4.2.1 DATA FLOW DIAGRAM AT THE INITIAL LEVEL (Level 0)

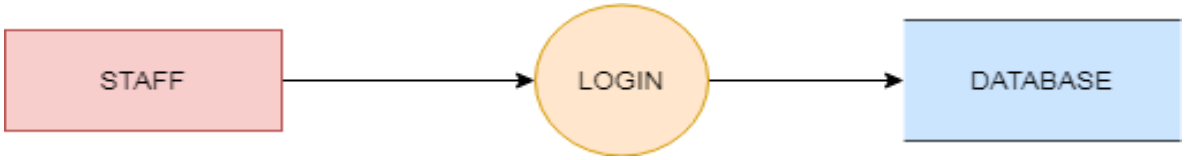


Fig 4.2.1 Flow Diagram Level 0 For The Initial Level

DFD Level 0 is also called a Context Diagram. It's a basic overview of the whole system or process being analyzed or modeled. It's designed to be an at-a-glance view, showing the systemas a single high-level process, with its relationship to external entities .

4.2.2 DATA FLOW DIAGRAM (LEVEL 1)

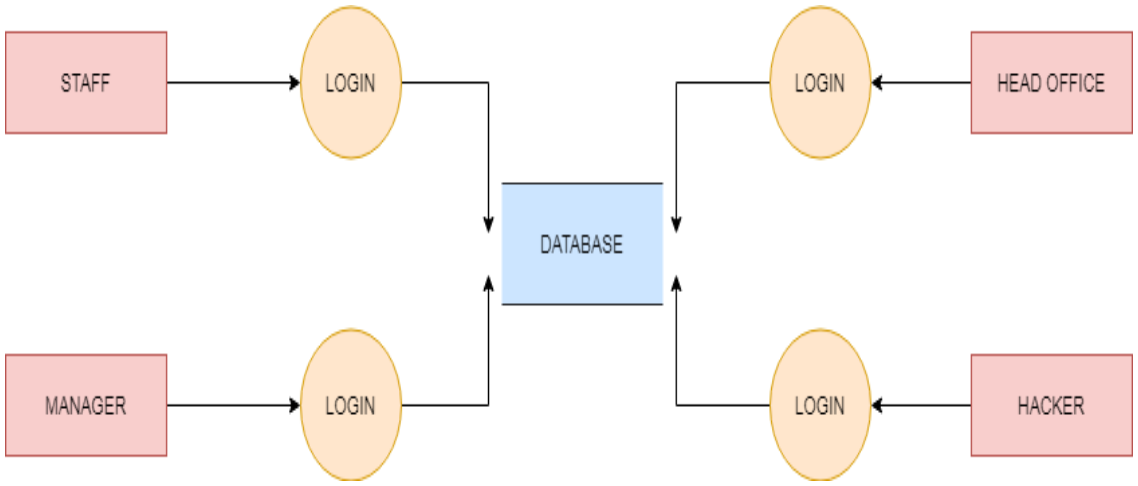
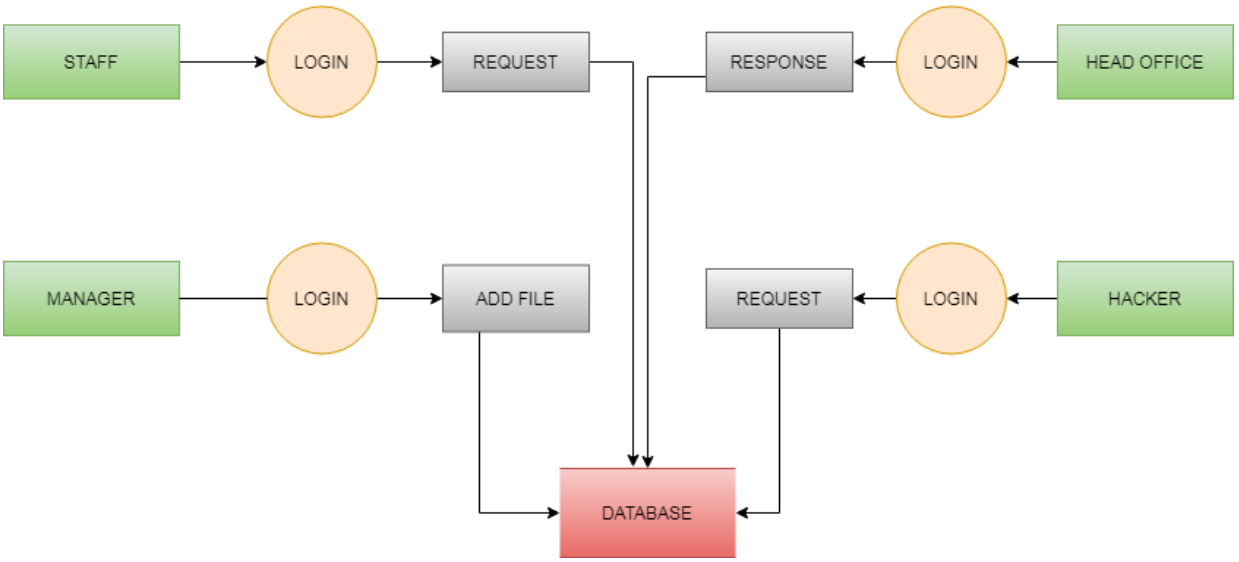


Fig.4.2.2 Data Flow Diagram Level 1

Data Flow Diagram Level 1 describes about the overall representation of each module andits functions. The level one data flow diagram has various modules and ththeirespective results. As described previously, context diagrams (level 0 DFDs) are diagrams where the whole system is represented as a single process. A level 1 DFD notates each of the maisub-processeses that together form the complete system.

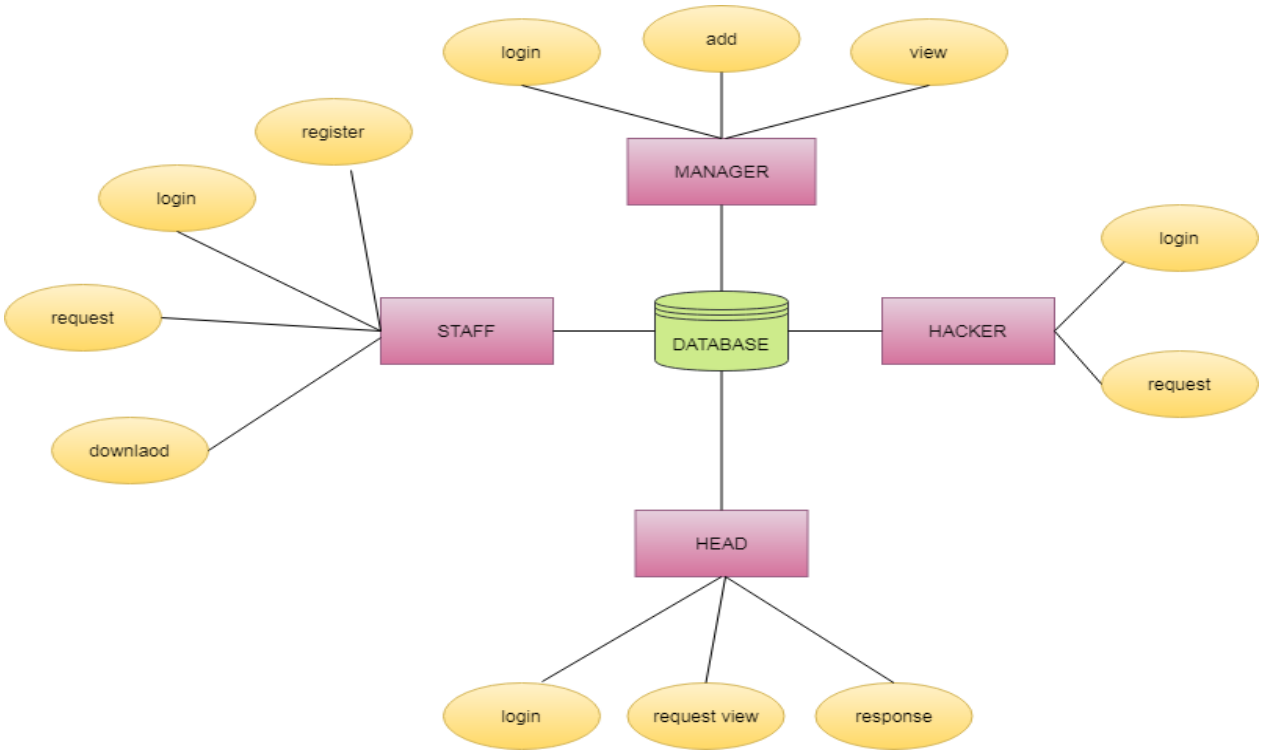
4.2.3 DATA FLOW DIAGRAM (LEVEL 2)

In this level, we highlight the main functions of the system and breakdown the high-level process of 0-level DFD into subprocesses. 2-level DFD: 2-level DFD goes one step deeper intoparts of 1-level DFD. It can be used to plan or record the specific/necessary detail about the system's functioning and We are going to see



Fi g.4.2.3 Data Flow Diagram Level 2

ER DIAGRAM



Fi g.4.2.4 ER Diagram

An entity relationship diagram (ERD), also known as an entity relationship model, is a graphical representation that depicts relationships among people, objects, places, concepts or events within an information technology (IT) system.

4.3 DESIGN DIAGRAMS

USECASE DIAGRAM

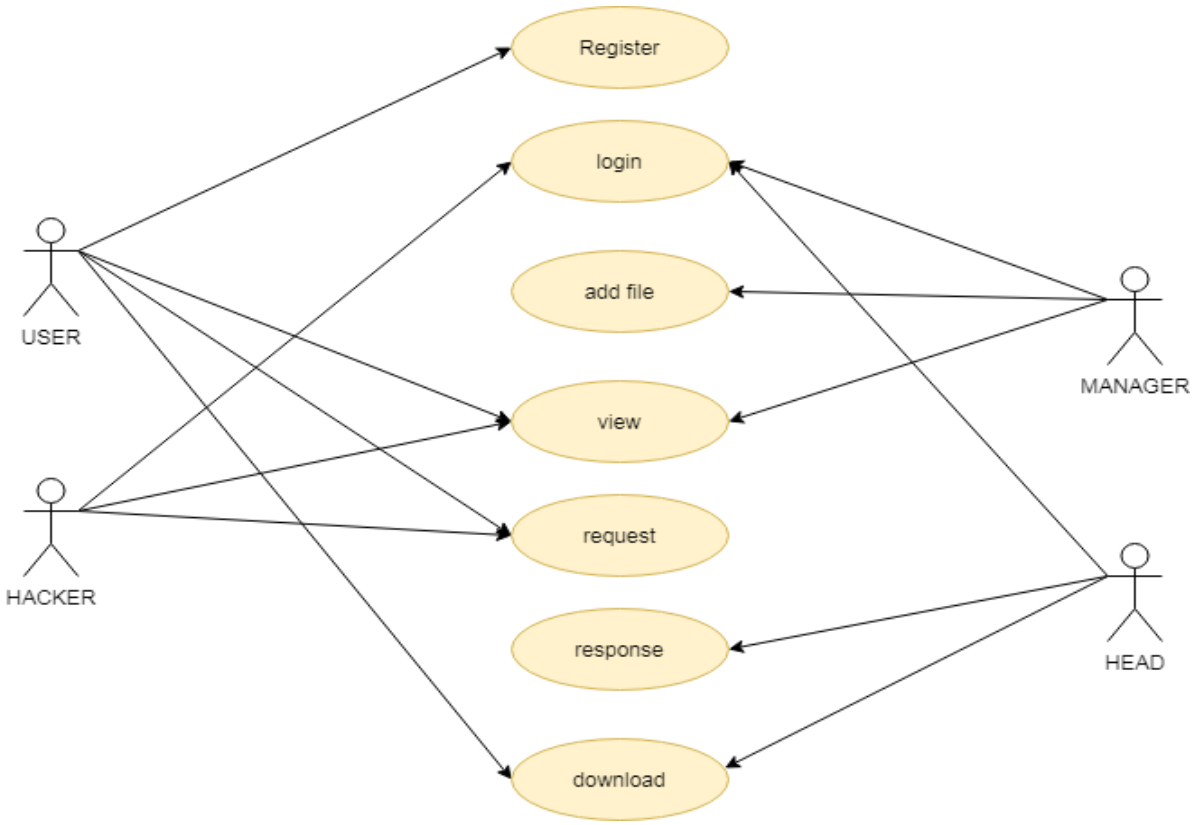


Fig.4.3.1 Usecase Diagram

A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of users the system has and willoften be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses .

SEQUENCE DIAGRAM

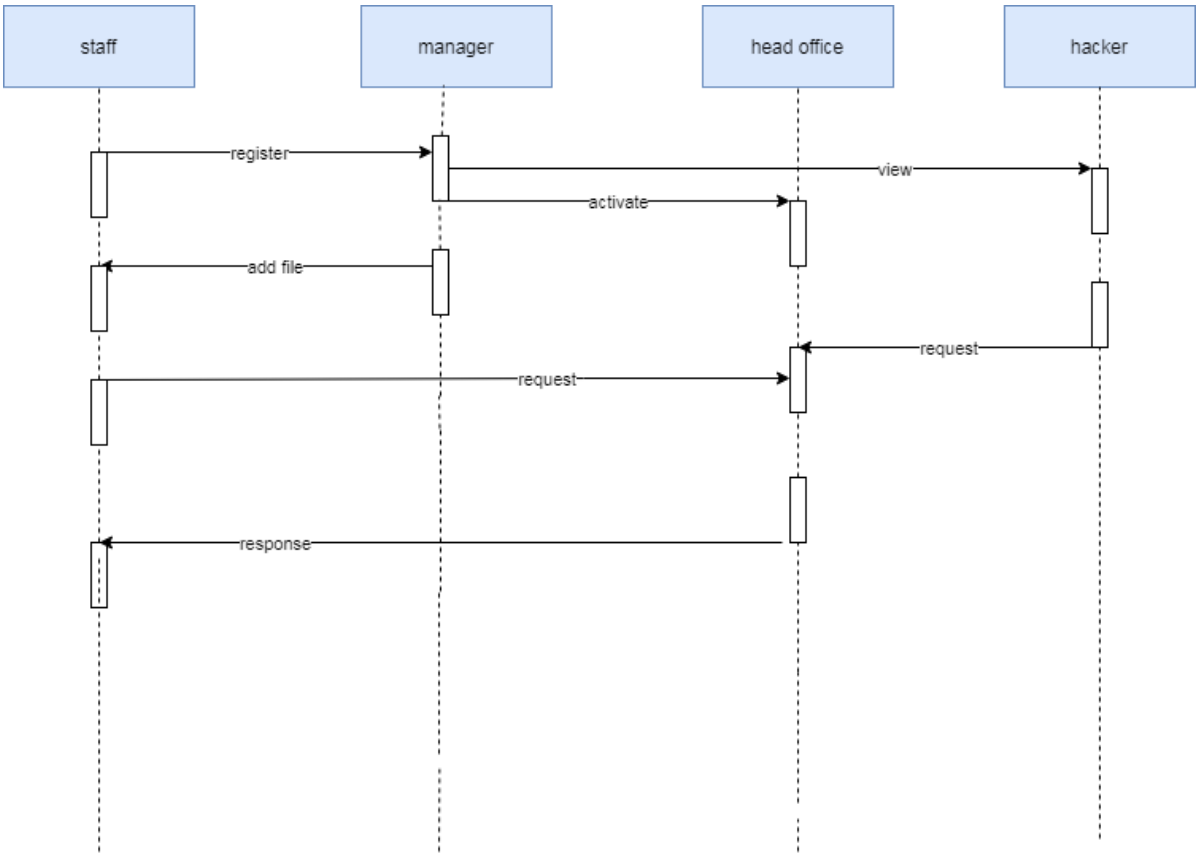


Fig.4.3.2 Sequence Diagram

A sequence diagram or system sequence diagram shows process interactions arranged in time sequence in the field of software engineering. It depicts the processes involved and the sequence of messages exchanged between the processes needed to carry out the functionality.

ACTIVITY DIAGRAM

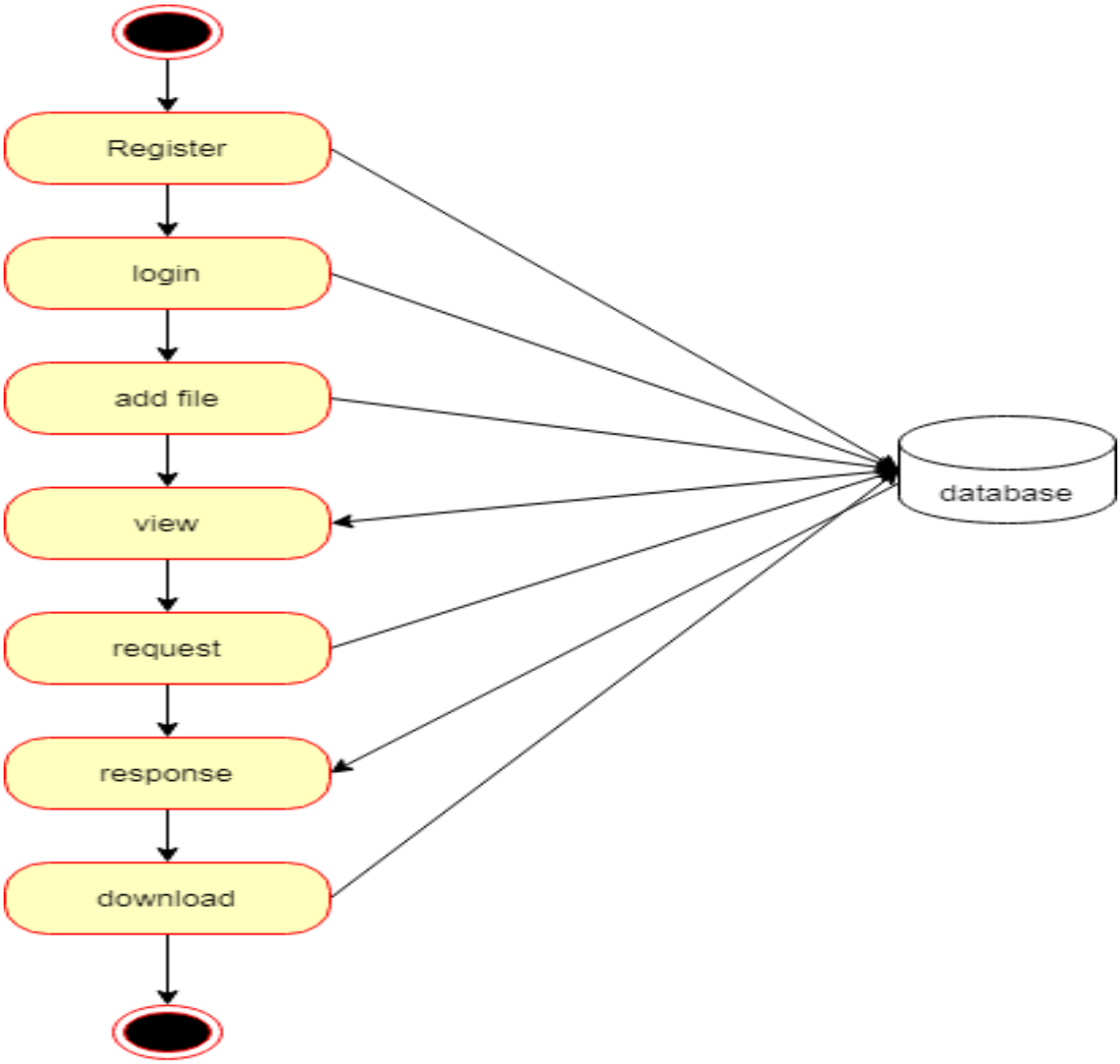


Fig.4.3.3 Activity Diagram

An activity diagram is a behavioral diagram i.e. it depicts the behavior of a system. An activitydiagram portrays the control flow from a start point to a finish point showing the various decision paths that exist while the activity is being executed.

CLASS DIAGRAM

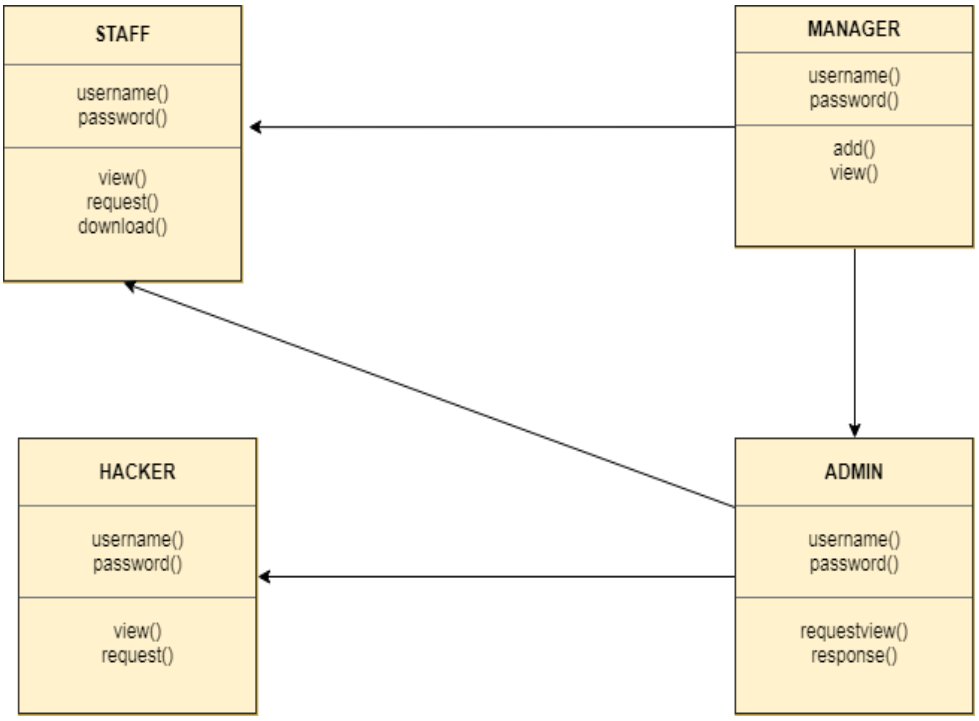


Fig:4.3.4 Class Diagram

The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the structure of the application, and for detailed modeling, translating the models into programming code. Class diagrams can also be used for data modeling.

STATE DIAGRAM

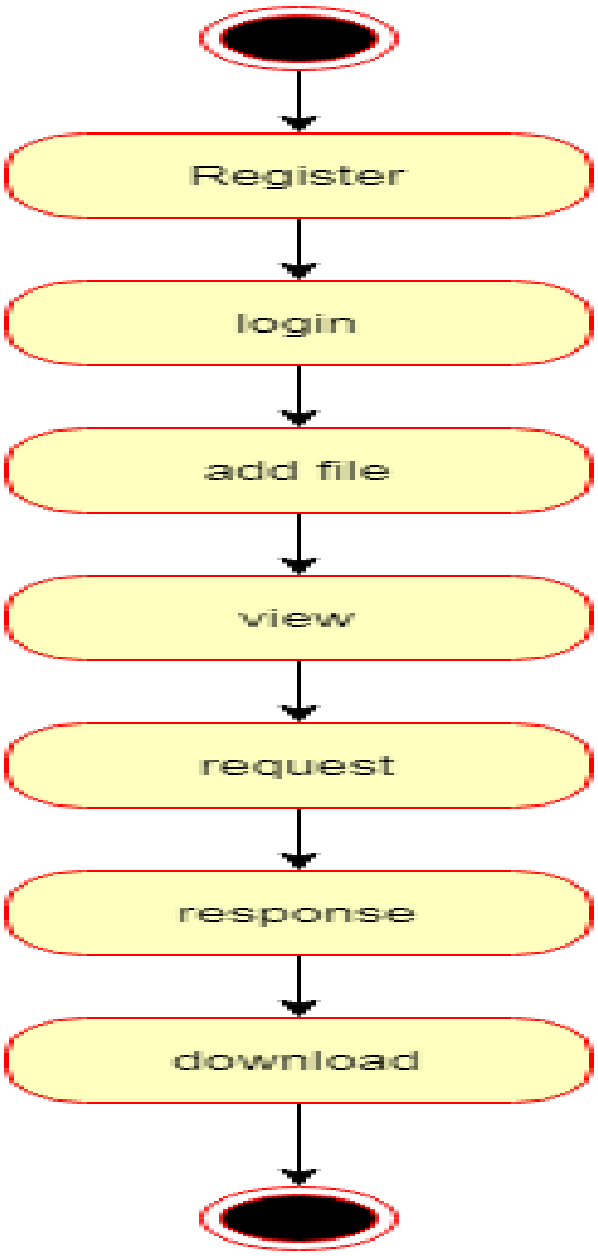


Fig:4.3.5 State Diagram

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction.

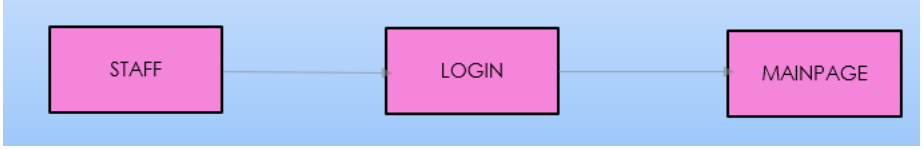
CHAPTER-5

SYSTEM IMPLEMENTATION

5.1 MODULES

LOGIN:

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



5.1.1

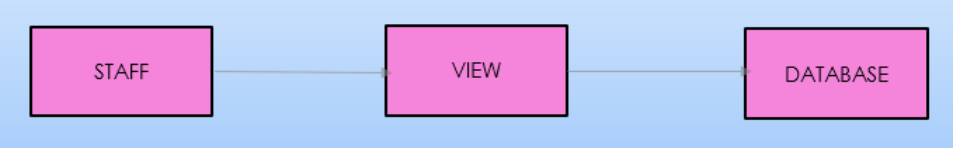
ADD FILE:

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

5.1.2

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.



5.1.3

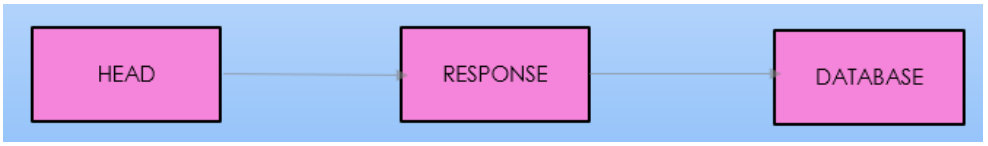
REQUEST:

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.

5.1.4

RESPONSE:

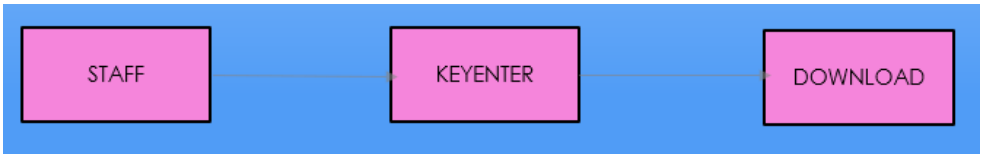
This module to help to staff requested file to head office accept the request. And the hacker or third party also request the file. But the hacker request doesn't Show the ip address of the hacker. Then the head office will identify the requested person is hacker or valid user.



5.1.5

DOWNLOAD:

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



5.1.6

5.2 ALGORITHM:

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember:

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Encryption and Decryption

Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it. Decryption is the process of converting an encrypted message back to its original (readable) format. The original message is called the plaintext message. The encrypted message is called the ciphertext message.

Digital encryption algorithms work by manipulating the digital content of a plaintext message mathematically, using an encryption algorithm and a digital key to produce a ciphertext version of the message. The sender and recipient can communicate securely if the sender and recipient are the only ones who know the key.

5.3 IMPLEMENTATION

JAVA

Java is a **programming language** and a **platform**. Java is a high level, robust, object- oriented and secure programming language.

Java was developed by *Sun Microsystems* (which is now the subsidiary of Oracle) in the year 1995. *James Gosling* is known as the father of Java. Before Java, its name was *Oak*. Since Oak was already a registered company, so James Gosling and his team changed the name from Oak to Java.

Platform: Any hardware or software environment in which a program runs, is known as a platform. Since Java has a runtime environment (JRE) and API, it is called a platform.

```
package servlet;
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import sun.misc.*;
public class AES
{
private static String algorithm = "AES";
private static byte[] keyValue=new byte[]

{ 'A', 'S', 'e', 'c', 'u', 'r', 'e', 'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y' };
```

OPEN SOURCE AND FREE

OpenJDK (Open Java Development Kit) is a free and open-source implementation of Java SE. It is an alternative that allows more than 70% of Java developers to continue stabilizing their Java application environments while remaining within the open-source ecosystem. OpenJDK is primarily licensed under the GNU GPLv2. The freedoms guaranteed by this distribution strategy have made OpenJDK the default choice for Java developers to build desktop applications that are compatible with Java SE.Visual Studio Code

ECLIPSE

Eclipse is an excellent platform for building integrated development environments, it is far more general than that; Eclipse is used as a platform for tools that are not specifically related to software development.

HTML

HyperText Markup Language (HTML) is a simple markup system used to create

hypertext documents that are portable from one platform to another. HTML documents are SGML documents with generic semantics that are appropriate for representing information from a wide range of applications.

HyperText Markup Language (HTML) is the set of markup symbols or codes inserted into a f ile intended for display on the Internet. The markup tells web browsers how to display a web
page's words and images.

HTML is a file extension used interchangeably with HTM. ... The HTML tags can be used to define headings,paragraphs, lists, links, quotes, and interactive forms. It can also be used to embed Javascript, and CSS (cascading style sheets).

HTML tags are like keywords which defines that how web browser will format and display the content.With the help of tags, a web browser can distinguish between an HTML content and a simple content. HTML tags contain three main parts: opening tag, content and closing tag. ... Every tag in HTML perform different tasks.

CSS

CSS stands for Cascading Style Sheets. It is the **l**anguage for describing the presentation of Web pages, including colours, layout, and fonts, thus making our web pages presentable to the users. CSS is designed to make style sheets for the web.

JSP

- Java Server Pages (JSP) is a Web page development technology that supports dynamic content. This allows programmers to use specific JSP tags to insert Java code into HTML pages.
- A part of Java Server Pages is a type of Java servlet designed to perform the

function of a Java web application user interface. Java Server Pages (JSP) is a technology for developing Webpages that supports dynamic content.

- This helps developers insert java code in HTML pages by making use of special JSP tags, most of which start with <% and end with %>. A JSP file is a server-generated web page. It is similar to ASP or JSP Since the Java code is parsed on the web server, the end user never sees the JSP code, but only the HTML generated by the Java code in the page.
- JSP pages can be edited using a web development program or basic text editor.

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

    pageEncoding="ISO-8859-1"%>

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">

<title>Ipspoofing Homepage</title>

<style>

ul {

  list-style-type: none;

  margin: 0;
```

```
  padding: 0;
  overflow: hidden;
  background-color: #b3003b;
}
li {
  float: right;
  padding-right:185px;
}
li a {
  display: block;
  color: white;
  text-align: center;
  text-style:bold;
  padding: 14px 16px;
  text-decoration: none;
}
body {
  background-image: url("bgimages/spoof2.jpg");
```

```
 background-repeat: no-repeat;
 background-size: cover;
}
</style>
</head>
<body>
<ul>
<li><a href="hackerlogin.jsp">Hacker</a></li>
<li><a href="headlogin.jsp">HeadOffice</a></li>
<li><a href="managerlogin.jsp">Manager</a></li>
<li><a href="stafflogin.jsp">Staff</a></li>
</ul>
</body>
</html>
```

Advantages:

- The advantage of JSP is that the programming language used is JAVA, which is a dynamic language and easily portable to other operating systems.
- It is very much convenient to modify the regular HTML. Performance and

scalability of JSP are very good because JSP allows embedding of dynamic elements in HTML pages

5.4 Project Feature Highlights:

1.)To Secure File From Suspicious Migration by Implementing AES Algorithm to Enhance Security Method.

2.)To Provide RDS Cloud From AWS ,It is a Secure Database and Best Type of Storage.

3.)If we Want Replica in Multi AZ also we can migrate easy by using AWS Replication

To Multiple Availability Zone inorder to prevent from datacentre (or) Zone Failure.

CHAPTER-6

RESULT AND EVALUATION

6.1 RESULT

We provide the result of our work with screenshots as proof of work done:

Figure 6.1 Work Result

6.2Limitations

- No native support as a read replica for on-premise Databases.
- CPU and Storage performance is not guaranteed.
- Zero data loss is not guaranteed.
- A major risk to AES encryption comes from side-channel attacks. Rather than attempting a brute-force assault, side-channel attacks are aimed at picking up leaked information from the system. Side-channel attacks, however, may reduce the number of possible combinations required to attack AES with brute force.

6.3 FUTURE ENHANCEMENTS

1. Implementing a true unknown information base framework.
2. Improving the effectiveness of conventions, as far as number of messages traded and concerning their sizes, too.
3. Implement using AES algorithm.
4. Manage will find the legitimate client or programmer for secure the information record.

CHAPTER-7

CONCLUSION

We imagine two examination fronts for future work. One is to extend our methods to lessen bunch estimates considerably more, e.g., planning new calculations for picking focuses for harming, and involving BGP people group for controlling commodity strategies (and impact steering choices) on remote organizations. Another is to grow the framework to permit distinguishing proof of wellsprings of parodied traffic during DDoS assaults, e.g., by (I) mutually enhancing for group size and traffic volume, giving higher utility to diminishing the size of bunches deduced to send more ridiculed traffic; and (ii) further developing existing catchment expectation strategies [18] to permit age of declaration designs without earlier information and lessening the requirement for estimating catchments ahead of time.

One of a Best Encryption Algorithm is used to encrypt and decrypt the file and security enhancement to provide security and protect suspicious filemigration and better storage is applied (Aws Cloud-RDS)

APPENDICES

A1.SOURCE CODE OF AES:

```
package servlet;
  import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import sun.misc.*;
public class AES
{
private static String algorithm = "AES";
private static byte[] keyValue=new byte[]
{ 'A', 'S', 'e', 'c', 'u', 'r', 'e', 'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y' };
        // Performs Encryption
        public static String encrypt99(String plainText) throws Exception
        {
                Key key = generateKey();
                Cipher chiper = Cipher.getInstance(algorithm);
chiper.init(Cipher.ENCRYPT_MODE, key);
                byte[] encVal = chiper.doFinal(plainText.getBytes());
                String encryptedValue = new BASE64Encoder().encode(encVal);
                return encryptedValue;
        }
// Performs decryption
        public static String decrypt(String encryptedText) throws Exception
        {
                // generate key
                Key key = generateKey();
```

```
            Cipher chiper = Cipher.getInstance(algorithm);
            chiper.init(Cipher.DECRYPT_MODE, key);
            byte[] decordedValue = new
BASE64Decoder().decodeBuffer(encryptedText);
            byte[] decValue = chiper.doFinal(decordedValue);
            String decryptedValue = new String(decValue);
            return decryptedValue;
      }
//generateKey() is used to generate a secret key for AES algorithm
      private static Key generateKey() throws Exception
      {
            Key key = new SecretKeySpec(keyValue, algorithm);
            return key;
      }
}
```

A2. SOURCE CODE OF ENCRYPTION AND DECRYPTION

```
package servlet;
import java.security.Key;
import javax.crypto.Cipher;
import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder;

public class Encryptdata {
        public static String encrypt(String Data) throws Exception
        {
              System.out.println("Encrypted in coming");
```

```
            Key key = Publickey.generateKey();
            Cipher c = Cipher.getInstance("AES");
            c.init(Cipher.ENCRYPT_MODE, key);
            byte[] encVal = c.doFinal(Data.getBytes());
            String encryptedValue = new BASE64Encoder().encode(encVal);
            return encryptedValue;
        }
        public static String decrypt(String encryptedData) throws Exception
        {
      Key key = Publickey.generateKey();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.DECRYPT_MODE, key);
      byte[] decordedValue = new BASE64Decoder().decodeBuffer(encryptedData);
      byte[] decValue = c.doFinal(decordedValue);
      String decryptedValue = new String(decValue);
      //System.out.println("key is :::"+ABEKey.generateKey());
      return decryptedValue;
        }
}
```

A3. Mainpage.jsp:

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
 pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Ipspoofing Homepage</title>
<style>
ul {
  list-style-type: none;
  margin: 0;
  padding: 0;
  overflow: hidden;
  background-color: #b3003b;
}
li {
  float: right;
  padding-right:185px;
}
li a {
  display: block;
  color: white;
  text-align: center;
  text-style:bold;
  padding: 14px 16px;
  text-decoration: none;
```

```
}
body {
  background-image: url("bgimages/spoof2.jpg");
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>
<ul>
<li><a href="hackerlogin.jsp">Hacker</a></li>
<li><a href="headlogin.jsp">HeadOffice</a></li>
<li><a href="managerlogin.jsp">Manager</a></li>
<li><a href="stafflogin.jsp">Staff</a></li>
</ul>
</body>
</html>
```

B. SAMPLE OUTPUT

Figure B1: Home page.

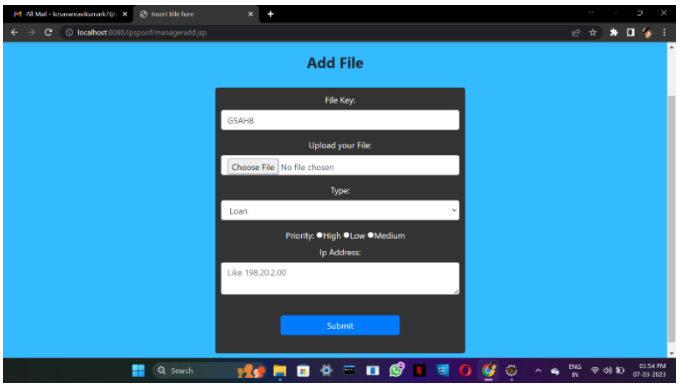


Figure B2: File upload.

Figure B3: Head office page

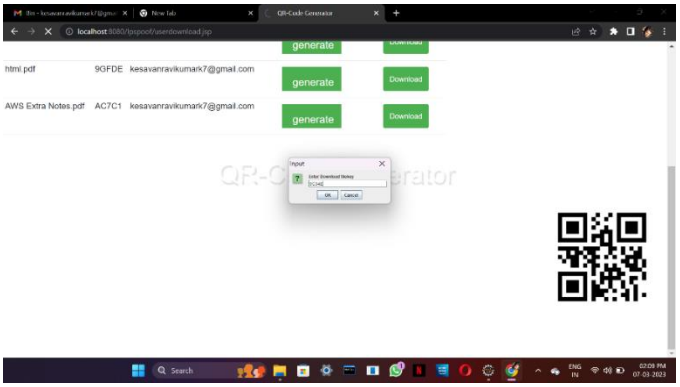


Figure B4: Decryption of a file.

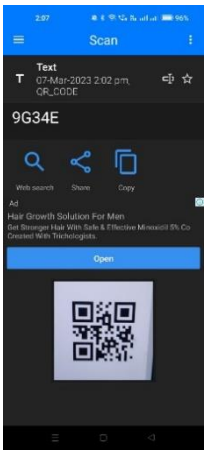


Figure B5: QR code scanner for decryption

REFERENCES

[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-ofservice Attacks," SIGCOMM Comput. Commun. Rev., vol. 31, no. 3, pp. 38–47, 2001.

[6] Miriam Allalouf, Itai Segall, Muli Ben- Yehuda, and Julian Satran, " Block storage listener for detecting train- position intrusions, " in March 2010 at IBM – Haifa Research Labs https//storageconference.us/ 2010/ donations/ disquisition/ 4.Allalouf.pdf

[7] Nassir Abuhamoud; Ibrahim Alsadi; Salwa Ali, " Detecting SIMBox Fraud Using CDR lines And Neo4j Technology, " in 2021 at Tripoli, Libya(IEEE-conference) https//ieeexplore.ieee.org/document/9464510

[8] Ethan Katz- Bassett, Colin Scott, David R. Choffnes, " LIFEGUARD Practical form of Persistent Route Failures, " in 2012 link https//dl.acm.org/doi/10.1145/2342356.2342435

[9] Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang, " Combating Ransomware using Content Analysis and Complex train Events, " in 2017

[10] T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Vicky, “ A distance- predicated system to descry anomalous attributes in log lines, ” in 2019.

[11] L.H. Newman, “ GitHub Survived the Biggest DDoS Attack Ever Recorded, ” Wired, March 2018.

[12] E. Targett, “ AWS megahit With a Record2.3 Tbps DDoS Attack, ” Jun 2020. (Online). Available HTTP// https//www.cbronline.com/news/ record- DDoS- attack- aws