INFORMATION DRIVEN SUPPORT FOR OPTIMIZING CYBER FORENSIC INVESTIGATION IMPROVED WITH SECURITY

A PROJECT REPORT

Submitted by

APARNA.L [REGISTER NO:211419104014]

MADHUMITHA.S [REGISTER NO:211419104156]

PREETHI.K [REGISTER NO:211419104201]

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

APRIL 2023

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **"Information driven support for optimizing cyber forensic investigation improved with security"** is the bonafide work of **"Aparna.L (211419104014), Madhumitha.S (211419104156), Preethi.K (211419104201)"** who carried out the project work under my supervision.

SIGNATURE

Dr.L.JABASHEELA,M.E.,Ph.D.,
HEAD OF THE DEPARTMENT

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE,
NASARATHPETTAI,
POONAMALLEE,
CHENNAI-600 123.

SIGNATURE

Mrs.K.SANGEETHA,M.E.,
ASSISTANT PROFESSOR

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE,
NASARATHPETTAI,
POONAMALLEE,
CHENNAI-600 123.

Certified that the above candidate(s) was/were examined in the End Semester Project Viva-Voce Examination held on.....

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

We…**Aparna.L(211419104014), Madhumitha.S(211419104156), Preethi.K(211419104201)**…. hereby declare that this project report titled **"Information driven support for optimizing cyber forensic investigation improved with security"**, under the guidance of **Mrs.K.Sangeetha,M.E** is the original work done by us and we have not plagiarized or submitted to any other degree in any university by us.

APARNA.L

MADHUMITHA.S

PREETHI.K

ACKNOWLEDGEMENT

We would like to express our deep gratitude to our respected Secretary and Correspondent **Dr.P.CHINNADURAI, M.A., Ph.D.** for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our beloved Directors **Tmt.C.VIJAYARAJESWARI**, **Dr.C.SAKTHI KUMAR,M.E.,Ph.D** and **Dr.SARANYASREE SAKTHI KUMAR B.E.,M.B.A.,Ph.D.,** for providing us with the necessary facilities to undertake this project.

We also express our gratitude to our Principal **Dr.K.MANI, M.E., Ph.D.** who facilitated us in completing the project.

We thank the Head of the CSE Department, **Dr. L.JABASHEELA , M.E.,Ph.D.,** for the support extended throughout the project.

We would like to thank our project guide **Mrs.K.SANGEETHA,M.E.,** and all the faculty members of the Department of CSE for their advice and encouragement for the successful completion of the project.

APARNA.L

MADHUMITHA.S

PREETHI.K

ABSTRACT

The venture known as "*Information-Driven Support for Optimizing Cyber Forensic Investigation improved with security*" is a web based application. This software provides facility for confirming criminal offenses, Problems, losing individuals to DIG. This software provides facility for reporting online crimes, online complaints, missing persons show criminal list and details on web page. Any ordinary person may file a complaint online. Each user first makes their login to server to share their availability. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the unit, whether those functions include high-technology crime investigations, evidence collection, or forensic analysis. However, Cyber forensic contains steps to investigate or collect the data It is defined as the processes and tools used in investigations and gathering evidence. Some of the instruction will be provided as a default such as category wise. By analysing the investigation report, process will be optimized to reduce the investigation process.

KEYWORDS: *Cyber forensic Investigation, Encryption and Decryption, crime detection, digital forensics, Web application*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
DB	DataBase
SMC	Secure Multiparty Computation
DBC	Data Base Confidentiality
JVM	Java Virtual Machine
JSP	Java Server Page

CHAPTER - 1
INTRODUCTION

CHAPTER 1: INTRODUCTION

1.1 OVERVIEW

The field of solving crimes has been completely transformed by modern science and technology, which has also sped up and improved the procedure. The term "forensic" refers to all of the technology and science utilised to solve crimes. This forensic management system's goal is to organise the massive amounts of data generated by the use of cutting-edge technology and scientific methodologies to solve crimes. The system will be able to save particular information in categories when generating a new case file. If the opposite department does not use this system, temporary user profiles can be created so that case files can be quickly collaborated on. "***Information-Driven Support for Optimizing Cyber Forensic Investigation improved with security***" is a web based application. This software provides facility for confirming criminal offenses and provides facility for reporting online crimes, online complaints, missing persons show criminal list and details on web page. Public can complaint through online. Each user first makes their login to server to share their availability. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the unit, whether those functions include high- technology crime investigations, evidence collection, or forensic analysis. However, Cyber forensic contains steps to investigate or collect the data. It is defined as the processes and tools used in investigations

and gathering evidence. Some of the instruction will be provided as a default such as category wise. By analyzing the investigation report, process will be optimized to reduce the investigation process.

1.2 PROBLEM DEFINITION

The increase in crime rate, the fear of crime among the general public, the insufficiency of expertise in the police service to conduct investigations, gather evidence, incriminate suspects are problems that people are facing in their day to day life. The difficulty for the general public in approaching directly each time for giving complaints and data security issues arising with the case details given by the public and data collected by the forensic department. It is important to make it easy for the public to raise complaints against these crimes. Modern science and technology has revolutionized the field of crime solving and has made the process much faster and more reliable. The word Forensic refers to all the science and technology used in the solving of crime. The aim of this Forensic Management System is to manage the large volumes of data that are produced in the process of solving crimes by the application of scientific methods and modern technology. Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. This system can be used to easily collaborate on case files, temporary user profiles can be created if the other department does not implement this system.

CHAPTER - 2
LITERATURE SURVEY

CHAPTER 2: LITERATURE SURVEY

TITLE: Data-Driven Decision Support for Optimizing Cyber Forensic Investigation

AUTHOR: Antonia Nisioti; George Loukas; Aron Laszka; Emmanouil Panaousis

YEAR: 2021

Forensic investigations of cyber assaults that include many attack operations can be quite difficult. Imagine the scenario in which a cyber security breach is suspected after only one attack activity has been identified, for instance, by seeing the alteration of sensitive registry keys, shady network traffic, or the misuse of valid credentials. Every new step will include the same situation. We contend that the effectiveness of this task, which is deciding what action to do next, can significantly affect the inquiry's total cost (for example, the length of the investigation). Here, we introduce DISCLOSE, the first decision support system powered by data for enhancing forensic examinations of cyber security breaches. DISCLOSE makes use of a database of well-known adversarial tactics, techniques, and procedures (TTPs), harvesting threat intelligence data for each one to determine its probability relationships with the others. In a case study using 31 adversarial TTPs, information gathered from six interviews with seasoned cyber security experts, information taken from the MITRE ATT&CK TIX repository, and information obtained from the Common Vulnerability Scoring System, we demonstrate the viability of this technique (CVSS).

MERITS: This paper proposes a novel model for decision support which aims to help the analyst overcome challenges in an efficient and cost-effective manner.

DEMERITS: It has limited functionalities to derive the optimized result as well as this method recommends one attack action at each step.

TITLE: Game Theoretic Decision Support for Cyber Forensic Investigation

AUTHOR: Antonia Nisioti, George Loukas, Stefan Rass, Emmanouil Panaousis

YEAR: 2021

The use of anti-forensic techniques is a very common practice that stealthy adversaries may deploy to minimise their traces and make the investigation of an incident harder by evading detection and attribution. In this paper, we study the interaction between a cyber forensic Investigator and a strategic Attacker using a game-theoretic framework. This is based on a Bayesian game of incomplete information played on a multi-host cyber forensics investigation graph of actions traversed by both players. The edges of the graph represent players' actions across different hosts in a network. In alignment with the concept of Bayesian games, we define two Attacker types to represent their ability of deploying anti-forensic techniques to conceal their activities. In this way, our model allows the Investigator to identify the optimal investigating policy taking into consideration the cost and impact of the available actions, while coping with the uncertainty of the Attacker's type and strategic decisions. To evaluate our model, we construct a realistic case study based on threat reports and data extracted from the MITRE ATT&CK STIX repository, CVSS, and interviews with cyber-security practitioners. We use the case study to compare the performance of the proposed method against two other investigative methods and three different types of Attackers.

MERITS: The proposed method can be utilized as a guide by the Investigator to navigate step by step the analysis of a multi-stage cyber incident.

DEMERITS: For simplicity reasons only one anti-forensic technique is available per edge but there are many options for the attacker.

TITLE: Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform

AUTHOR: Seonghyeon Gong; Changhoon Lee

YEAR: 2021

By their integration with the energy infrastructure, advanced information technologies have evolved into high-level services for the more effective use of energy resources. The energy cloud, which is a component of these technologies, maximises the use of energy resources by fostering an organic relationship between the organisations that create and use the energy. Yet, the disruption or devastation of energy cloud systems by hackers might result in situations like protracted blackouts, which can cause major catastrophes on a global scale. Moreover, the energy cloud environment must be built to withstand assaults given that the sophistication and frequency of contemporary cyber attacks are only becoming better. Yet because the environment of the energy cloud differs from more generic infrastructures like the smart grid and the AMI, it calls for security solutions tailored to the surroundings. This study suggests a system for collecting cyber threat intelligence to enhance the security of the energy cloud environment. By gathering and analysing multiple threat indicators and producing contextual information about the cyber dangers, Cyber Threat Intelligence (CTI) is a technology to actively respond to sophisticated cyber attacks. The architecture outlined in this article evaluates threat indicators that may be gathered using advanced metering infrastructure and suggests a method for generating cyber threat information that targets the energy cloud.

MERITS: The proposed method can be utilized as a guide by the Investigator to navigate step by step the analysis of a multi-stage cyber incident.

DEMERITS: For simplicity reasons only one anti-forensic technique is available per edge but there are many options for the attacker.

TITLE: Unknown Attack Detection Based on Zero-Shot Learning

AUTHOR: Zhun Zhang; Qihe Liu; Shilin Qiu; Shijie Zhou; Cheng Zhang

YEAR: 2020

In recent years, due to the frequent occurrence of network intrusions, more and more researchers have begun to focus on network intrusion detection. However, it is still a challenge to detect unknown attacks. Currently, there are two main methods of unknown attack detection: clustering and honeypot. But they still have unsolved problems such as difficulty in collecting unknown attack samples and failure to detect on time. ZSL is proposed to deal with the problem in this article, which can recognize unknown attacks by learning the mapping relations between feature space and semantic space. When the semantic descriptions of all attacks (including known and unknown attacks) are provided, the classifier built by ZSL can extract common semantic information among all attacks and construct connections between known and unknown attacks. The classifier then utilizes the connections to classify unknown attacks although there are no samples for unknown attacks. In this article, we first propose to use ZSL to overcome the challenge of unknown attack detection and illustrate the feasibility of this method. Secondly, we then propose a novel method of ZSL based on sparse auto encoder for unknown attack detection. Verification tests have been carried out by using the public dataset NSL_KDD. From the experiments conducted in this work, the results show that the average accuracy reaches 88.3%, which performs better than other methods.

MERITS: ZSL method can effectively improve the accuracy of unknown attack detection and the ability to recognize intrusion. It does not need to collect detailed samples of unknown attacks in advance, only needs to collect feature descriptions of unknown attacks.

DEMERITS: ZSL can only be used to train the models only with using the existing scenarios but cannot manage new cases.

TITLE: A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)

AUTHOR: Amol Borkar, Akshay Donode, Anjali Kumari

YEAR: 2017

Around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat. Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks. Data mining methods are proposed for cyber analytics in support of intrusion detection..

MERITS: IIDPS system provides comprehensive protection against identity theft, information mining, and network hacking, with constant network monitoring and improved detection accuracy.

DEMERITS: The main disadvantage of intrusion detection systems is their inability to tell friend from foe, is overcome using IIDPS system.

TITLE: Domain Specific Cyber Forensic Investigation Process Model

AUTHOR: Rabail Shafique Satti and Fakeeha Jafari

YEAR: 2015

Digital Forensics can be defined as a field of study involving the usage of technical and proved procedures for collecting, preserving, validating, analyzing, interpreting and presenting the digital evidences extracted from the digital sources for presenting those in the court of law. Different process models have been proposed by the researchers for cyber crimes' investigation process, each having its own suitability to environments where they are applicable and other pros and cons. The paper includes the tailoring of existing process models to the particular domain of higher education institutes. With the growing access of computing resources and internet to the students, employees and overall citizens, it is the need of time that organizations should establish and maintain their cyber forensics analysis policy along with whole process to be followed in case of any cyber crime scene reporting.

MERITS: The proposed model (DSCFIPM) can serve the purpose of laying foundation for providing secure and monitored computing environment.

DEMERITS: The model should suit the nature and requirements of the domain and moreover the particular case undertaken for investigations.

TITLE: A Multi-layer Semantic Approach for Digital Forensics Automation for Online Social Networks

AUTHOR: Humaira Arshad, Saima Abdullah, Moatsum Alawida Abdulatif

YEAR: 2012

Nowadays, social media platforms are widely used by law enforcement and legal advisors to quickly get information on the organizers of illicit gatherings. Yet, due to diverse and unstructured data and privacy restrictions, obtaining this publicly available information for legal purpose is technically difficult and legally complex, creating a huge workload of cognitively taxing cases for investigators. Thus, it is crucial to create programs and equipment that can aid researchers in their research and decision-making. Automating digital forensics is not only a technological challenge; there are always privacy and legal concerns in addition to the technical ones. Here, we provide a multi-layer automation strategy that covers the automation difficulties in online social network forensics from evidence gathering to analysis. The collection of analytic operators we provide in the end is based on domain correlations. To assist the investigators in reaching valid findings, these operators can be included into software tools. Using Twitter ontology, these operators are put into practise and put to the test using a case study. The proof-of-concept method for forensic automation on online social networks is described in this article.

MERITS: This system has separate models for managing evidence collection, analysis, and interpretation. Work explains a model that allows the extraction of essential data from online social networks and prepares them to be presented in legally acceptable formats.

DEMERITS: The inability to deal with data complexities might lead to errors in the process that would severely affect the subjectivity.

TITLE: The Proactive and Reactive Digital Forensics Investigation Process

AUTHOR: Soltan Alharbi1, Jens Weber-Jahnke, IssaTraoreSoltanAlharbi

YEAR: 2011

Recent papers have urged the need for new forensic techniques and tools able to investigate anti-forensics methods, and have promoted automation of live investigation. Such techniques and tools are called proactive forensic approaches, i.e., approaches that can deal with digitally investigating an incident while it occurs. To come up with such an approach, a Systematic Literature Review (SLR) was undertaken to identify and map the processes in digital forensics investigation that exist in literature. According to the review, there is only one process that explicitly supports proactive forensics, the multi component process. However, this is a very high-level process and cannot be used to introduce automation and to build a proactive forensics system. As a result of our SLR, a derived functional process that can support the implementation of a proactive forensics system is proposed.

MERITS: It is a functional process compared to the high-level multi-component process. Gives solid leads so that the responsive component can happen.

DEMERITS: Not yet fully implemented and may be adapted to implementation requirements.

TITLE: Cyber Forensics Ontology for Cyber Criminal Investigation

AUTHOR: Heum Park, SunHo Cho, Hyuk-Chul Kwon

YEAR: 2009

We developed Cyber Forensics Ontology for the criminal investigation in cyber space. Cyber crime is classified into cyber terror and general cyber crime, and those two classes are connected with each other. The investigation of cyber terror requires high technology, system environment and experts, and general cyber crime is connected with general crime by evidence from digital data and cyber space. Accordingly, it is difficult to determine relational crime types and collect evidence. Therefore, we considered the classifications of cyber crime, the collection of evidence in cyber space and the application of laws to cyber crime. In order to efficiently investigate cyber crime, it is necessary to integrate those concepts for each cyber crime-case. Thus, we constructed a cyber forensics domain ontology for criminal investigation in cyber space, according to the categories of cyber crime, laws, evidence and information of criminals. This ontology can be used in the process of investigating of cyber crime-cases, and for data mining of cyber crime; classification, clustering, association and detection of crime types, crime cases, evidences and criminals.

MERITS: This concept can be used for data extraction as well as the investigation of cybercrime cases. It can be used to convict criminals, it is cost effective, it is tamper proof, and it is admissible in court.

DEMERITS: It is time consuming, it requires special training, and it can be expensive.

CHAPTER - 3
SYSTEM ANALYSIS

CHAPTER 3: SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. Here, DISCLOSE, the first data-driven decision support framework for optimizing forensic investigations of cyber security breaches. DISCLOSE benefits from a repository of known adversarial tactics, techniques, and procedures (TTPs), for each of which it harvests threat intelligence information to calculate its probabilistic relations with the rest. General objective of a Disclosure Framework is to ensure that all and only relevant information is disclosed in an appropriate manner, so that detailed information does not obscure relevant information in the notes.

3.1.1 DEMERITS OF THE EXISTING SYSTEM:

- It has limited functionalities to derive the optimized result.
- The use of disclose framework technology is based on probabilistic standards and need not to be accurate all the time.

3.2 PROPOSED SYSTEM:

The system is a hybrid model making use of two encrypting algorithms while transferring data from one module to another. Data will be analyzed to optimize the process. From the report, analysis process provides the decision making solution. Cyber forensic contains steps to investigate or collect the data It is defined as the processes and tools used in investigations and gathering evidence. Some of the instruction will be provided as a default such as category wise. By analyzing the investigation report, process will be optimized to reduce the investigation process. In our system, we make use of AES Algorithm and blowfish Algorithm which enhances the security of the information as well as make it difficult to decrypt.

3.2.1 ADVANTAGES OF THE PROPOSED SYSTEM:

Two different algorithms (i.e) AES Algorithm and Blowfish algorithm can be used for efficient data functionality when compared to disclosure framework technology.

- AES algorithm can be used for storing large amount of information and provides enhanced data security.
- Blowfish is a symmetric key encryption technique designed as an alternative to the DES encryption algorithm.

CHAPTER - 4
REQUIREMENTS ANALYSIS

CHAPTER 4: REQUIREMENTS ANALYSIS

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.

4.1 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	:	PENTIUM IV 2.6 GHz,Intel Core 2 Duo.
RAM	:	4GB DD RAM
MONITOR	:	15" COLOR
HARD DISK	:	40 GB

4.2 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 team's progress throughout the development activity.

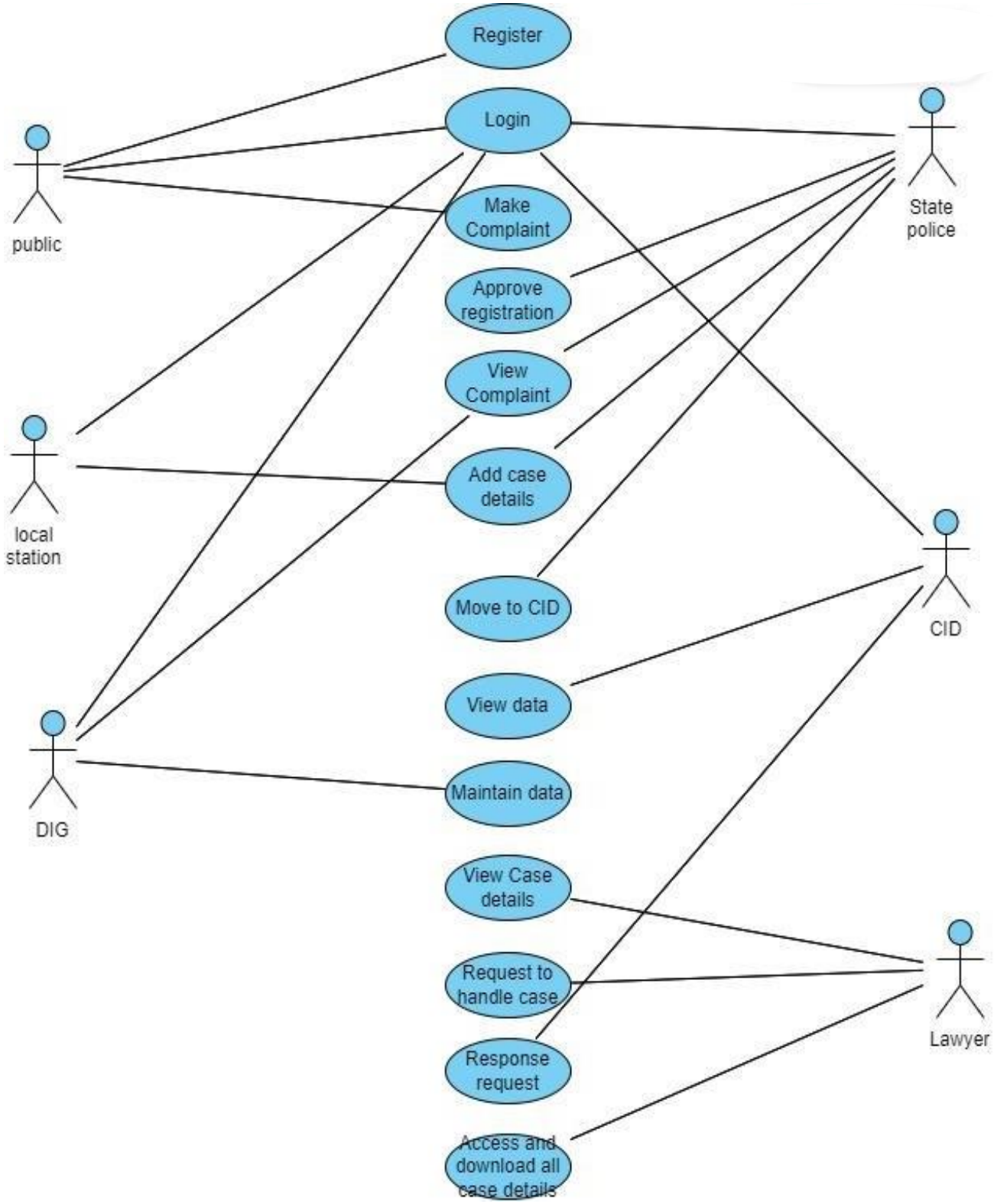
Front End	:	J2EE (JSP, SERVLETS) JAVASCRIPT
Back End	:	MY SQL 5.5
Operating System	:	Windows 07
IDE	:	Eclipse

CHAPTER - 5
SYSTEM DESIGN

CHAPTER 5: SYSTEM DESIGN

UML DIAGRAMS

5.1 USE-CASE DIAGRAM:



EXPLANATION:

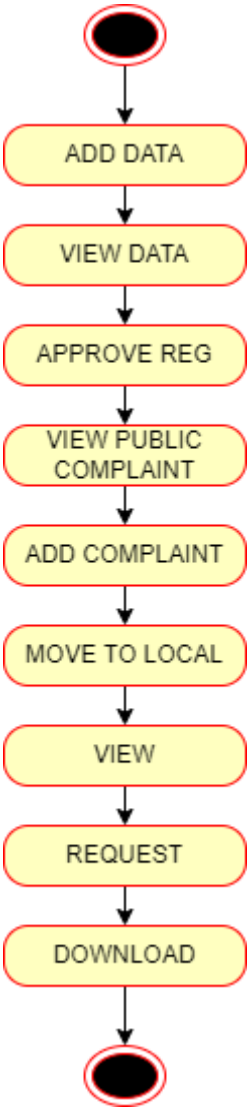
A use case diagram is a type of Unified Modelling Language (UML) diagram that represents the interactions between a system and its actors, and the various use cases that the system supports. It is a visual representation of the functional requirements of the system and the actors that interact with it.

Use case diagrams typically include the following elements:

- Actors: Actors are external entities that interact with the system. They can be human users, other systems, or devices.
- Use Cases: Use cases are the specific functions or tasks that the system can perform. Each use case represents a specific interaction between an actor and the system.
- Relationships: Relationships are used to indicate how the actors and use cases are related to each other. The two main relationships in a use case diagram are "uses" and "extends". "Uses" relationship indicates that an actor uses a specific use case, while "extends" relationship indicates that a use case extends or adds functionality to another use case.
- System Boundary: The system boundary is a box that contains all the actors and use cases in the system. It represents the physical or logical boundary of the system being modelled.

Use case diagrams are useful for identifying the functional requirements of a system, and for communicating these requirements to stakeholders. They can be used in the requirements gathering phase of software development, as well as in the design and testing phases.

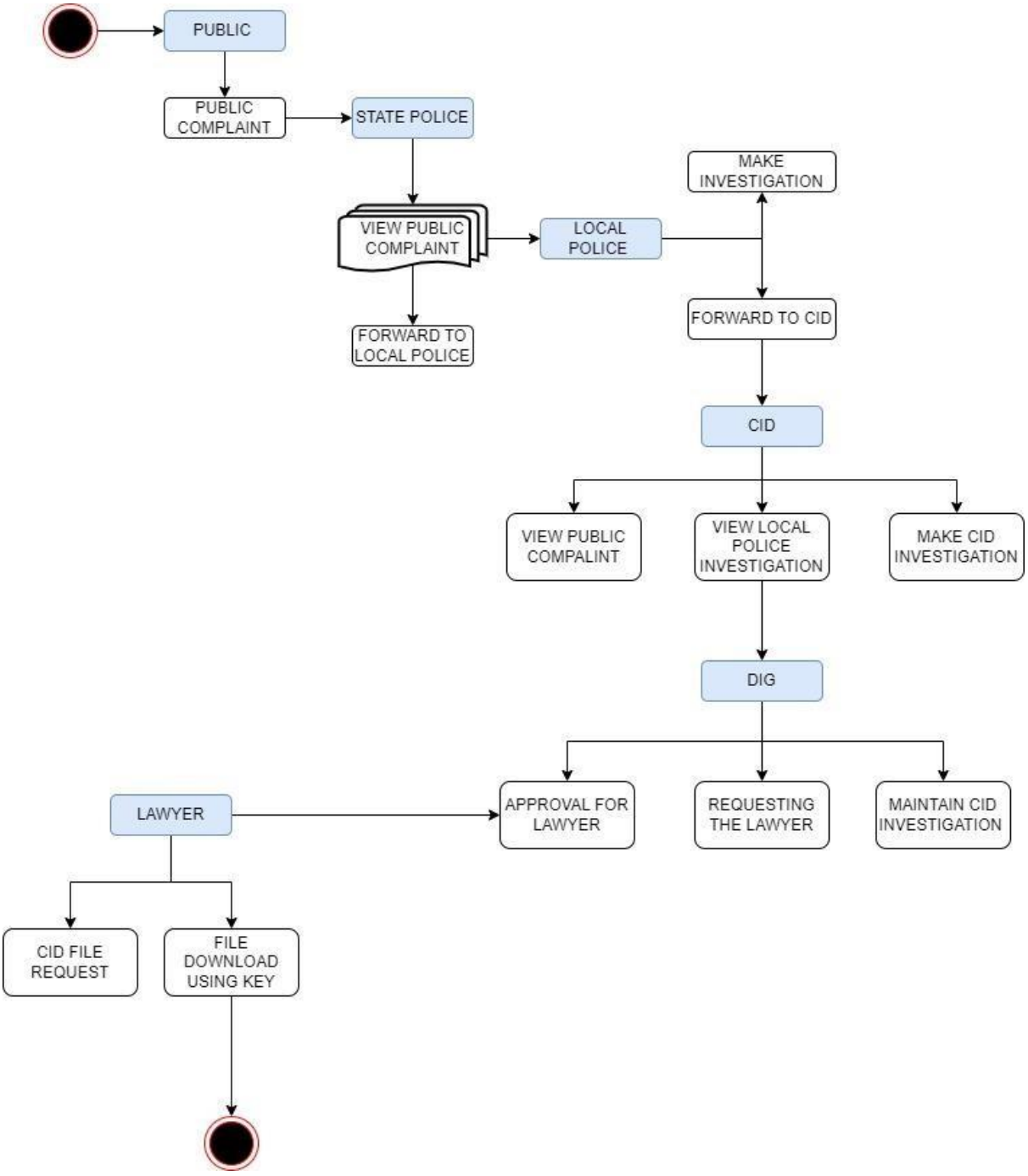
5.2 STATE DIAGRAM:



EXPLANATION:

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. Many forms of state diagrams exist, which differ slightly and have different semantics. We first suggest a data in our state diagram for this in our component diagram for this proposed technique, and then use the Hash-Solomon Code Algorithm to encrypt the data.

5.3 ACTIVITY DIAGRAM:

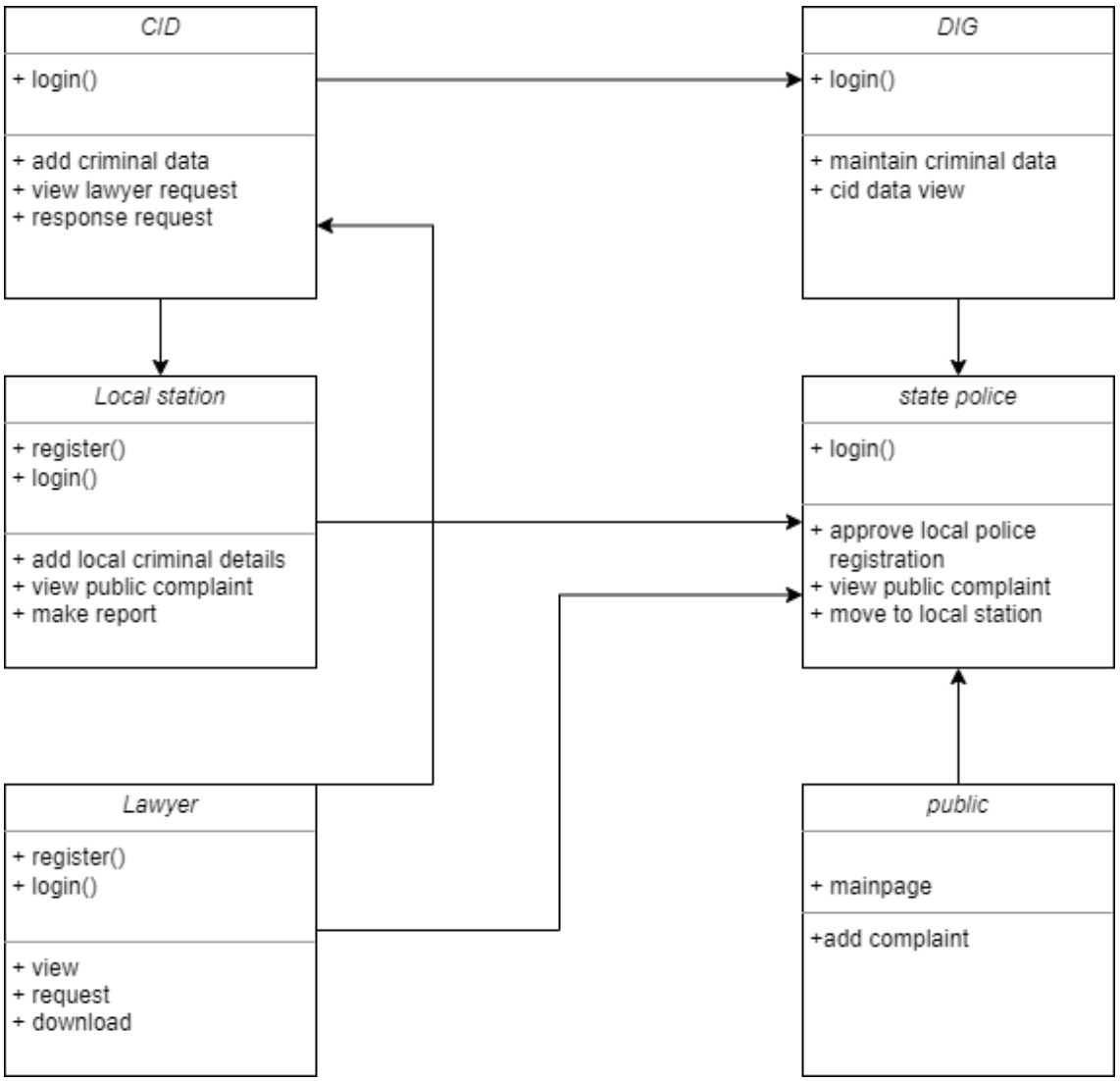


EXPLANATION:

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.

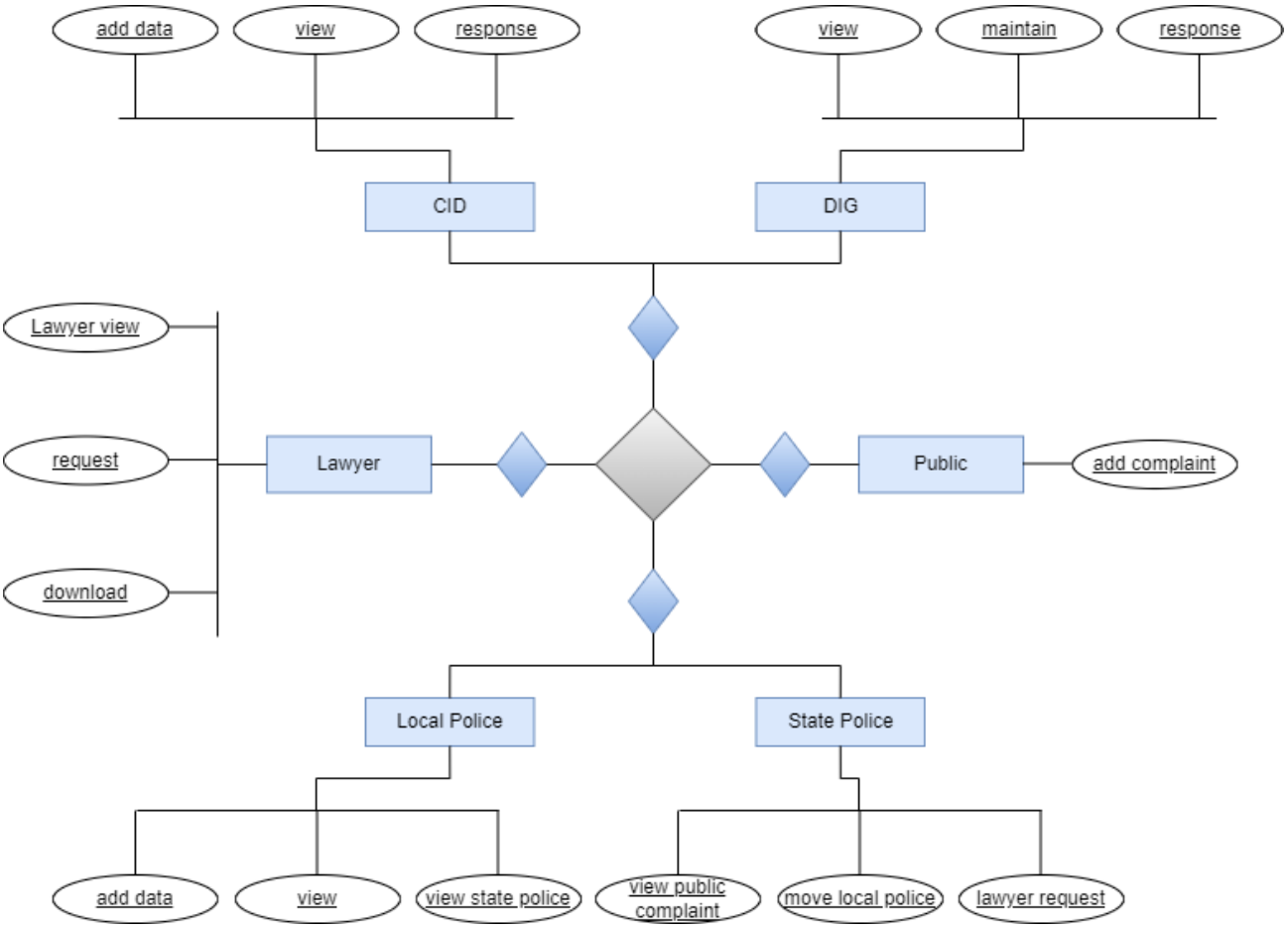
5.4 CLASS DIAGRAM:



EXPLANATION:

Class diagram is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes. The classes in a class diagram represent both the main objects and or interactions in the application and the objects.

5.5 ER DIAGRAM:



EXPLANATION:

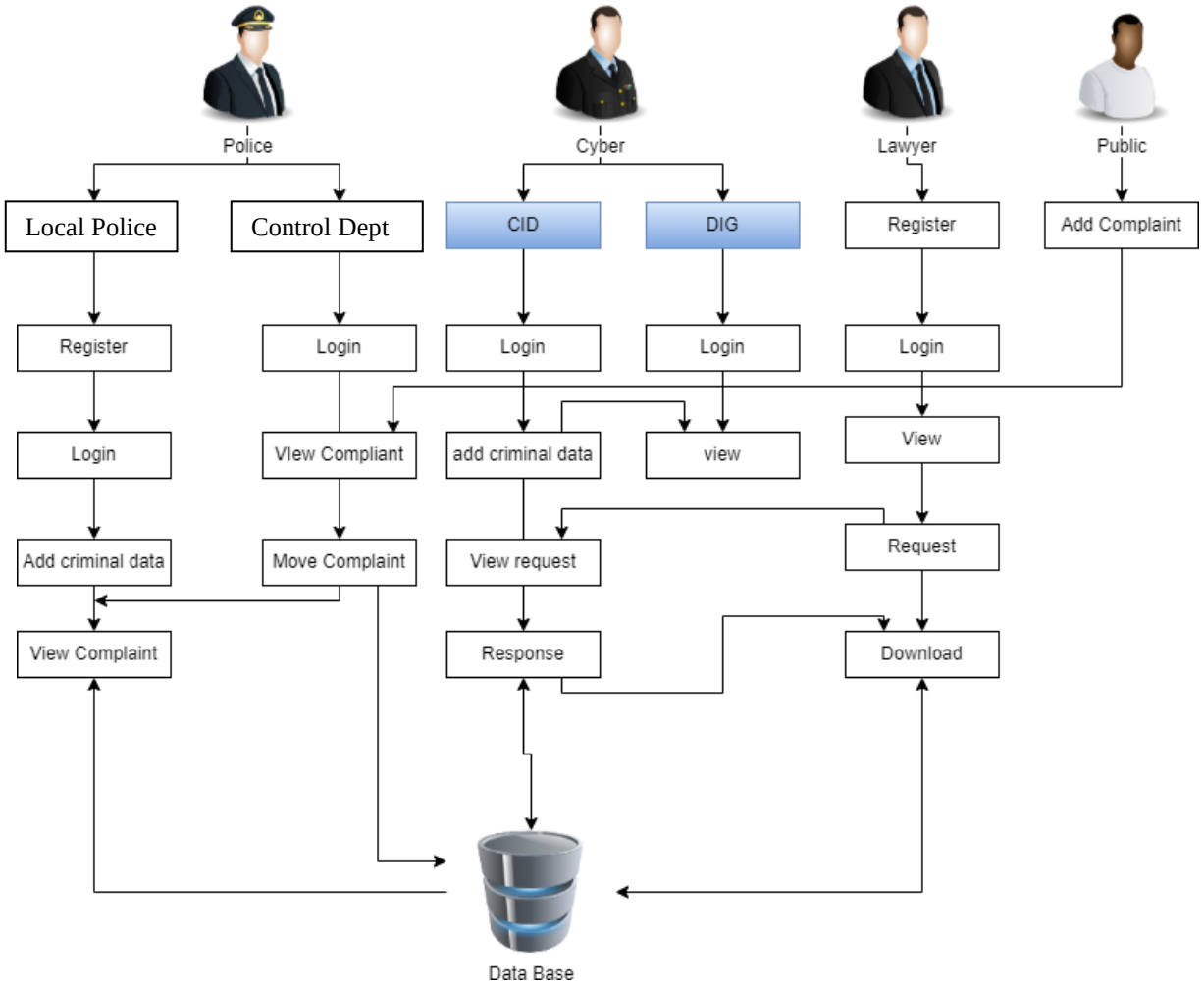
An entity is represented as rectangle in an ER diagram. For example: In the following ER diagram we have two entities Student and College and these two entities have many to one relationship as many students study in a single college. We will read more about relationships later, for now focus on entities.

CHAPTER - 6
SYSTEM ARCHITECTURE

CHAPTER 6: SYSTEM ARCHITECTURE

6.1 ARCHITECTURE OVERVIEW

6.1.1 SYSTEM ARCHITECTURE DIAGRAM:



EXPLANATION:

An architecture diagram is a visual representation of a number of concepts, including the principles, elements, and components, that makes up the architecture. It can also be described as a picture that shows how a software system's component parts will be implemented physically. It displays the relationships, constraints, and boundaries between each piece as well as the overall structure of the software system.

CHAPTER - 7
SYSTEM IMPLEMENTATION

CHAPTER 7: SYSTEM IMPLEMENTATION

7.1 MODULE DESIGN SPECIFICATION

MODULES:

- **REGISTER**
- **LOGIN**
- **PUBLIC ADD COMPLIANT**
- **CONTROL DEPARTMENT ACTIVITIES**
    - APPROVE REGISTRATION
    - VIEW PUBLIC COMPLAINT
    - MOVE TO LOCAL STATION
- **LOCAL POLICE INVESTIGATION**
    - ADD CRIMINAL DATA
    - VIEW CONTROL DEPARTMENT FILES
    - MAKE REPORT

7.1.1 MODULE DESCRIPTION:

REGISTER:

The register module provides a conceptual framework for entering data on those department in a way that: eases data entry & accuracy by matching the department entry to the data source (usually paper files created at point of care) such as local police and lawyer, ties easily back to individual department records to connect registers to department data, and collects data elements to enable better supervision of tender programs.

LOGIN:

In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database each module login to show their page.

PUBLIC ADD COMPLAINT:

In this module in our project, common people make complaint through online. The complaint is directly viewed by the control department.

CONTROL DEPARTMENT ACTIVITIES:

In this module in our project, here describe the Control Department work and techniques,

1. **APPROVE REGISTRATION:**

   In this module in our project, control department need to approve the local police registration for his references. Here the registration is not accepted by the control department, then the local police cannot login. So control department need to accept the registration.

2. **VIEW PUBLIC COMPLAINT:**

   In this module in our project, here the control department view the public complaint.

3. **MOVE TO LOCAL STATION:**

   In this module in our project, here the control department is going to move the people complaint to the local police station is located in same zone area from people complaint.

LOCAL POLICE INVESTIGATION:

In this module in our project, here describe the Local police work and techniques,

1. **ADD CRIMINAL DATA:**

   In this module in our project, here the local police also need to add criminal record in database. It will be view by DIG.

2. **VIEW CONTROL DEPARTMENT FILES:**

   In this module in our project, here the local police view the control department forwarded file for the new investigation.

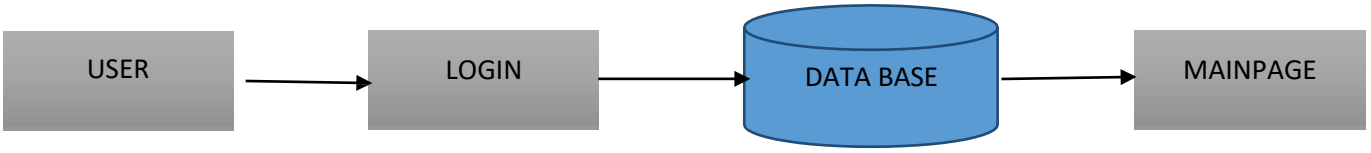
3. **MAKE REPORT:**

   In this module in our project, here local police make the report for every investigation.

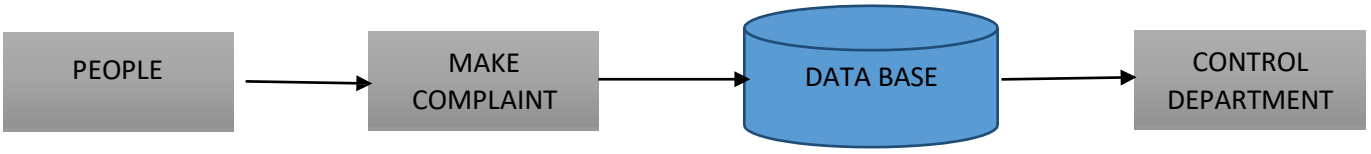
7.1.2 MODULE DIAGRAM:

REGISTER:

LOGIN:

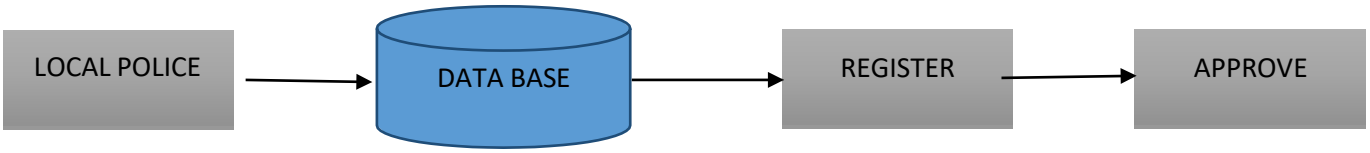


PUBLIC ADD COMPLAINT:

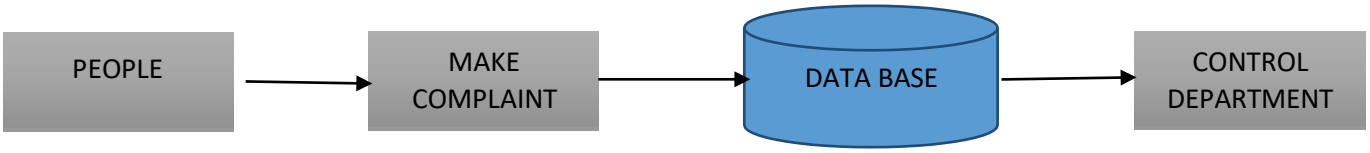


CONTROL DEPARTMENT ACTIVITIES:

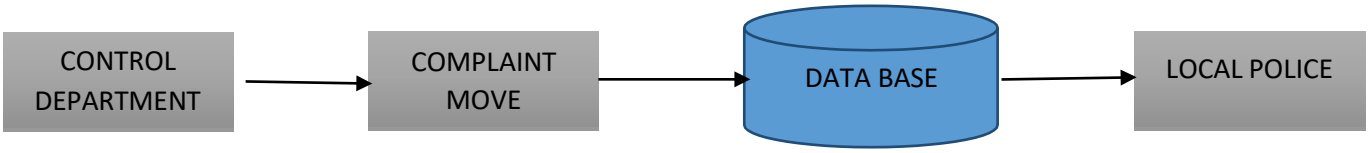
1. APPROVE REGISTRATION:



2. VIEW PUBLIC COMPLAINT:

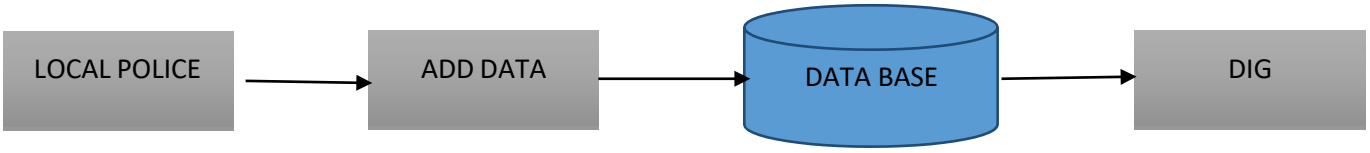


3. MOVE TO LOCAL STATION:

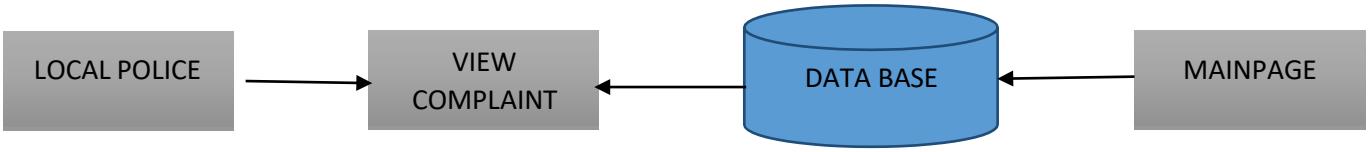


LOCAL POLICE INVESTIGATION:

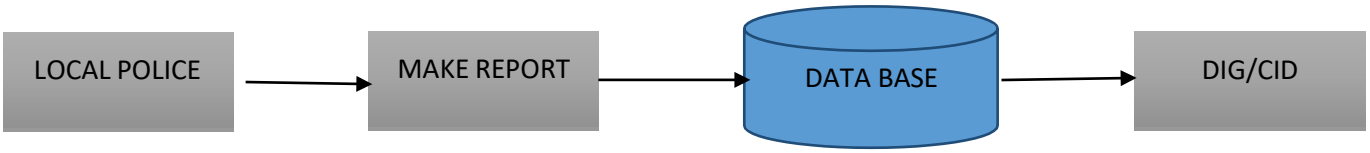
1. ADD CRIMINAL DATA:



2. VIEW CONTROL DEPARTMENT FILES:



3. MAKE REPORT:



7.2 ALGORITHM DESCRIPTION:

1. BLOWFISH ALGORITHM:

Blowfish is a variable-length, symmetric, 64-bit block cipher. Designed by Bruce Schneier in 1993 as a "general-purpose algorithm," it was intended to provide a fast, free, drop-in alternative to the aging Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) encryption algorithms.

Blowfish is significantly faster than DES and IDEA and is unpatented and available free for all uses. However, it couldn't completely replace DES due to its small block size, which is considered insecure.

This algorithm is implemented at the place where the public complaint through the developed web application. The purpose of implementing this algorithm at this place is to encrypt the data that is given by the public.

Blowfish features a 64-bit block size and takes a variable-length key, from 32 bits to 448 bits. It consists of 16 Feistel-like iterations, where each iteration operates on a 64-bit block that's split into two 32-bit words. Blowfish uses a single encryption key to both encrypt and decrypt data.

Blowfish encryption/decryption process example

Assume the message "Hi world" is to be encrypted with Blowfish. The following are the steps involved:

1. Initially, the input "Hi world" consists of seven characters plus one space, which is equal to 64 bits or 8 bytes.
2. The input is split into 32 bits. The left 32 bits -- "Hi w" -- are XORed with P1, which is generated by key expansion to create a value called P1. (**Note:** *P denotes prime number, a number that is not divisible except by 1 and itself.*)
3. Then, P1 runs through a transformative F-function (F In) in which the 32 bits are split into 4 bytes each and passed to the four S-boxes.
4. The first two values from the first two S-boxes are added to each other and XORed with the third value from the third S-box.
5. This result is added to the output of the fourth S-box to produce 32 bits as output.
6. The output of F In is XORed with the right 32 bits of the input message -- "orld" -- to produce output F1'.
7. Then, F1' replaces the left half of the message, while P1' replaces the right half.
8. This same process is repeated for successive members of P-array for 16 rounds in total.
9. Finally, after 16 rounds, the outputs P16' and F16' are XORed with the last two entries of the P-array, i.e., P17 and P18. They are then recombined to produce the 64-bit cipher text of the input message.

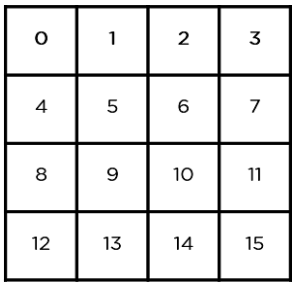
2. AES ALGORITHM:

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the cipher text.

It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).

HOW DOES AES WORK?

To understand the way AES works, you first need to learn how it transmits information between multiple steps. Since a single block is 16 bytes, a 4x4 matrix holds the data in a single block, with each cell holding a single byte of information.

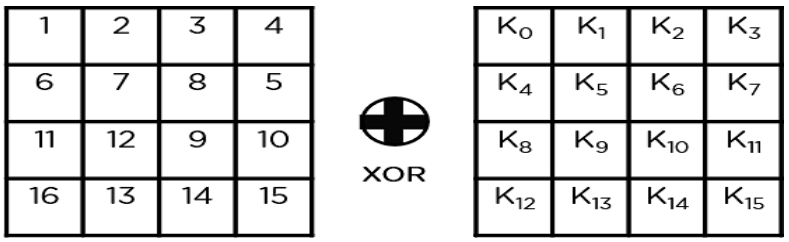


The matrix shown in the image above is known as a state array. Similarly, the key being used initially is expanded into (n+1) keys, with n being the number of rounds to be followed in the encryption process. So for a 128-bit key, the number of rounds is 16, with no. of keys to be generated being 10+1, which is a total of 11 keys.

STEPS TO BE FOLLOWED IN AES

The mentioned steps are to be followed for every block sequentially. Upon successfully encrypting the individual blocks, it joins them together to form the final cipher text. The steps are as follows:

- Add Round Key: You pass the block data stored in the state array through an XOR function with the first key generated (K0). It passes the resultant state array on as input to the next step.

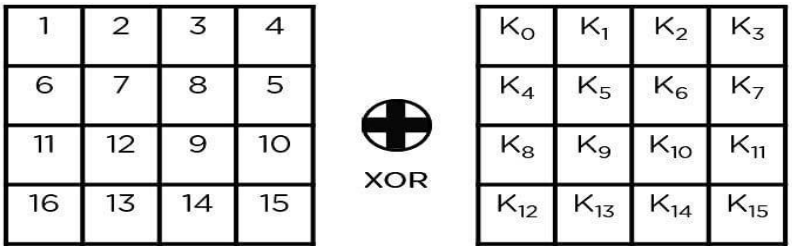


- Sub-Bytes: In this step, it converts each byte of the state array into hexadecimal, divided into two equal parts. These parts are the rows and columns, mapped with a substitution box (S-Box) to generate new values for the final state array.

- Shift Rows: It swaps the row elements among each other. It skips the first row. It shifts the elements in the second row, one position to the left. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.

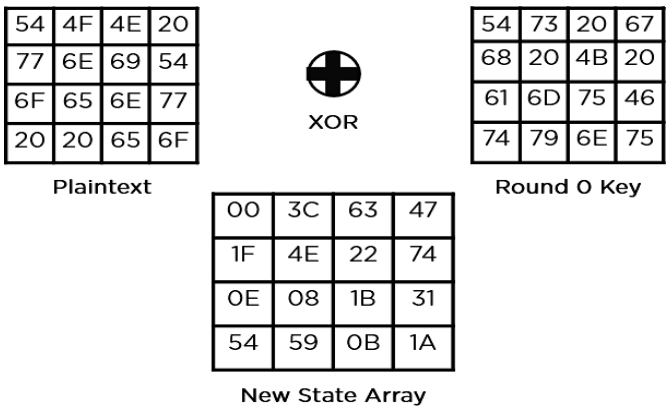
- Mix Columns: It multiplies a constant matrix with each column in the state array to get a new column for the subsequent state array. Once all the columns are multiplied with the same constant matrix, you get your state array for the next step. This particular step is not to be done in the last round.

- Add Round Key: The respective key for the round is XOR'd with the state array is obtained in the previous step. If this is the last round, the resultant state array becomes the ciphertext for the specific block; else, it passes as the new state array input for the next round.

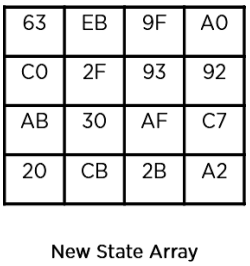


You need to follow the same steps explained above, sequentially extracting the state array and passing it off as input to the next round. The steps are as follows:

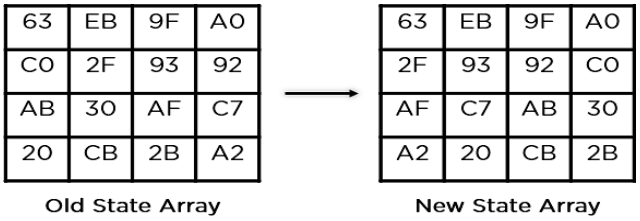
- Add Round Key:



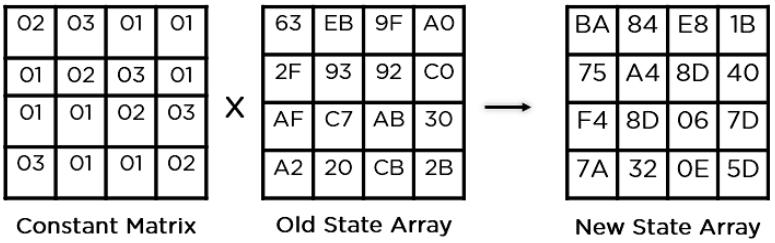
- Sub-Bytes: It passes the elements through a 16x16 S-Box to get a completely new state array.



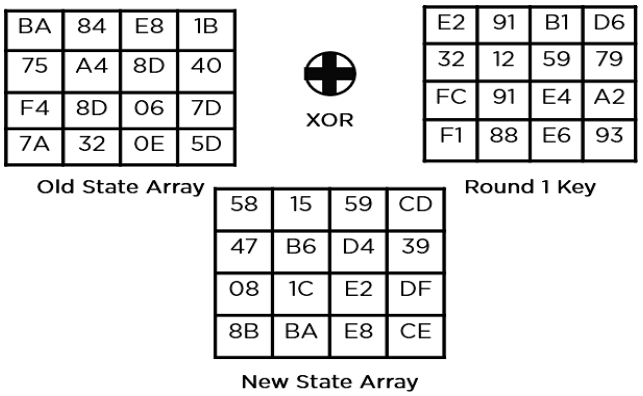
- Shift Rows:



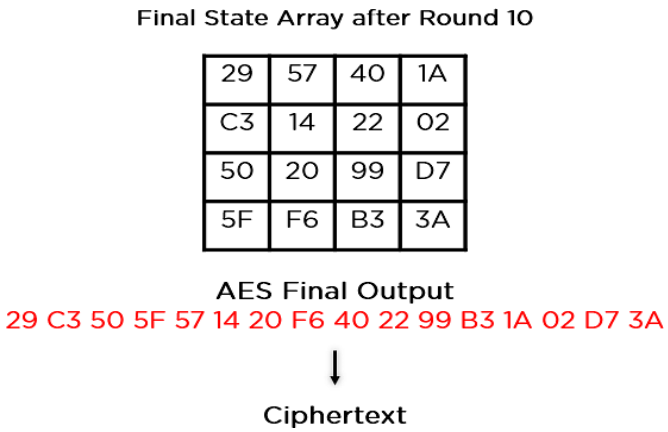
- Mix Columns:



- Add Round Key:



This state array is now the final cipher text for this particular round. This becomes the input for the next round. Depending on the key length, you repeat the above steps until you complete round 10, after which you receive the final cipher text.



CHAPTER - 8
SYSTEM TESTING

8.1 SOFTWARE TESTING

The software, which has been developed, has to be tested to prove its validity. Testing is considered to be the least creative phase of the whole cycle of system design. In the real sense it is the phase, which helps to bring out the creativity of the other phases makes it shine.

8.1.1 UNIT TESTING

Unit testing is a software verification and validation method that tests individual units of source code, sets of one or more computer program modules, and associated control data, usage procedures, and operating procedures. It involves the design of test cases that validate the internal program logic and that program inputs produce valid outputs. It is done after the completion of an individual unit before integration.

8.1.2 FUNCTIONAL TESTING

Functional testing is a type of software testing whereby the system is tested against the functional requirements specifications. Functions or features are tested by feeding them input and examining the output. Functional testing ensures that the requirements are properly satisfied by the application. This type of testing is not concerned with how processing occurs but rather with the results of processing. During functional testing, Black box testing technique is used in which the internal logic of the system being tested is not known to the tester. Functional testing is normally performed during the levels of system testing and acceptance testing. Typically, it involves the following steps:

• Identify functions that the software is expected to perform.

• Create input data based on the function’s specification.

• Determine the output based on the function’s specification.

8.1.3 PERFORMANCE TESTING

Generally speaking, testing is done to find out how a system responds and remains stable under a specific load. Additionally, it can be used to look into, gauge, confirm, or evaluate other system quality characteristics like scalability, dependability, and resource utilisation. Performance engineering is a growing field in computer science that aims to incorporate performance into system implementation, design, and architecture. Performance testing is a subset of performance engineering.

8.1.4 INTEGRATION TESTING

Integration testing is a systematic technique for constructing the program structure while conducting tests to uncover errors associated with individual modules. It takes input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers the integrated system ready. The purpose of integration testing is to verify functional, performance, and reliability requirements placed on major design items. Test cases are constructed to test whether all components within assemblages interact correctly.

8.1.5 SYSTEM TESTING

System testing of software or hardware is a black box testing that evaluates the system's compliance with its specified requirements. It is performed on the entire system in the context of a Functional Requirement Specification(s) and/or a System Requirement Specification(s). It tests not only the design, but also the behaviour and customer expectations.

8.1.6 OUTPUT TESTING

After performing the validation testing, next step is output testing of the proposed system since no system could be useful if it does not produce the

required output generated or considered in to two ways. One is on screen and another is printed format. The output comes as the specified requirements by the user. Hence output testing does not result in any correction in the system.

8.1.7 USER ACCEPTANCE TESTING

User acceptance of a system is the factor for the success of any system. The system under consideration is tested for the user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required.

• Input screen design.

• Output screen design.

• Online message to guide user.

• Format of the ad-hoc reports and other outputs.

8.2 TEST CASE REPORTS

TEST REPORT : 01

PRODUCT : Cyber forensic investigation

USECASE : Add Complaint

TEST CASE ID	**TEST CASE/ ACTION TO BE PERFORMED**	**EXPECTED RESULT**	**ACTUAL RESULT**	**PASS/FAIL**
1	Complaint cannot be raised until the mandatory fields are filled	Please fill out the field	As expected	PASS
2	Complaint must be filed properly after clicking on complaint button	Complaint raised page must appear	As expected	PASS

3	Complaint given by public	Complaint encrypted and stored	As expected	PASS
4	Complaint ID must be unique	Complaint ID must be changed after each refresh	As expected	PASS

Table-8.2.1 Test Case For Adding Complaint

TEST REPORT : 02

PRODUCT **:** Cyber forensic investigation

USECASE **:** Control Department

TEST CASEID	**TEST CASE/ ACTION TO BE PERFORMED**	**EXPECTED RESULT**	**ACTUAL RESULT**	**PASS/FAIL**
1	Complaint goes to control department	Control department must be able to view the complaint	As expected	PASS
2	Correct username and password must be given to access the complaint raised	Control department able to login	As expected	PASS
3	Activation of the complaint by the control department	Respected local stations must be allocated based on the area mentioned in the complaint filed	As expected	PASS

Table-8.2.2 Test Case For Control Department

TEST REPORT : 03

PRODUCT **:** Cyber forensic investigation

USECASE **:** Local police

TEST CASE ID	**TEST CASE/ ACTION TO BE PERFORMED**	**EXPECTED RESULT**	**ACTUAL RESULT**	**PASS/FAIL**
1	Local station view the complaint	Only the allocated local stations can view the complaint	As expected	PASS
2	Police adding acquist details	Added details must be encrypted and saved properly	As expected	PASS

Table-8.2.3 Test Case For Local Police

TEST REPORT : 04

PRODUCT **:** Cyber forensic investigation

USECASE **:** DIG

TEST CASE ID	**TESTCASE/ ACTION TO BE PERFORMED**	**EXPECTED RESULT**	**ACTUAL RESULT**	**PASS/FAIL**
1	Gives access to the lawyer to download the investigation report	Ability to give the access	As expected	PASS

Table-8.2.4 Test Case For DIG

CHAPTER - 9
CONCLUSION

CHAPTER 9: CONCLUSION

9.1 CONCLUSION:

Digital forensics involves the process of identifying, collecting, acquiring, and preserving. Analysing, and presenting of digital evidence. Digital evidence must be authenticated to ensure its admissibility in a court of law. Ultimately, the forensic artefacts and forensic methods used to static or live acquisition depend on the cases and its section. Real evidence must be competent (authenticated), relevant, and material. This software is developed with modular approach. All modules in this system have been tested with valid data and everything worked successfully.

9.2 FUTURE ENHANCEMENTS:

Upcoming project have designed the model with double expert or administrator to check and give the suggestion to the public with the authorization services. One phase will be implemented under various complaint sectors such as murder and kidnap, robbery etc. Another phase cybercrime report will be added.

APPENDICES:

A.1 SAMPLE CODING:

MAIN PAGE:

```
<%@ 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>Insert title here</title>
</head>
<style>
* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Abel", sans-serif;
font-size: 10px;
scroll-behavior: smooth;
}
.wrapper {
width: auto;
height: 100vh;
background-image: url("image/6.jfif");
background-position: center;
background-size: cover;
```

```
background-repeat: no-repeat;
backdrop-filter: opacity(80%);
}
.Container {
width: 100%;
height: 100%;
display: flex;
justify-content: center;
align-items: center;
}
.nav  {
position: fixed;
top: 0;
left: 0;
width: 100%;
height: 80px;
border-bottom: 1px solid rgba(255, 255, 255, 0.521);
display: flex;
justify-content: space-between;
align-items: center;
padding: 0 50px;
}
.logo {
font-family: "Abel", sans-serif;
font-size: 2.5rem;
font-weight: 600;
letter-spacing: 0.7rem;
```

```
color: white;
margin: 4%;
}
.menu {
display: inline-block;
line-height: 80px;
}
.menu ul {
list-style: none;
  /* display: flex;
flex-direction: row;
justify-content: center;
align-items: center; */
}
.menu ul li {
display: inline-block;
}
.menu ul li a {
text-decoration: none;
font-family: "Raleway", sans-serif;
font-size: 1.2rem;
font-weight: 600;
letter-spacing: 0.1rem;
color: white;
border: 1px solid transparent;
border-radius: 4px;
padding: 10px 15px;
```

```
margin: 0 5px;
transition: 0.5s ease;
}
.menu ul li a:hover {
border-color: white;
}
.menu ulli:nth-child(5) a {
color: #fff200;
border: 1px solid #fff200;
}
.menu ulli:nth-child(5) a:hover {
color: black;
background-color: #fff200;
}
.header {
text-align: center;
}
.header h1 {
font-family: "Raleway", sans-serif;
font-size: 4rem;
font-weight: 600;
letter-spacing: 0.2rem;
color: white;
padding: 45% 20px 8px;
}
.header p {
font-family: "Raleway", sans-serif;
```

```
font-size: 1.5rem;
font-weight: 600;
letter-spacing: 0.2rem;
color: white;
padding: 10px 15px;
}
button {
font-size: 1.5rem;
font-weight: 600;
letter-spacing: 0.15rem;
color: black;
background-color: #fff200;
padding: 20px 30px;
margin: 50px 5px 0;
border: none;
cursor: pointer;
}
</style>
<body>
<div class="wrapper">
<div class="Container">
<div class="nav">
<div class="logo">
</div>
<div class="menu">
<ul class="navMenu">
<li><a href="#">Home</a></li>
```

```
<li><a href="lawerlog.jsp">Lawer</a></li>
<li><a href="police.jsp">Police</a></li>
<li><a href="pubcomplaint.jsp">Public complaint</a></li>
<li><a href="cyberlog.jsp">cyber</a></li>
</ul>
</div>
</div>
<div class="header">
<h1>Cyber</h1>
</div>
</div>
</div>
</body>
</html>
```

VIEW PAGE:

```
<%@ 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">
<%@page import=" Dbcon.dbcon"%>
<%@page import="java.sql.ResultSet"%>
<%@page import="java.sql.PreparedStatement" %>
<%@page import="java.sql.*" %>
<%@page import="java.util.*" %>

<html>
<head>
```

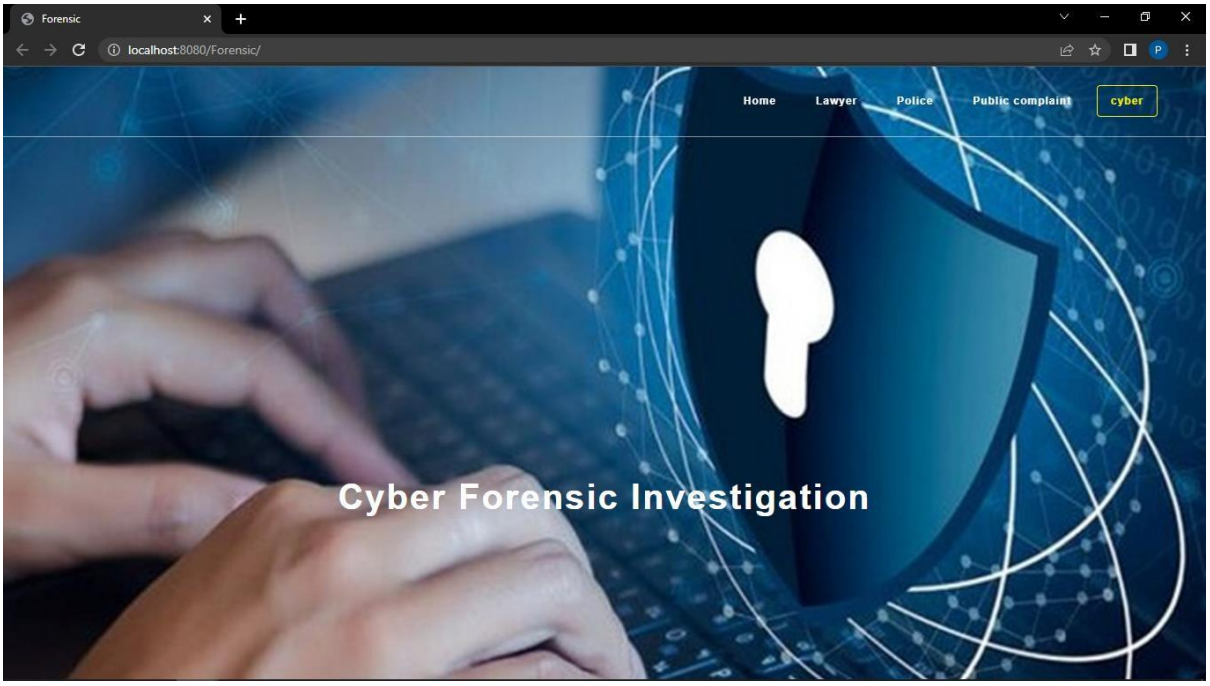
```
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
<link href="css/style.css" rel="stylesheet" type="text/css" media="all" />
<link href="css1/bootstrap.min.css.map" rel="stylesheet" type="text/css" media="all" />
<script src="text/javascript" src='js/jquery-3.6.0.min.js'></script>
<script src="text/javascript" src='js/bootstrap.min.js'></script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="css/font-awesome.min1.css">
</head>
<style>
body{
background-color:#9fa9bb;
}
table, td, th {
border: 1px solid black;
}
table {
border-collapse: collapse;
width: 70%;
margin-rigth: 70px;
}
td{
text-align: center;
padding-top: 1.0em;
padding-bottom: 1.0em;
}
```

```
th{
border: 3px solid black;
}
</style>
<body>
<% String pcid=session.getAttribute("pcids").toString(); %>
<center>
<div class="container-fluid">
<table class="table-dark">
<thead>
<tr>
<th scope="col">NAME</th>
<th   scope="col">Case.no</th>
<th   scope="col">Address</th>
<th scope="col">ZONE</th>
<th scope="col">City</th>
<th   scope="col">MOBILE</th>
<th   scope="col">STATUS</th>
</tr>
</thead>
<%

     Connection con;
con=dbcon.create();
PreparedStatementps=con.prepareStatement("SELECT * FROM
`forensic`.`publiccomplaint` where status='Investigated' ");
ResultSetrs=ps.executeQuery();
```

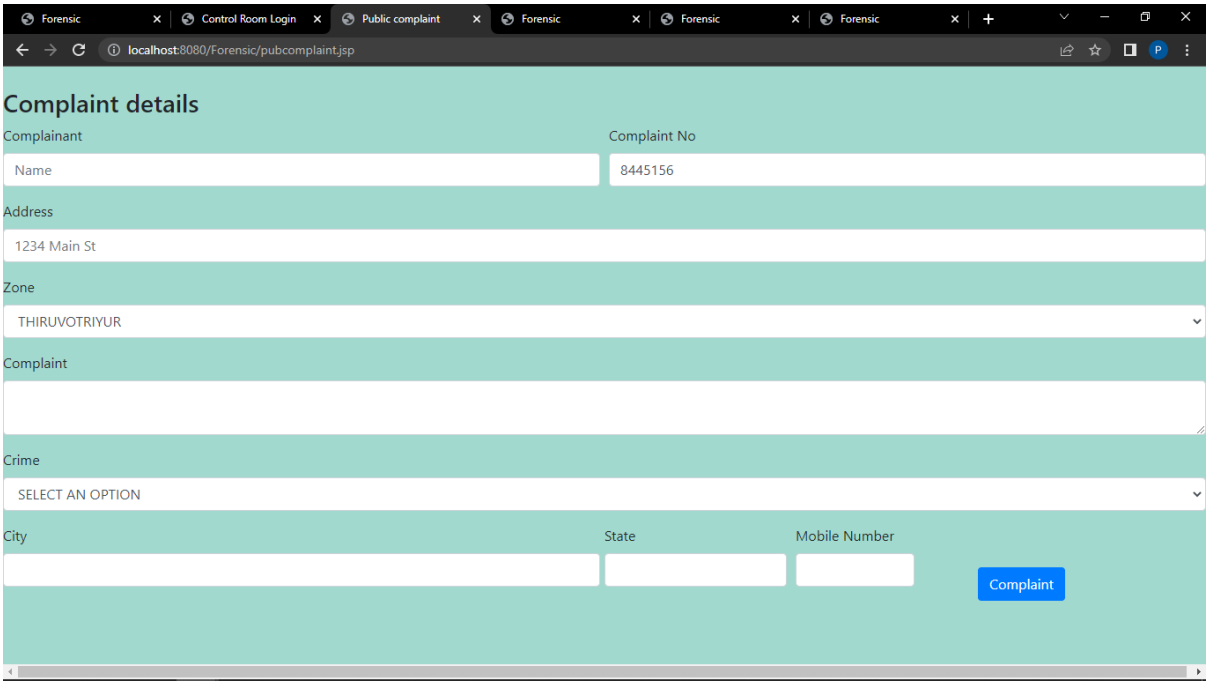
```
while(rs.next())
      {
          String email=rs.getString(2);
         String cname=  rs.getString(1);


      %>
<tr>
<td style="text-align: center;"><%=rs.getString(1)%></td>
<td style="text-align: center;"><%= rs.getString(2) %></td>
<td style="text-align: center;"><%=  rs.getString(3) %></td>
<td style="text-align: center;"><%=  rs.getString(4) %></td>
<td style="text-align: center;"><%=  rs.getString(5) %></td>
<td style="text-align: center;"><%=  rs.getString(7) %></td>
<td><a
href="compliantinvestigate.jsp?id=<%=rs.getString(2)%>&&cname=<%=rs.get
String(1)%>"><button class="btnbtn-primary">Investigate </button></a></td>
</tr>
        <%} %>
</table>
</div>
</center>
</body>
</html>
```

A.2 SAMPLE SCREENSHOTS:

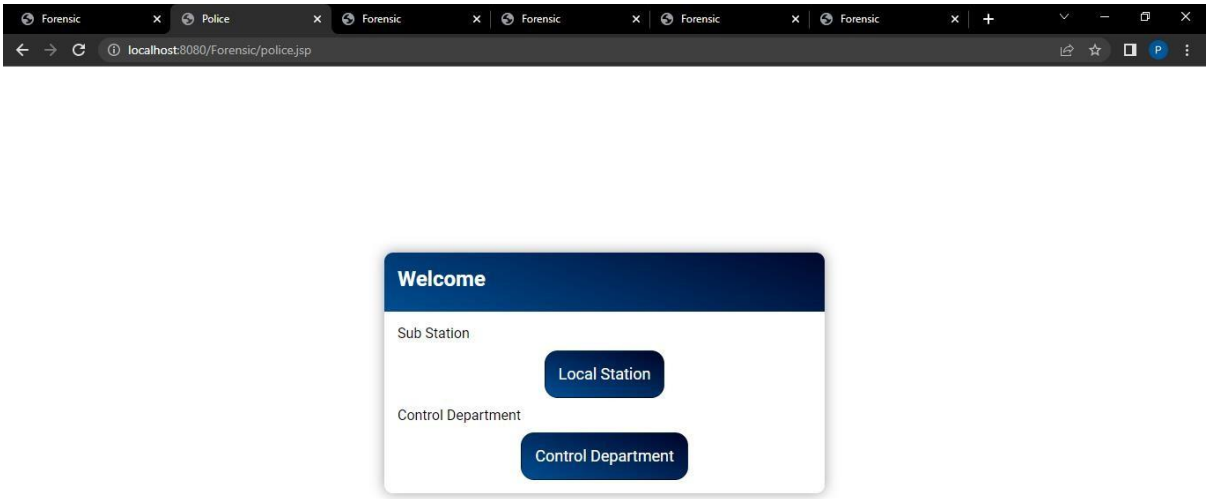
A.2.1 Home Page:



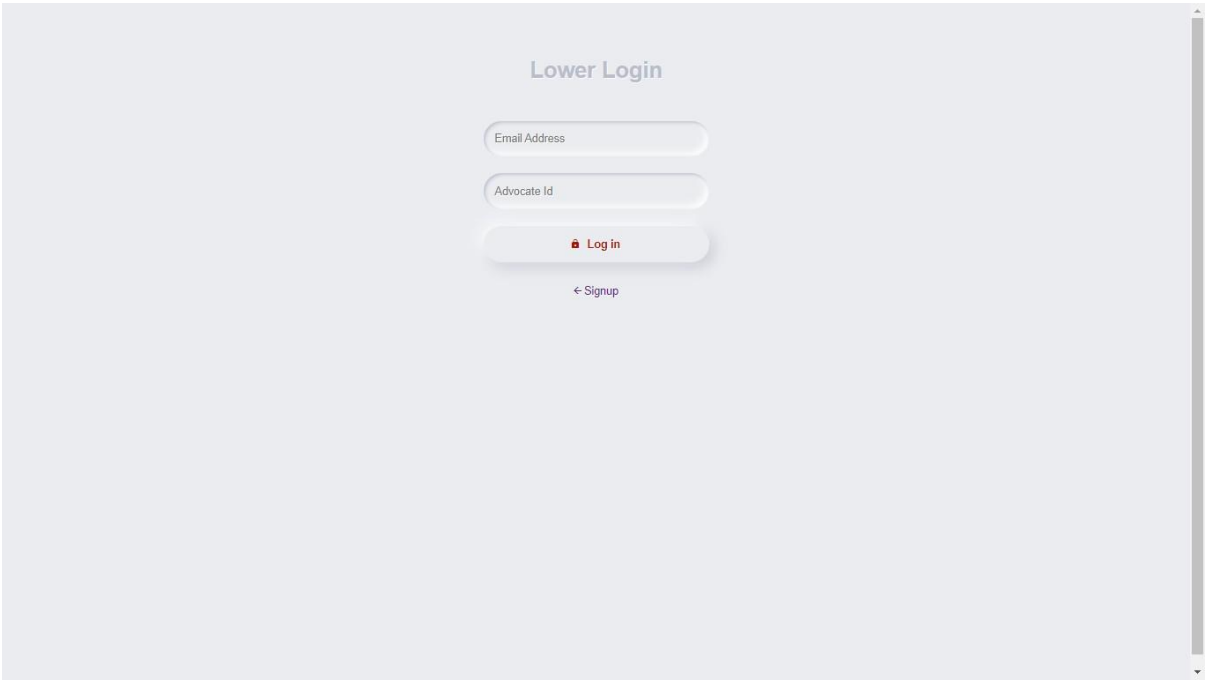
A.2.2 Public Complaint Page:



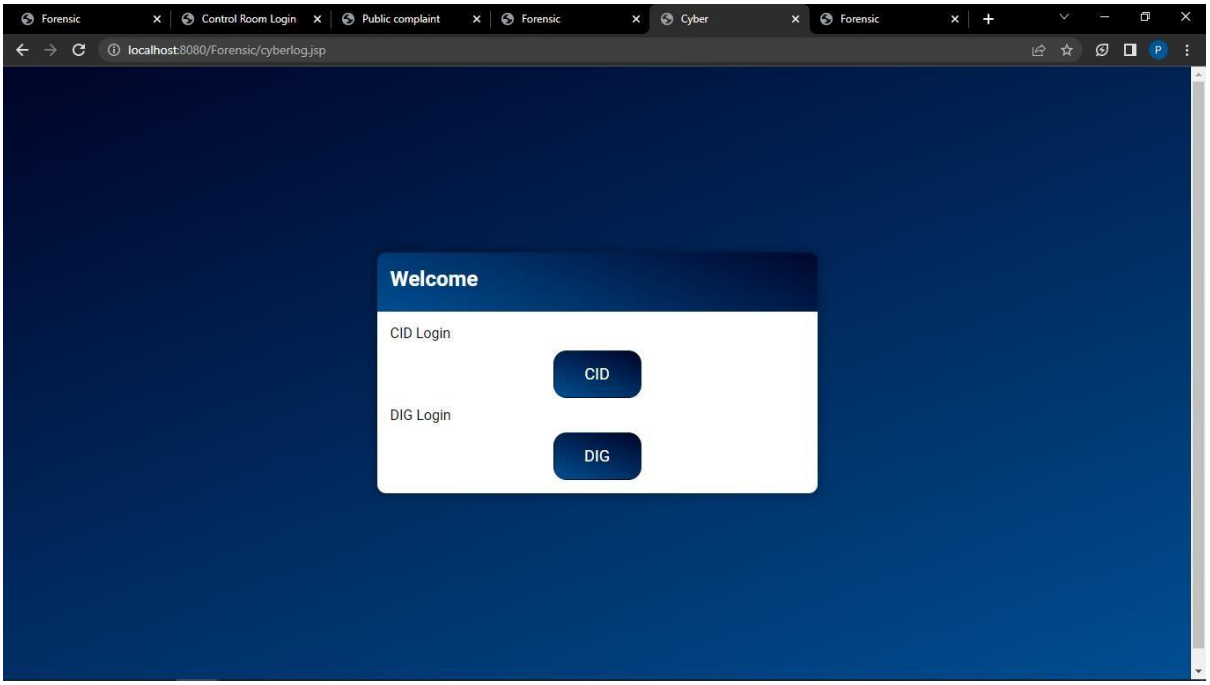
A.2.3 Police Log Selection Page:



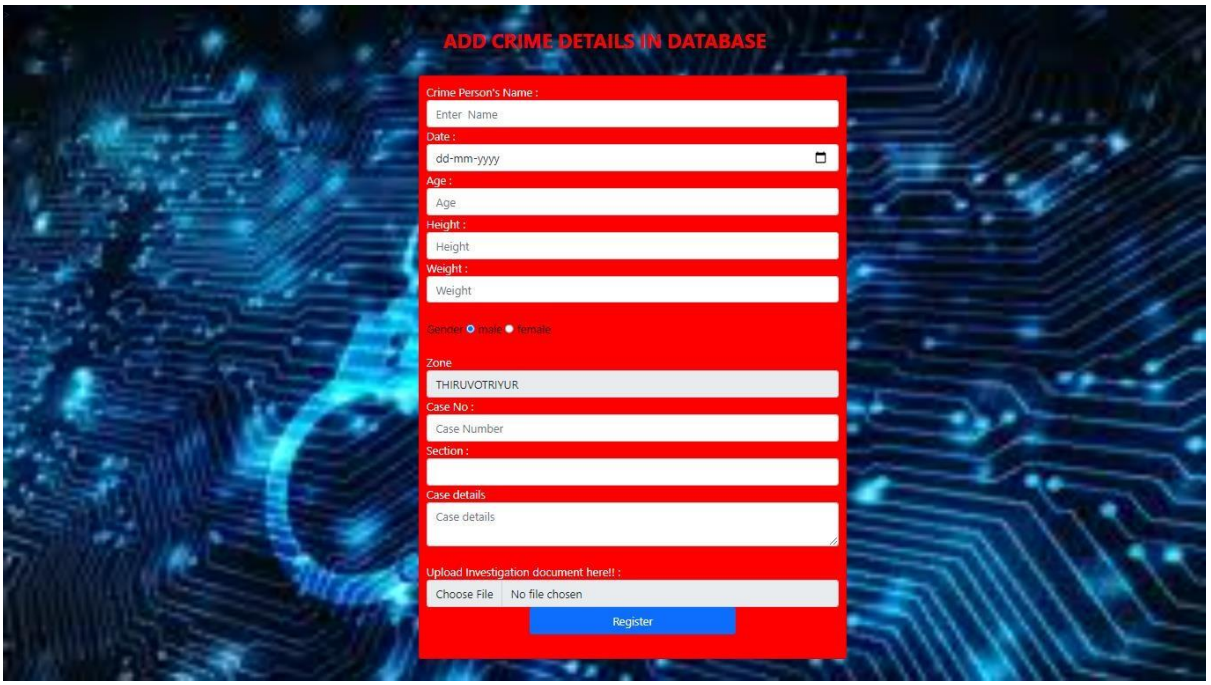
A.2.4 Lawyer Login Page:



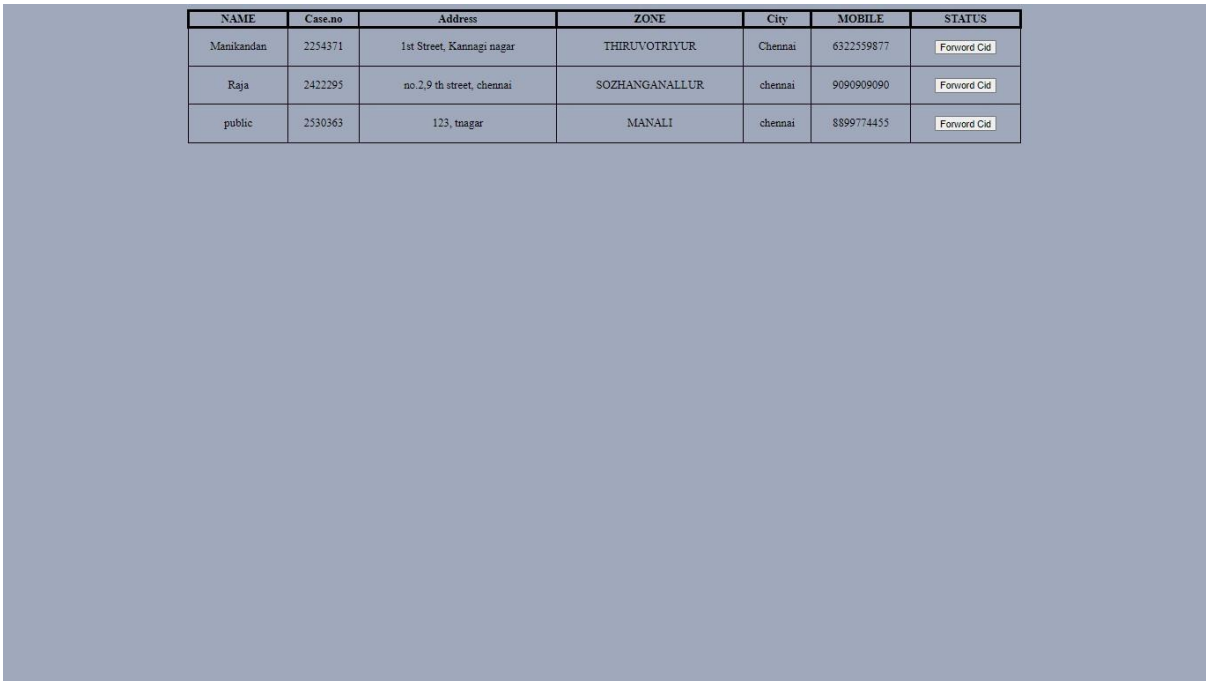
A.2.5 Cyber Log Selection Page:



A.2.6 Add Crime Details Page:



A.2.7 View Investigation Page:



NAME	Case.no	Address	ZONE	City	MOBILE	STATUS
Manikandan	2254371	1st Street, Kannagi nagar	THIRUVOTRIYUR	Chennai	6322559877	Forword Cid
Raja	2422295	no.2,9 th street, chennai	SOZHANGANALLUR	chennai	9090909090	Forword Cid
public	2530363	123, tnagar	MANALI	chennai	8899774455	Forword Cid

A.2.8 DIG Case View Page:

back

Date	Name	Age	Height	Weight	Gender	Zone	Case Number	Section	Case Details
2022-01-04	aa	24	6"ft	60 kg	male	THIRUVOTRIYUR	111	section 302	murder
2022-01-04	Admin	24	6"ft	60 kg	male	THIRUVOTRIYUR	111	section 302	murder
2021-12-30	vicky	24	6"ft	60 kg	male	SOZHANGANALLUR	111	section 302	more than billion child in kills every days
2022-01-02	bilal	24	5.50"ft	40	male	ADYAR	112	section 420	pycho rapist want criminal
2022-01-04	raja	26	5.30	70 kg	male	SOZHANGANALLUR	113	section 378	young girls heart Hacker (like a playboy)
2022-01-07	Raja , Thalapthi	45,26	5.30,5.50	40,50	male	SOZHANGANALLUR	12a235	section 378	thief
2022-01-07	Paul	24	5.30	60kg	male	ROYAPURAM	case123	section 378	Kill some Grandma
2022-01-07	Justus	25	5.10	55kg	male	KODAMBAKKAM	case101	section 372	Rapist
2022-01-29	Sampath	38	5.5	60	male	KODAMBAKKAM	case 103	section 372	Most wanted Acquist
2022-01-29	Barathi	28	5.30	50	female	KODAMBAKKAM	case104	section 511 IPC	Cheating So many members
2022-01-29	XXXX	25	6	65	male	MANALI	114	section 420	Chain snathching

REFERENCES:

[1] Antonia Nisioti; George Loukas; Aron Laszka; Emmanouil Panaousis, “Data-Driven Decision Support for Optimizing Cyber Forensic Investigations”, IEEE, January 2021

[2] Seonghyeon Gong; Changhoon Lee, “Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform”, Seoul National University of Science and Technology, vol. 10, January 2021

[3] Antonia Nisioti, George Loukas, Stefan Rass, Emmanouil Panaousis, “Game Theoretic Decision Support for Cyber Forensic Investigation”, University of Greenwich, London, UK, vol. 21, August 2021

[4] Zhun Zhang; Qihe Liu; Shilin Qiu; Shijie Zhou; Cheng Zhang, “Unknown Attack Detection Based on Zero-Shot Learning”, IEEE, vol. 8, October 2020

[5] K. Finnerty, S. Fullick, H. Motha, J. N. Shah, M. Button, and V. Wang, “Cyber security breaches survey 2019,” Dept. Digit., Media Sport, London, U.K., Tech. Rep., Apr. 2019

[6] Cost of a Data Breach Report 2019, IBM Security, New York, NY, USA, 2019

[7] V. Diaz, D. Emm, and C. Raiu, “Kaspersky security bulletin 2019: Advanced threat predictions for 2020,” Kaspersky Lab., Moscow, Russia, Tech. Rep., 2019

[8] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, and V. Venkatakrish-nan, “Holmes: real-time APT detection through correlation of suspicious information flows,” IEEE, 2019

[9] G. Horsman, “Formalising investigative decision making in digital forensics: Proposing the digital evidence reporting and decision support(DERDS) framework,” Digital Investigation, vol. 28, 2019

[10] S. Soltani and S. A. H. Seno, “A formal model for event reconstructionin digital forensic investigation,” Digital Investigation, vol. 30, 2019

[11] J. Navarro, A. Deruyver, and P. Parrend, “A systematic survey on multistep attack detection,” Comput.Secur., vol. 76, pp. 214–249, Jul. 2018

[12] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, “A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later,” Mar. 2016

[13] R. I. de Braekt, N.-A. Le-Khac, J. Farina, M. Scanlon, and T. Kechadi,“Increasing digital investigator availability through efficient workflow management and automation”, IEEE, 2016

[14] Rabail Shafique Satti and Fakeeha Jafari, “Domain Specific Cyber Forensic Investigation Process Model”, Journal of Advances in Computer Network, vol. 3, March 2015

[15] L. Martin. (2014). Cyber Kill Chain.[Online]. Available: http://cyber. lockheedmartin.com/hubfs/GainingAdvantageCyberKillChain.pdf

[16] J.Williams, “Acpo good practice guide for digital evidence,” Metrop. Police Service, Assoc. Chief Police Officers, GB, London, U.K., Tech. Rep., Mar. 2012

[17] Humaira Arshad, Saima Abdullah, Moatsum Alawida Abdulatif, “A Multi-layer Semantic Approach for Digital Forensics Automation for Online Social Networks”, February 2012

[18] S. Barnum, “Standardizing cyber threat intelligence information with the structured threat information expression (STIX),” Mitre Corp., vol. 11, pp. 1–22, Jan. 2012

[19] L. F. da Cruz Nassif and E. R. Hruschka, “Document clustering for forensic analysis: An approach for improving computer inspection,”IEEE transactions on information forensics and security, vol. 8, 2012

[20] S. Alharbi, J. Weber-Jahnke, and I. Traore, “The proactive and reactive digital forensics investigation process: A systematic literature review,” in Proc. Int. Conf. Berlin, Germany: Springer, October 2011

[21] S. Rekhis and N. Boudriga, “A system for formal digital forensic investigation aware of anti-forensic attacks,” IEEE transactions on information forensics and security, vol. 7, 2011

[22] S. Saad and I. Traore, “Method ontology for intelligent network forensicsanalysis,” in 2010 Eighth International Conference on Privacy, Securityand Trust. IEEE, 2010

[23] SunHo Cho, Hyuk-Chul Kwon, “Cyber Forensics Ontology for Cyber Criminal Investigation” Digit. Invest., vol. 3, January 2009

[24] A. Brinson, A. Robinson, and M. Rogers, “A cyber forensics ontology: Creating a new approach to studying cyber forensics,” Digit. Invest., vol. 3, pp. 37–43, Sep. 2006

[25] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” NIST Special Publication, vol. 10, no. 14, pp. 800–886, 2006