International Journal of Innovative Research in Engineering
Volume 4, Issue 3(May-June 2023), PP: 435-445.
www.theijire.com ***ISSN No: 2582-8746***

Data-Driven Decision Support For Optimizing Cyber Forensic Investigations

Poorna Chandar V
Dr. M.G.R. Educational and Research Institute, MGR University, Tamilnadu, India.

How to cite this paper:
Poorna Chandar V, "Data-Driven Decision Support For Optimizing Cyber Forensic Investigations", IJIRE-V4I03-435-445.

Abstract: *The venture known as "Data-Driven Decision Support for Optimizing Cyber Forensic Investigations" is a web based application. This software provides facility for confirming criminal offenses, Problems, losing individuals to DIG. This software provide facility for reporting online crimes, online complaints, missing persons show criminal list and details on web page. Any number of 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 analysing the investigation report, process will be optimized to reduce the investigation process.*

I.INTRODUCTION

Modern science and technology has revolutionised 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. When creating a new case file the system will be able to store specific information in categories. 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.

EXISTING SYSTEM	**PROPOSED SYSTEM**
Concept: Benefits from a repository of known adversarial tactics, techniques, and procedures, for each of which it harvests threat intelligence information to calculate its probabilistic relations with the rest.	**Concept:** Data will be analyzed to optimize the process. From the report, analysis process provide the decision making solution.
Technique: Disclose framework	**Technique:** AES Algorithm
Disadvantage: It has limited functionalities to derive the optimized result.	**Advantage:** It will be efficient to data driven process.

1.2.Literature Survey

Title: Cyber Threat Intelligence – Issue and Challenges
AUTHOR NAME: S. Siti Rahayu, Md Sahrom Abu, Dr Aswami Ariffin (DrAA);
Year: Mar 18, 2018

Explanation:

The threat landscape is rapidly evolving today and many organizations are constantly exposed to sophisticated and devastating cyber threats. Cybercriminals are more sophisticated and well-funded than ever before. Cyber threat intelligence (CTI) has become a hot topic and is being considered by many organizations to counter the increasing number of cyber attacks. The purpose of this paper is to review research related to CTI. Through the literature review process, comparing existing definitions to find common ground or disagreement is the ultimate question about what CTI examines. It was found that organizations and vendors do not fully understand what information is considered CTI, so more research is needed to define CTI. This article also identifies CTI's current products and services, including threat data feeds, threat intelligence standards, and tools used by CTI.

There is a special industry effort to share only critical threat information, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), which collaborates on critical security threats faced by the global financial services industry. Research and development centers such as MITRE are working on developing standard formats (eg STIX, TAXII, CybOX) for sharing threat messages to solve interoperability issues among peers sharing threats. Based on a review of CTI definitions, standards, and tools, this paper identifies four research challenges in cyber threat intelligence and analyzes the state-of-the-art work done on each. With organizations inundated with multiple threats, the demand for skilled threat intelligence analysts to leverage CTI and transform data into actionable intelligence is more important than ever. Data quality is not a new issue, but with the development of CTI, more research is needed in this area

Title: Unknown Attack Detection Based on Zero-Shot Learning
Author Name: ZHUN ZHANG, QIHE LIU.
Year: November 4, 2020.

Explanation:

In recent years, as network intrusions become more frequent, more researchers have begun to focus on network intrusion detection. However, unknown attacks are still difficult to detect. Currently, there are two main ways to detect unknown attacks: clustering and scoring. But there are still unsolved problems such as the difficulty in collecting samples of unknown attacks and the lack of timely detection. Zero-Shot training, which can recognize unknown attacks by learning the mapping relationship between this space and semantics, is proposed to solve this problem in this paper. space (like attribute space). Given the semantic description of all attacks (including known and unknown attacks), classi_erbuilt with Zero-Shot training can extract common semantic information between all attacks and the relationship between known and unknown attacks. The classifier then applies the classification to the unknown attack, even if there are no examples for the unknown attack. In this paper, we first propose the use of Zero-Shot learning to overcome the unknown attack detection problem and demonstrate the potential of this method. Second, we propose a novel Zero-Shot training method based on sparseautoencoder for unknown attack detection. This method maps known attack features into semantic space and remaps semantic space into feature space with reconstruction errors and defines semantic mapping features used to detect unknown attacks. Verication tests are performed using the public NSL_KDD database. From the experiments conducted in this work, it shows that the results achieve an average accuracy of 88.3%, which is better than other methods.

Title: Real-time Attack Scenario Reconstruction from COTS Audit Data_
Author Name: Sadegh M. Milajerdi2, Junao Wang1
Year: August 16–18, 2017

Explanation:

We provide a host of companies with approaches and systems to recover from attack scenarios in real time. We develop a platform-neutral, main memory-based, dependency graph abstraction of audit-log data to meet the scalability and real-time needs of the problem. We then present an efficient signature-based technique for attack detection and reconstruction, including source identification and impact analysis. We also developed a way to open the big picture of the attack by building a compact, visual graphic of the attack steps. Our system participated in DARPA-organized attack team evaluations and was able to successfully discover and reconstruct the details of the team's attacks on hosts running Windows, Free BSD, and Linux.

Title:A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.
Author Name: Anna L. Buczak, Erhan Guven
Year: 26 October 2015

Explanation:

This research paper describes a literature review focused on machine learning (ML) and data mining (DM) techniques for cyber analytics to support intrusion detection. A brief tutorial explanation of each ML/DM method is provided. Based on the number of citations or the relevance of the emerging method, papers illustrating each method were identified, read, and summarized. Since data is very important in ML/DM approaches, some well-known cyber datasets used in ML/DM are described. The complexities of ML / DM algorithms are addressed, the challenges in using ML / DM for cyber security are discussed, and some recommendations are made for when to use the given technique.

Title:A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)
Author Name: Amol Borkar, Akshay Donode, Anjali Kumari
Year: 23-24 Nov. 2017

Explanation:

Today, billions of people around the world access the Internet. Intrusion detection technology is a new generation of security technology that monitors systems to avoid malicious activity. This paper consists of a literature review on internal intrusion detection systems (IIDS) and intrusion detection systems (IDS) and uses some data mining and forensic algorithms for real-time system operation. Data mining techniques are proposed for cyber analytics to support intrusion detection.

II.CHAPTER

2.1 Methodology:

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

2.2 Modules:

➢ **REGISTER**

➢ **LOGIN**

➢ **CID**

- ADD CRIMINAL DATA
- VIEW LAWER REQUEST

➢ **DIG**

- MAINTAIN CRIMINAL DATA
- RESPONSE TO LAWER

➢ **STATE POLICE**

- APPROVE REGISTERATION
- VIEW PUBLIC COMPLAINT
- MOVE LOCAL STATION

➢ **LOCAL POLICE**

- ADD CRIMINAL DATA
- VIEW STATE POLICE FILES
- MAKE REPORT

➢ **PUBLIC ADD COMPLIANT**

➢ **LAWYER**

- VIEW THE LOCAL POLICE DATA
- REQUEST CRIMINAL DATA
- DOWNLOAD CRIMINAL DATA

2.3 Module Description:

Register:

The registration module provides a conceptual framework for entering information about the department: local police and prosecutors, etc., facilitating data entry and accuracy by matching the department's data source (usually a paper file created at the point of care). easily return to individual department records to link registers to departmental information and collect data elements for better control of the tender program.

Login:

In this module in our project, it refers to a unit implemented in a database management system (or a similar system) and managed independently and reliably from other processes. Transaction usually refers to all the changes in the database in each entry of the module to display the page.

Cid:

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

1. Add Criminal Data:

In this module in our project, CID can add the data about past criminal data such as kidnaping, chain snatching, murder, and other cases Acquist details to the database.

2. View Lawyer Request:

In this module in our project, CID must know the details of the crime for their investigation like a lawyer. If the lawyer is the person authorized to see the crime information sent by the CID to the DIG**.**

Dig:

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

1. Maintain Criminal Data:

In this module our project, DIG have to maintain the all criminal details in his data base, such as CID added data and local police added data.

2. Response To Lawyer

In this module in our project, we have to answer DIG to store data. Here the DIG is looking at the lawyer's request. If the attorney is an authorized user, the DIG responds to the attorney asking for the secret key name.

State Police:

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

1. Approve Registeration:

In this module in our project, we need to validate the local police badge for the reference of the police officer. Registration here is not accepted by the state police, local police cannot access. Therefore, the state police must accept the registration.

2. View Public Complaint:

In this module in our project, the state police handles public complaints.

3. Move To Local Station:

In This Module In Our Project, where the state police will refer public complaints to the local police station in the same area.

Local Police:

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

1. Add Criminal Data:

In this module in our project, we also need to add criminal records to the local police database. This will be presented by the DIG.

2. View State Police File:

In this module in our project, the local police see the file sent by the state police for a new investigation.

3. Make Report:

In this module in our project, the local police report for each investigation.

Public Add Complaint:

In this module in our project, ordinary people apply online. Complaints are handled directly by the police.

Lawyer:

1. View The Local Police Data:

In this module in our project, the lawyer looked at some records from the local police department. But not all posts can be viewed. Some confidential files will be kept confidential by the DIG department.

2. Request Criminal Data:

In this module in our project, a private lawyer needs some criminal information for investigation. So the lawyer asked the DIG for criminal information.

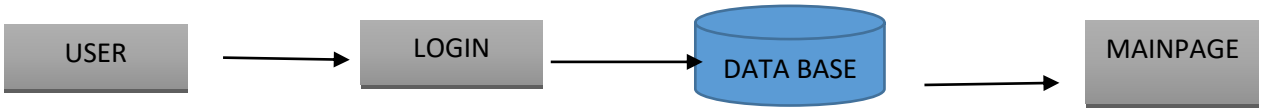
3. Download:

In this module in our project, after DIG has responded with the secret key request. Then enter the key to download the recording.

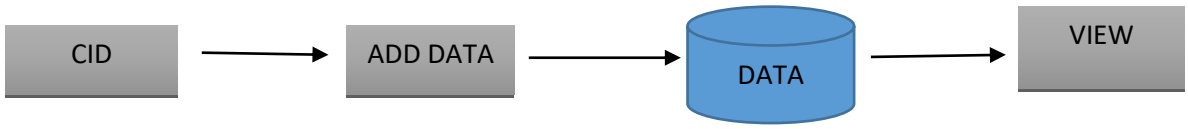
2.4.Module Diagram:

1. Register:

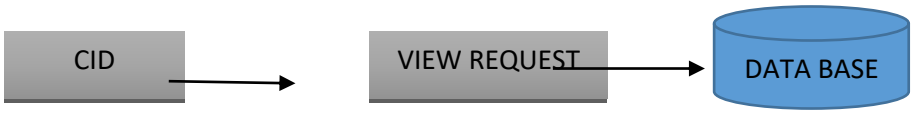
2. Login:



3. Cid:
Add Criminal Data:

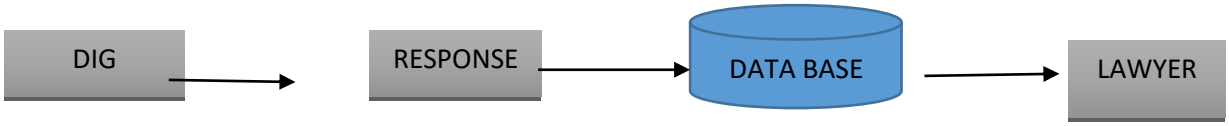


3.1. View Lawyer Request:

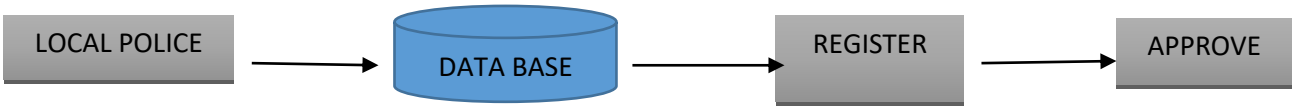


4. DIG:
Maintain Criminal Data:

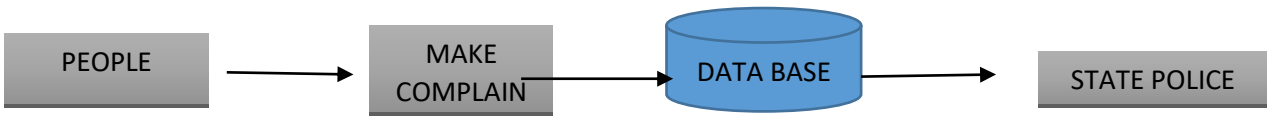
4.1. Response Lawyer Request:



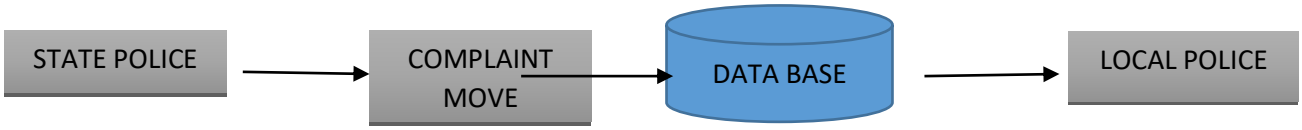
5. State Police:
Approve Registration:



View Public Complaint:

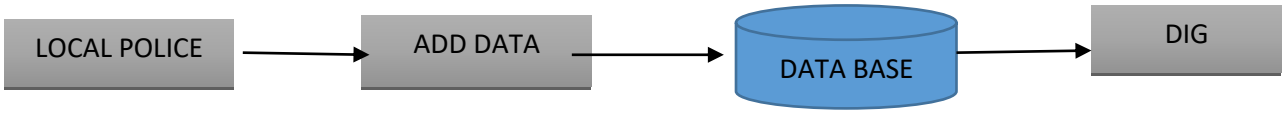


Move To Local Police:

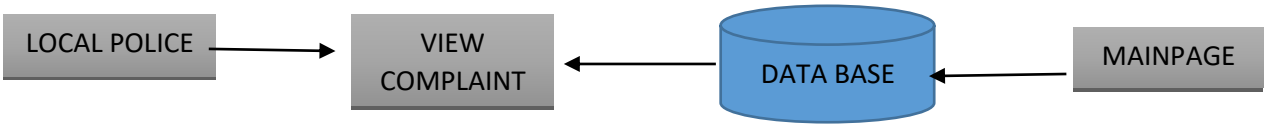


6. Local Police:

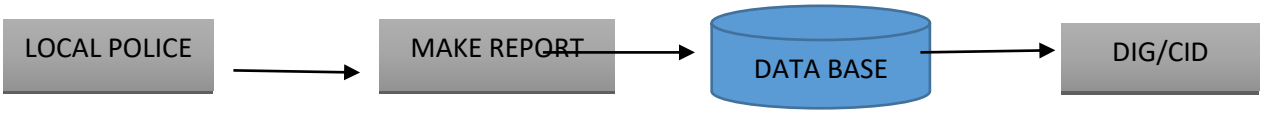
Add Criminal Data:



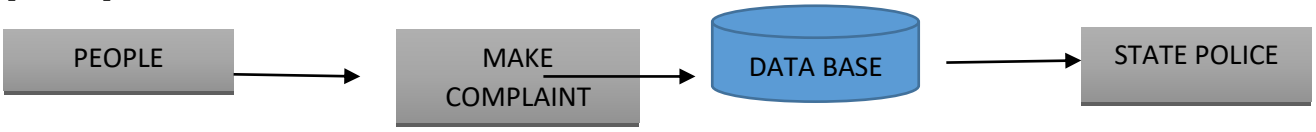
6.1. View State Added Data:



Make Report:

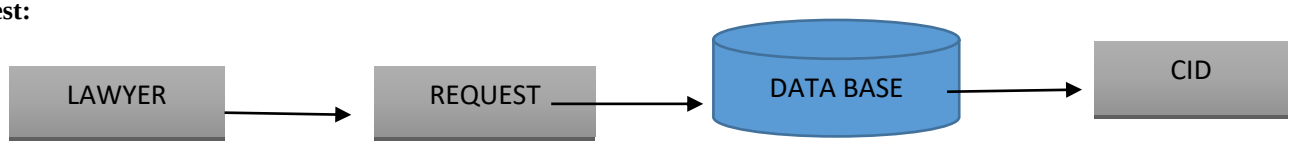


7. People Complaint:

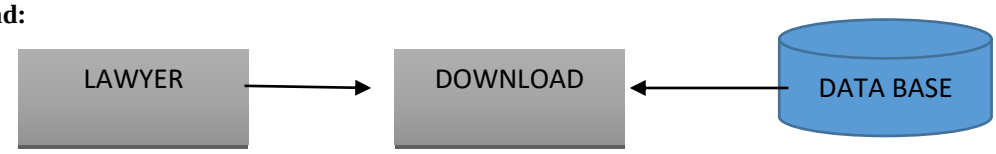


8. Lawyer:
View:

Request:



Download:



III.REQUIREMENTS ENGINEERING

3.1 General

This is a requirement to complete the project. Without using these tools and software, we cannot do the project. So we have two requirements to carry out the project. They are

1. Hardware requirements.
2. Software requirements.

3.2 Hardware Requirements

Hardware requirements may form the basis of the contract for system implementation and should therefore be a complete and consistent specification for the entire system. Software engineers work as a starting point for system design. It does not show what the system does and 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

3. 3 Software Requirements

A software requirements document is a system specification. It should include definition and specification of requirements. A system is a set of what to do, not how to do it. Software requirements provide the basis for creating software requirements specifications. Useful for estimating costs, planning team activities, executing tasks and tracking team progress and team development progress.

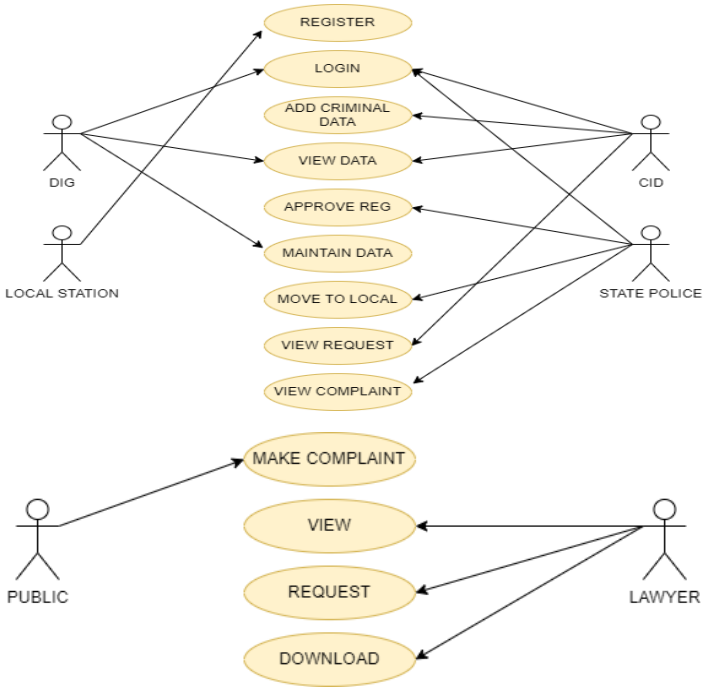
Front End : J2EE (JSP, SERVLETS) JAVASCRIPT
Back End : MY SQL 5.5
Operating System : Windows 07
IDE : Eclipse

IV.DESIGN ENGINEERING

4.1 General

Engineering Design deals with various UML [Unit Modeling Language] diagrams to implement a project. A design is a meaningful engineering representation of the thing to be built. Software design is the process of translating requirements into software representations. Design is where quality is expressed in software engineering. Design is a means of accurately translating customer requirements into finished products.

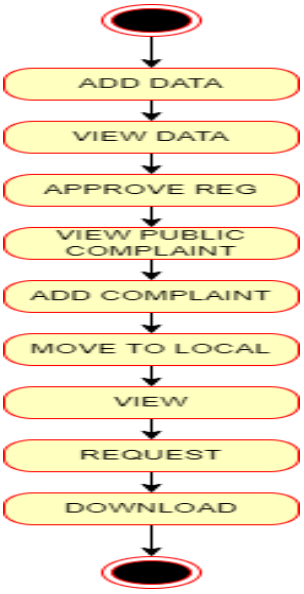
4.1.1 Use-Case Diagram:



Explanation:

Application diagrams are the basic building blocks of object-oriented modeling. It is used for continuous general concept modeling of the program and complete modeling to translate the model into program code. For this, we recommend the data in this proposed method that uses the Hash-Suleiman code algorithm to first encrypt the data in our component diagram.

4.1.2 State Diagram:

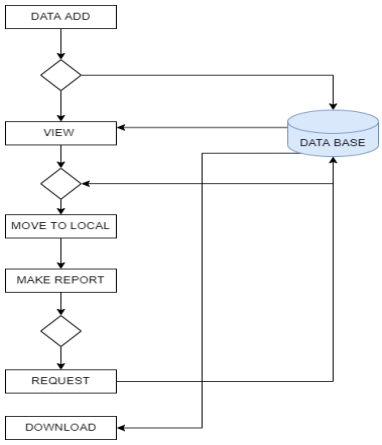


Explanation:

State diagram requires that the system represented consists of a finite set of numbers; sometimes, it's true, other times it's a convenient abstraction. There are many types of state charts, they are quite different and have different meanings.

For this in our state diagram, first submit the data in this proposed method that uses Hash-Suleiman code algorithm to encrypt the data in our component diagram.

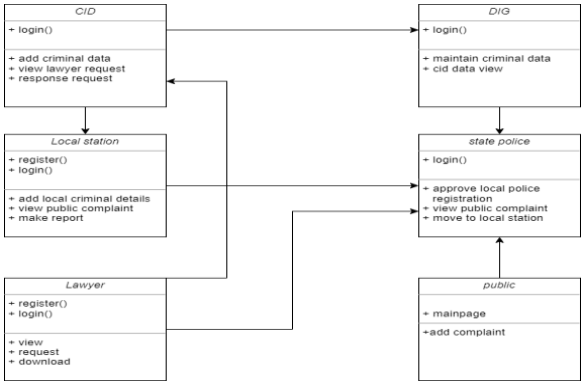
4.1.3 Activity Diagram:



Explanation:

An action diagram is a well-defined diagram for showing a step-by-step workflow of activities and actions with support for choices, iterations, and compromises. In UML, activity diagrams can be used to describe the operations and steps of components in a system. UML activity diagram can model the internal logic of a complex process. In many ways, UML activity diagrams are the object-oriented equivalent of structural development flow diagrams and data flow diagrams (DFDs).

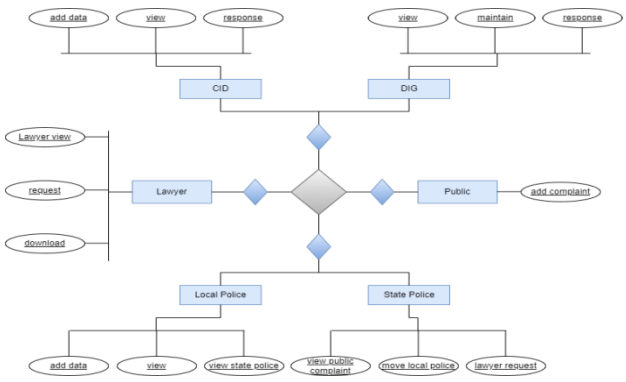
4.1.4 Classdiagram:



Explanation:

A class diagram is a type of static structure diagram that describes the structure of a system by showing classes, properties, and relationships between classes. A class in a class diagram represents an object or an interaction between an object and a program.

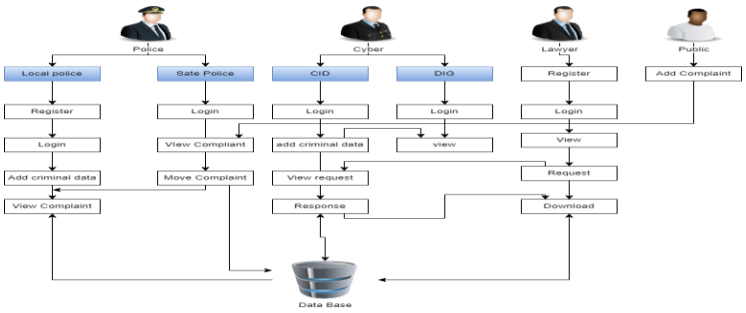
4.1.5 E-R Diagram:



Explanation:

An entity is represented as a rectangle in an ER diagram. For example: In the ER diagram below, there are Students and Universities, and these two entities have a relationship such as how many students are in a college. We will read about relationships later, but for now we will focus on entities.

4.1.6 System Architecture:



Explanation:

The System Architect defines the basic structure of the system, and we propose Solomon's code Hash algorithm. To protect privacy, we may leave a small amount of data on local devices and cloud servers. In addition, based on computational intelligence, this algorithm can calculate the share of distribution stored in the cloud, fog, and local machines, respectively. The performance of our scheme has been verified by theoretical security analysis and experimental evaluation, which is indeed a strong complement to existing cloud storage schemes.

V.CHAPTER

Development Tools

5.1 General:

This chapter is about programming languages and tools used in project development. The platform used here is JAVA. The main languages are JAVA, J2EE and J2ME. J2EE is selected for implementation in this project.

5.2 Features of Java

5.2.1 The Java Framework

Java is a programming language developed by James Gosling at Sun Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but has a simpler object model and low-level objects. Java programs are typically compiled in bytecode that can be run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, consistent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It is intended to allow developers to "write once, run anywhere."

Java is considered one of the most influential programming languages in the 20th century and is widely used in everything from software applications to web applications. The java framework is a new platform that simplifies Internet application development. The flexibility, efficiency, platform portability and security of Java technology make this technology the best for network computing. From laptops to data centers, gaming consoles, scientific supercomputers, mobile phones to the Internet, Java is everywhere!

5.2.2 Objectives of Java

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

Why Software Developers Choose Java:

Java has been tested, refined, extended and proven by a dedicated community. With more than 6.5 million developers, it is the largest and most active in the world. With its versatility, efficiency and portability, Java has become valuable to developers, allowing them to:

• Write software for one platform and run it on almost any other platform
• Create applications to run in web browsers and web services
• Create server-side applications for online forums, stores, questionnaires, HTML form processing, and more
• Integrate applications or services using the Java language to create special applications or services
• Write powerful and efficient applications for cell phones, remote processors, low-cost consumer products and other digital heart rate devices.

Some Ways Software Developers Learn Java:

Today, many colleges and universities offer programming courses for the Java platform. In addition, developers can improve their Java programming skills by reading Sun's java.sun.com website, subscribing to Java technology-oriented

newsletters, using Java Tutorials and New to Java Programming Center, and registering on the Web. or instructor-led courses.

Object oriented:

To be an object-oriented language, any language must follow at least four characteristics.

1. Inheritance: The process of creating new classes and using the behavior of existing classes by reusing existing code and extending it to add enhancements as needed.
2. Encapsulation: A mechanism to combine and abstract data.
3. Polymorphism: As the name suggests, polymorphism is a way of providing different functionality to a function of the same name based on the method signature.
4. Dynamic Linking: Sometimes when we write code we don't know about the specific type of object. Runtime is a way to ensure that programs run at peak performance.

5.2.3 Java Server Pages - Overview

Java Server Pages, or JSP for short, is today's solution for developing dynamic web pages. JSP provides excellent server-side scripting support for creating database-driven web applications. JSP allows developers to embed jasp code directly into jsp files, making the development process simpler and easier to maintain.

JSP pages are efficient, they are loaded into the web server's memory the first time they receive a request, and subsequent calls are served very quickly.

In today's environment, most websites provide dynamic pages based on user demand. A database is a great way to store information about users and other objects. JDBC provides a good database in a homogeneous database environment. Creating database driven web applications using JSP and JDBC cc very much.

Java is known for its "write once, run anywhere" feature. A JSP page is a Java Server Page

Java Server Pages (JSP) technology is a Java platform technology for delivering dynamic content to web clients in a compact, reliable, and transparent format. The Java Server Pages specification extends the Java Servlet API to provide web application developers with a powerful framework for creating dynamic web content on the server using HTML, XML templates, and Java code, independent of the server platform.

JSP is built on top of the Servlet API and uses Servlet semantics. JSP is a request and response mechanism. Although JSP technology will be a strong successor to the main Servlets, they have an evolutionary relationship and can be used in a collaborative and complementary way.

Servers are sometimes a bit difficult when it comes to creating strong and complex HTML. Most services contain a small amount of code that handles application logic and more code that handles output formatting. A different output format can make it difficult to extract and reuse part of the code when needed. Because of this, web application developers are turning to JSP as their preferred service environment.

5.2.4 Evolution of Web Applications:

Over the past few years, web server applications have evolved from static to dynamic applications. This evolution is necessitated by some shortcomings of website design. For example, traditional website design techniques are insufficient to put more business processes online, whether in the commercial-to-consumer (B2C) or business-to-business (B2B) market. The main problems that every developer faces when developing a web application are:

1. Scalability - a successful site will have more users and as the number of users increases rapidly, the web application must scale accordingly.
2. Integration of data and business logic - the web is a different way of doing business, so you need to be able to use the same middleware and data access code.
3. Management - the website continues to grow and we need some convenient mechanism to manage our growing content and interaction with the business system.
4. Personalization - Adding a personal touch to the website is a key factor in keeping our customers coming back. Knowing their preferences, allowing them to customize the information they see, remind them of past actions or remember frequently searched keywords, in other words, is important to get feedback and interaction from a one-way conversation.

In addition to the general need for business-oriented websites, there is a need for new technologies to create reliable, dynamic and mobile server-side web applications. Key features of modern dynamic web server applications are:

1. Serve HTML and XML and transmit data to the web client
2. separate display, logic and data
3. Interface to database, other Java applications and CORBA, directory and mail service
4. Use application server middleware to provide transaction support.
5. Track client sessions.

5.2.5 Benefits of JSP

One of the main reasons why Java Server Pages technology became and continues to evolve today is the technical need to simplify application design by separating dynamic content from static template presentation data. Another advantage of using JSP is that it allows you to separate the role of the web application/HTML designer from the application developer. JSP technology has several interesting advantages below:

1. JSP technology is a platform independent of dynamic web pages, web server and core server components. That is, JSP pages are not perfect on any platform, on web servers and web application servers. JSP pages can be accessed from any web server.

2. JSP technology emphasizes the use of reusable components. These components can be combined or manipulated to develop more targeted components and site designs. In addition to reducing development time, JSPs are very different from Servlets, but at runtime they are divided into Servlets and executed by the JSP engine built into the Web application server, such as BEA Web Logic. and IBM Web Sphere.

5.3 Servlets:

Previously, in client-server computing, each program had its own client program that acted as a user interface and had to be installed on each user's personal computer. Most web applications use HTML/XHTML, which all browsers support, and web pages are presented to clients as static documents.

Websites can only display static content and allow users to navigate content, but web applications provide a more interactive experience.

Any computer running servlets or JSPs must have a container. Containers are not just software responsible for loading, executing and unloading Servlets and JSPs. Servlets can be used to extend the functionality of a Java-enabled server.

It is commonly used to extend web servers and effectively replaces CGI scripts. CGI is one of the earliest and most prominent server-side dynamic content solutions, so it's important to know the difference between CGI and Servlets before moving forward.

5.4 Java Servlets

Java Servlet is a generic server extension which means you can dynamically load java classes to extend server functionality. The service is used by web servers and runs inside the Java Virtual Machine (JVM) on the server, making it secure and portable. Unlike apps, they do not require java support in web browsers. Unlike CGI, the server does not use multiple processes to handle a single request. The server can be managed by separate threads in the same process. The server is mobile and platform independent.

A web server is a combination of a computer and the software installed on it. Web servers communicate with clients through web browsers. It serves web pages to clients and applications using web browsers and the HTTP protocol.

Define a web server as a set of software packages installed on a computer connected to the Internet or an intranet to download the files needed to serve e-mail and build and distribute web pages using the File Transfer Protocol. A web server works in a client-server model.

5.5 Conclusion

JSP and Servlets are rapidly being adopted to provide dynamic content on the web. With full access to the Java platform and working securely from a server, the application possibilities are almost limitless. When JSP is used with Enterprise JavaBeans technology, e-commerce and database resources can be further enhanced to meet the demand for web applications that provide secure operation on an open platform. J2EE technology makes it easier to develop, deploy, and use web server applications than messing around with other technologies like CGI and ASP. There are many tools available to facilitate fast web application development and easily convert existing server-side technologies to JSP and Servlets.