Ex No: 15 APPLYING DATA MINING IN CYBER CRIME

PROBLEM DEFINITION

- Our project is based on the reliability and availability of network services are being threatened by the growing number of Denial-of-Service (DoS) attacks.
- Effective mechanisms for DoS attack detection are demanded.
- Investigate and extract second-order statistics from the observed network traffic records.
- These second-order statistics extracted by the proposed analysis approach can provide important correlative information hiding among the features.
- By making use of this hidden information, the detection accuracy can be significantly enhanced.

INTRODUCTION

Cloud computing is a recent technology that aims at providing access to resources instantly as per the needs of the end users. Cloud enables its customers to make use of the resources that are widely distributed in the internet to perform computations without installing in their own PC's and has to pay only for the service they consumed. All the computational requirements will be taken care of by the cloud service providers and hence all the complexities involved will be hidden from the user. NIST identifies the five key characteristics of cloud computing as on- demand self- service, resource pooling, broad network access, rapid elasticity and measured service.

Cloud offers services in three basic forms namely infrastructure (IaaS),platforms (PaaS) and Software (SaaS) and is on the stage of evolution to provide everything as a service (XaaS). As large magnitudes of data are moving onto the cloud, the attackers are keener to exploit the vulnerabilities associated with cloud and thereby to steal the sensitive data. Among the various threats tocloud computing, Denial of Service(DoS) attacks can prove to be the deadliest attack and even the Cloud Security Alliance has identified DoS attack as one of the nine major threats. In DoS attack, the intruder overloads the target system with service requests so that it cannot respond to any further requests and hence resources will be made unavailable to its users. Distributed Denial of Service(DDoS) attack makes use of several compromised machines called zombies to launch DoS attack on the target machine and the service is disrupted or delayed.DDoS attacks are getting more frequent these days and hence proper intrusion detection systems has to be deployed.

This project discusses the 2 various kinds of DDOS attacks possible and the various countermeasures that need to be followed to avert such attacks.

In computing,a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources.

This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations. Criminal perpetrators of DoS attacks often target sites or services hosted on highprofile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

SYSTEM REQUIREMENTS

Below are the tools, languages and software that were used to develop a Book Resale Application System:

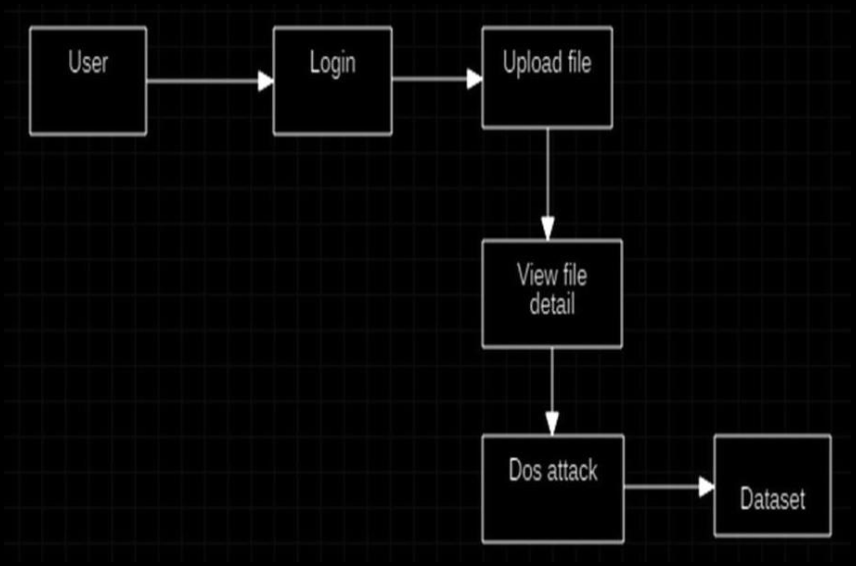
HARDWARE REQUIREMENTS

Processor	:	Intel Core 2
Speed	:	1.1 GHz
Hard Disk	:	250 GB.
Monitor	:	SVGA
Mouse	:	Optical
Ram	:	1GB

SOFTWARE REQUIREMENTS

Operating System	:	Windows95/98/2000/XP/7.	Operating System
Application Server	:	Tomcat6.0/7/8.X.	Application Server
Front End &CSS	:	Java,HTML	Front End &CSS
Scripts	:	JavaScript.	Scripts
Server side Script	:	Java Server Pages.	Server side Script
IDE	:	Eclipse/ Net beans	IDE
Back End	:	MYSQL 5.0/ Heidi SQL 8.1	Back End

DATA FLOW DIAGRAM



TESTING

SYSTEM TESTING

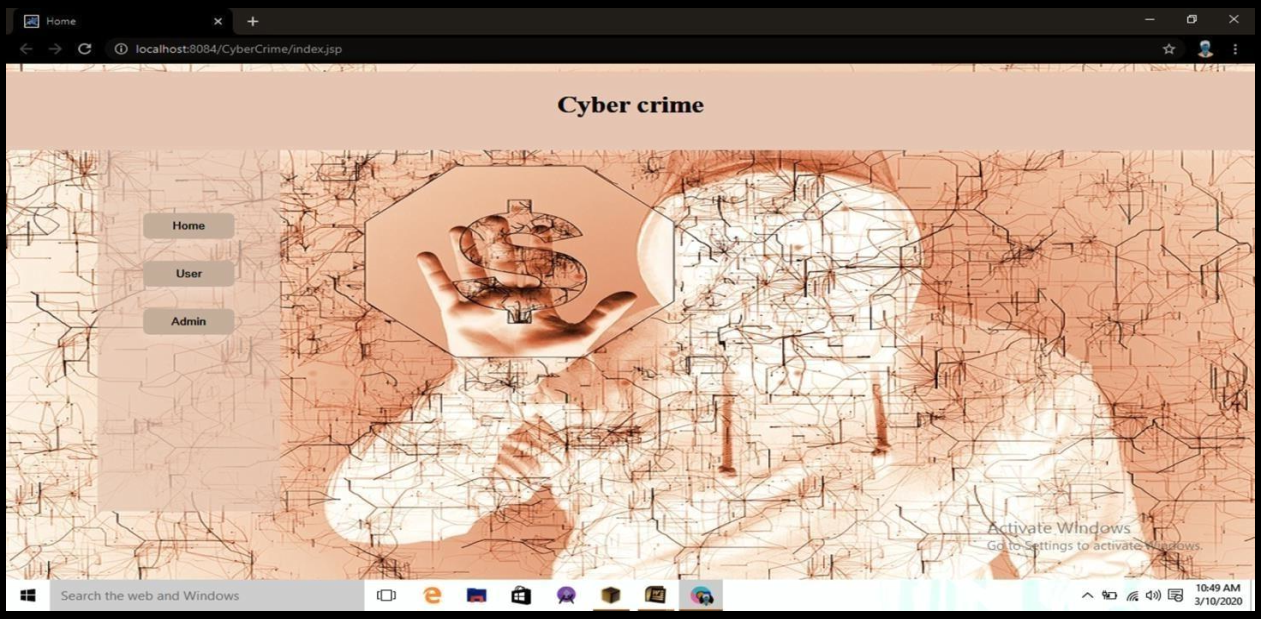
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product ,it is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

UNIT TESTING

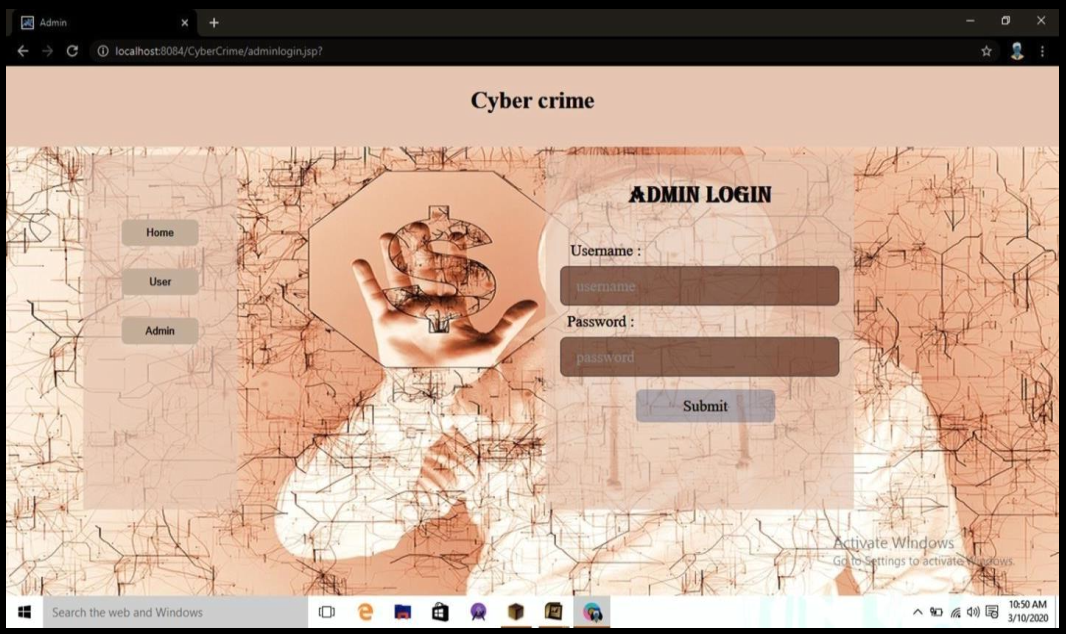
Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

SCREENSHOTS

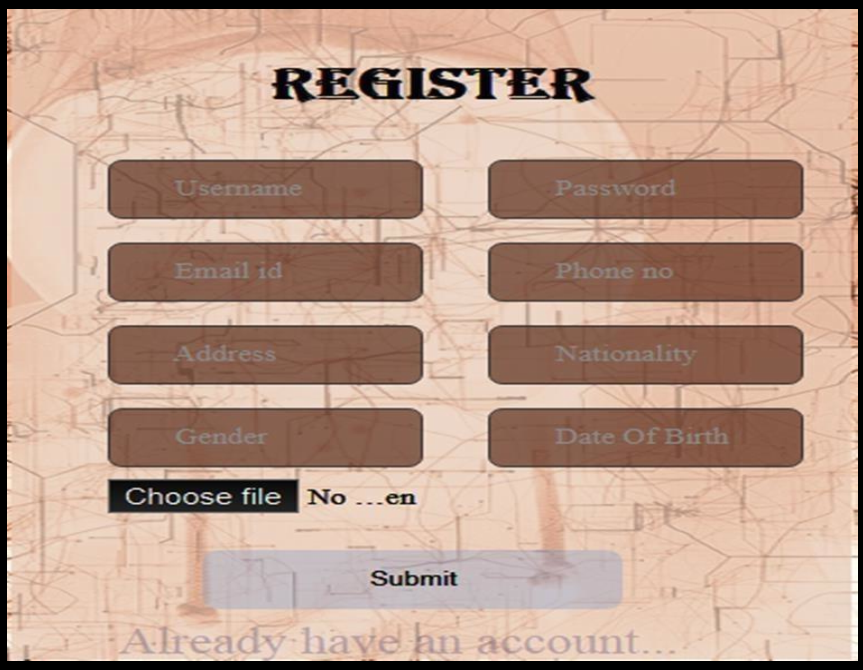
HOME



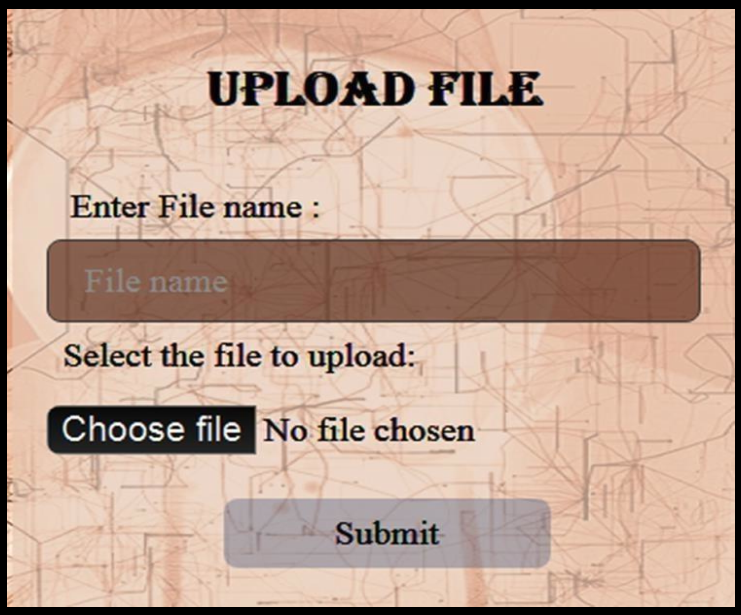
ADMIN



USER



USER REGISTRATION



RESULT

Thus, the Book Resale Application System was implemented using the specified front end andback end tools.