

MANAGING FRAUD DETECTION PROPAGATION IN MOBILE SOCIAL NETWORKS

*Mini Project Report submitted to Jawaharlal Nehru Technological University Hyderabad in
Partial Fulfillment of The Requirements for The Award of Degree of*

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE & ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

BY
KANCHUKATLA MAHA LAKSHMI
(21X31A6625)

Under the Guidance of
Mrs B. SARITHA
(Assistant Professor)



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

SRI INDU INSTITUTE OF ENGINEERING & TECHNOLOGY

(Affiliated to JNTUH, Hyderabad, Approved by AICTE, New Delhi)
Sheriguda (V), Ibrahimpatnam (M), R.R.Dist., Telangana- 501510.

(2024-2025)

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Affiliated to JNTUH, Kukatpally, Hyderabad)

Sheriguda (V), Ibrahimpatnam (M), R.R.Dist. 501510.



CERTIFICATE

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)**

This is to certify that the dissertation entitled “**MANAGING FRAUD DETECTION PROPAGATION IN MOBILE SOCIAL NETWORKS**”, being Submitted by **KANCHUKATLA MAHA LAKSHMI (21X31A6625)**, to **Jawaharlal Nehru Technological University Hyderabad** in partial fulfillment of the requirements for the award of the degree of *Bachelor of Technology in Computer Science & Engineering(Artificial Intelligence and Machine Learning)*, is a record of bonafide work carried out by them. The results of investigations enclosed in this report have been verified and found satisfactory. The results embodied in this dissertation have not been submitted to any other University or Institute for the award of any other degree.

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

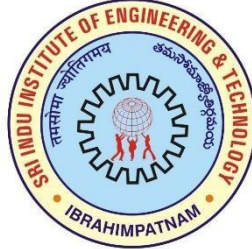
PRINCIPAL

EXTERNAL EXAMINER

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Affiliated to JNTUH, Kukatpally, Hyderabad)

Sheriguda (V), Ibrahimpatnam (M), R.R.Dist. 501510.



DECLARATION

I, **KANCHUKATLA MAHA LAKSHMI (21X31A6625)**, hereby certify that the dissertation **“MANAGING FRAUD DETECTION PROPAGATION IN MOBILE SOCIAL NETWORKS”**, carried out under the guidance of **Mrs. B.SARITHA** is submitted to **Jawaharlal Nehru Technological University Hyderabad** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science & Engineering (Artificial Intelligence and Machine Learning)**. This is a record of bonafide work carried out by me and the results embodied in this dissertation have not been reproduced or copied from any source. The results embodied in this dissertation have not been submitted to any other University or Institute for the award of any other degree.

Date:

KANCHUKATLA MAHA LAKSHMI

(21X31A6625)

Department of CSE (AI&ML), SIET

ACKNOWLEDGEMENT

With great pleasure I take this opportunity to express my heartfelt gratitude to all the persons who helped me in making this project work a success.

First of all, I express my sincere thanks to **Mr. R. VENKAT RAO, Chairman**, Sri Indu Group of Institutions, for his continuous encouragement.

I am highly indebted to **Principal, Dr. I. SATYANARAYANA** for giving me the permission to carry out this project.

I would like to thank **Dr M.C.RAJU** Professor & Head of the Department CSE(AI&ML), for giving support throughout the period of my study in SIJET. I am grateful for his valuable suggestions and guidance during the execution of this project work.

My sincere thanks to project guide **Mrs. B.SARITHA**, Assistant Professor, for potentially explaining the entire system and clarifying the queries at every stage of the project.

My whole hearted thanks to the staff of **Computer Science and Engineering (Artificial Intelligence and Machine Learning)** who co-operated me for the completion of the project in time.

I also thank my parents and friends who aided me in completion of the project.

KANCHUKATLA MAHA LAKSHMI
(21X31A6625)

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY



Accredited by NAAC A+ Grade

Recognized under 2(f) of UGC Act 1956.
(Approved by AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)

Khalsa Ibrahimpatnam, Sheriguda(V), Ibrahimpatnam(M), Ranga

Reddy Dist.,

Telangana – 501 510



<https://siiet.ac.in/>

INSTITUTE VISION

To become a premier institute of academic excellence by providing the world class education that transforms individuals into high intellectuals, by evolving them as empathetic and responsible citizens through continuous improvement.

INSTITUTE MISSION

IM1: To offer outcome-based education and enhancement of technical and practical skills.

IM2: To continuous assess of teaching-learning process through institute-industry collaboration.

IM3: To be a center of excellence for innovative and emerging fields in technology development with state-of-art facilities to faculty and students fraternity.

IM4: To create an enterprising environment to ensure culture, ethics and social responsibility among the stakeholders

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY



Accredited by NAAC A+ Grade

Recognized under 2(f) of UGC Act 1956.

(Approved by AICTE, New Delhi and Affiliated to JNTUH,

Hyderabad)

Khalsa Ibrahimpatnam, Sheriguda(V), Ibrahimpatnam(M), Ranga Reddy Dist.,

Telangana – 501 510



<https://siiet.ac.in/>

Department of Computer Science and Engineering (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

DEPARTMENT VISION

To nurture proficient and socially responsible engineers specializing in Artificial Intelligence and Machine Learning, making significant contributions to society.

DEPARTMENT MISSION

- DM1:** To educate students in the fundamental principles of computing and cultivate the skills necessary for solving practical problems using modern computer-based technologies.
- DM2:** To offer state-of-the-art computing laboratories and enrich students' practical knowledge.
- DM3:** To instill self-learning abilities, foster a sense of teamwork, and promote professional ethics among students, preparing them to meet the society's demands.
- DM4:** To provide intensive training to cultivate expertise in the latest concepts and technologies within Artificial Intelligence and Machine Learning.

ABSTRACT

Mobile social networks (MSNs) provide real-time information services to individuals in social communities through mobile devices. However, due to their high openness and autonomy, MSNs have been suffering from rampant rumors , fraudulent activities, and other types of misuses. To mitigate *such* threats, it is urgent to control the spread of fraud information. The research challenge is: how to design control strategies to efficiently utilize limited resources and meanwhile minimize individuals' losses caused by fraud information ? To this end, we model the fraud information control issue as an optimal control problem, in which the control resources consumption for implementing control strategies and the losses of individuals are jointly taken as a constraint called total cost, and the minimum total cost becomes the objective function. To address these challenges, effective mechanisms for mitigating fraudulent information dissemination are paramount. This entails the formulation of robust control strategies that judiciously allocate finite resources to curtail the spread of harmful content. Central to this endeavor is the balance between resource efficiency and the minimization of user detriment caused by misinformation. By conceptualizing the fraud information control problem as an optimal control framework, a dual-objective approach emerges: minimizing the cumulative losses to users while optimizing resource utilization. Our research focuses on developing a mathematical model that integrates resource expenditure and user impact into a unified cost function.

CONTENTS

| TITLE | Page No |
|---------------------------------------|----------------|
| Acknowledgement | i |
| Institute Vision,Mission | ii |
| Department Vision Mission | iii |
| Abstract | iv |
| Contents | v,vi |
| List of Figures | vii |
| List of Screens | viii |
| CHAPTER-1: INTRODUCTION | 1 |
| CHAPTER-2: LITERATURE SURVEY | 3 |
| CHAPTER-3: SYSTEM ANALYSIS | 5 |
| 3.1 Existing System | 5 |
| 3.2 Proposed System | 6 |
| CHAPTER-4: SYSTEM REQUIREMENTS | 7 |
| 4.1 Functional Requirements | 7 |
| 4.2 Non Functional Requirements | 8 |
| CHAPTER-5: SYSTEM STUDY | 10 |
| 5.1 Feasibility Study | 10 |
| 5.2 Feasibility Analysis | 11 |
| CHAPTER-6: SYSTEM DESIGN | 13 |
| 6.1 System Architecture | 13 |
| 6.2 UML Diagrams | 14 |
| 6.2.1 Use Case Diagram | 16 |
| 6.2.2 Class Diagram | 17 |
| 6.2.3 Sequence Diagram | 18 |
| 6.2.4 Collaboration diagram | 19 |
| 6.2.5 Activity Diagram | 20 |

| | |
|--|----|
| CHAPTER-7: INPUT AND OUTPUT DESIGNS | 21 |
| 7.1 Input Designs | 21 |
| 7.2 Output Designs | 23 |
| CHAPTER-8: IMPLEMENTATION | 24 |
| 8.1 Modules | 24 |
| 8.2 Module Description | 24 |
| CHAPTER-9: SOFTWARE ENVIRONMENT | 26 |
| 9.1 Java Technology | 26 |
| 9.3 Source Code | 35 |
| CHAPTER-10: RESULTS | 38 |
| 10.1 System Testing | 38 |
| 10.2 Output Screens | 41 |
| CHAPTER-11: CONCLUSION | 45 |
| CHAPTER-12: REFERENCES | 46 |

LIST OF FIGURES

Following are the list of figures used in this project documentation at various locations.

| Figures | Page. No |
|-----------------------------|-----------------|
| 6.1 System Architecture | 13 |
| 6.2 UML Diagrams | 14 |
| 6.2.1 Use Case Diagram | 16 |
| 6.2.2 Class Diagram | 17 |
| 6.2.3 Sequence Diagram | 18 |
| 6.2.4 Collaboration diagram | 19 |
| 6.2.5 Activity Diagram | 20 |
| 9.1.1 Java Interpreter | 27 |
| 9.1.2 Java Compiler | 27 |

LIST OF SCREENS

Following are the list of Screens developed in this project at various stages.

| Screen | Page. No |
|------------------------------------|-----------------|
| 10.2.1 Application Window | 41 |
| 10.2. 2Admin Login | 42 |
| 10.2.3 User Registration | 43 |
| 10.2.4 User Login | 43 |
| 10.2.5 User Posts | 44 |
| 10.2.6 Fraud Information Spreading | 44 |

CHAPTER-1

INTRODUCTION

With the boom of the Internet and the rapid popularization of intelligent mobile devices, mobile social networks (MSNs) have grown up to become an important platform for information dissemination . MSNs can provide people with a variety of real-time information services and have already penetrated into our daily life. The Internet-based MSNs have exhibited their great charm and broad prospect in many application fields, such as instant communication, life service, interactive entertainment, etc., and have attracted extensive attention of the industry and the academia . However, the development of MSNs is like a double-edged sword . When MSNs are increasingly becoming an indispensable part of people's lives, a series of unhealthy phenomena, such as fake news, rumors, online promotion, and fraudulent activities are becoming more and more rampant, which pose a serious threat on the normal social network activities . Besides, by means of the emerging technologies of intelligent terminals, wireless networks, and online payment in recent years, the high rate of fraud has caused great losses to people . According to the official data released by the security ministry, telecommunications fraud in MSNs has grown at an annual rate of 20%–30%. The following are two representative scenarios

Scenario A: One scenario is the Veracruz incident in August 2015 . A piece of rumor saying “shootouts and kidnappings by drug gangs happening near schools in Veracruz” spread in Twitter and Face book. This rumor caused severe chaos in the city and many serious car crashes happened amid the hysteria.

Scenario B: Another shocking scenario occurred in August 2016 when a Chinese university professor suffered a telecommunication-based fraud, leading to a serious loss of 17.6 million Yuan . Criminals fabricated an elaborate hoax, used the network to transmit fraud information and perform remote frauds to victims. Fraud information diffusion has become a prominent problem in social networks . Those evidence highlight that effectively controlling the fraud information in MSNs applications is of great significance. Here, we define the so-called fraud information as a piece of malicious information or false information. which aims to intentionally cause adverse effects, such as mass panic or defraud victims of their property. In order to cope up with

the spread of such information in MSNs more effectively, it is an urgent need to study the pattern of fraud information diffusion and further put forward the corresponding control measures. Previously, some mathematical models have been used to model the diffusion evolutionary process of fraud information in the network. Most of these models are based on the theory of biological infectious disease because the spread process of infectious diseases in biology and the diffusion process of fraud information in the network are very similar. The most widely used model is the susceptible-infected recovered (SIR) model, in which all individuals are divided into three categories: 1) susceptible; 2) infected; and 3) recovered. From the perspective of information diffusion, the semantics of susceptible, infected, and recovered can fully correspond to the process of fraud information diffusion. If an individual has not yet received any fraud information, it belongs to the susceptible state. If an individual received fraud information and was misled, it belongs to the infected state. If an individual was ever infected and now no longer believes the fraud information, it belongs to the recovered state.

Although the existing SIR-based derivation models can correctly describe the transitional relationship and the dynamic evolutionary processes of node states, the spread of fraud information in MSNs shows some new characteristics. First, the information sender and receiver are human beings, and human mental activities are often complex. For example, the individual will likely experience a series of mental activities, such as thinking, hesitating, and wandering when receiving a piece of information. Second, the fraud information diffusion processes in MSNs are the complex results of the continuous interactions of nodes in different states. Third, because of the psychological effect, repeated reception of the same information may give users the feeling of disgust and lead to reverse psychology. The data analysis about 4.4 million Twitter messages diffusion shows that in the process of information diffusion, users will deviate from the original intention of information and produce the phenomenon of emotional transfer. Due to these new characteristics, the existing SIR-based inference models fail to describe the evolutionary process of information diffusion accurately. Therefore, if the above characteristics can be taken into account in

the model, the dynamic evolution process of fraud information diffusion can be described more effectively.

CHAPTER 2

LITERATURE SURVEY

A wide range of techniques has been proposed for detecting fraudulent activities in mobile social networks. Early approaches relied on rule-based systems and heuristics to identify unusual behaviors, such as excessive messaging or repetitive interactions. However, with the increasing sophistication of fraudsters, machine learning and deep learning models have gained prominence. Supervised learning techniques, such as support vector machines and random forests, have been used to classify malicious users or activities, while unsupervised methods, like clustering and anomaly detection, focus on identifying deviations from typical user behavior. Recently, graph-based methods that analyze social connections and propagation patterns have shown promise, leveraging the network structure to identify suspicious nodes or edges. The integration of AI has further improved the adaptability of detection mechanisms, enabling the identification of new and evolving fraud patterns. Understanding how fraud propagates in mobile social networks is essential for effective detection and mitigation. Studies have shown that fraudsters exploit the inherent trust among connected users to propagate their activities. Social engineering techniques, combined with automated bots, facilitate rapid spread through weak links in the network. Researchers have developed models to simulate fraud propagation, such as the Susceptible-Infectious-Recovered (SIR) model and variations of epidemic models, to predict the spread of fraudulent activities. These models help in designing interventions to limit the reach of fraud, such as identifying critical nodes for targeted monitoring or quarantine. Hybrid approaches combining graph theory and temporal analysis have proven effective in capturing both spatial and temporal dimensions of fraud propagation. Managing fraud detection in mobile social networks faces several challenges. The dynamic and resource-constrained nature of mobile environments limits the deployment of computationally intensive algorithms. Additionally, ensuring user privacy while monitoring interactions remains a significant concern. False positives in fraud detection can harm user trust and platform reliability, necessitating improvements in precision and accuracy. Future research is focused on incorporating federated learning to enhance

privacy-preserving fraud detection and deploying edge computing for real-time analysis. Advanced techniques like reinforcement learning are also being explored to create adaptive systems that can respond to evolving fraud tactics. Addressing these challenges will require a balance between technical innovation, ethical considerations, and practical implementation. Another significant area of research in managing fraud detection propagation in mobile social networks is the use of collaborative filtering and trust-based systems. Collaborative filtering, often used in recommendation systems, has been adapted to detect fraudulent users by analyzing shared behaviors and common interactions among suspicious accounts. Trust-based models, on the other hand, evaluate the trustworthiness of users and their connections within the network. These models assign trust scores to users based on their interaction history, behavior consistency, and endorsements from other trusted users. By incorporating trust scores into fraud detection mechanisms, researchers aim to enhance the accuracy of identifying fraudulent accounts while minimizing false positives. Additionally, hybrid models combining trust metrics with graph-based propagation analysis have demonstrated improved effectiveness in halting fraud propagation at its early stages. This integration of collaborative and trust-based approaches is particularly promising in dynamic and large-scale mobile social networks where traditional methods may struggle to scale effectively.

Furthermore, the integration of blockchain technology is gaining attention for fraud detection in mobile social networks. Blockchain's decentralized nature and its ability to provide immutable transaction records make it an ideal solution for tracking and verifying user interactions. By storing user behavior data in a secure and transparent ledger, it becomes easier to detect inconsistencies and fraudulent activities. Additionally, blockchain can enable the implementation of decentralized reputation systems, allowing users to independently verify the trustworthiness of their connections. This approach not only enhances fraud detection but also promotes a more transparent and secure mobile social network environment.

CHAPTER-3

SYSTEM ANALYSIS

3.1. EXISTING SYSTEM

In recent years, research that explores social relationship structure for information diffusion in MSNs has been very active. Especially, the problem of maximizing the influence of information has attracted the attention from both the academia and industry, and a number of innovative research results.

At present, the research on information diffusion mainly develops along two branches: 1) modeling of the information diffusion process and 2) control of information diffusion process.

In view of the modeling of the information diffusion process, most scholars use the infectious disease diffusion model, the independent cascade model, the linear threshold model, the real dataset fitting method, and so on, to model the spatio-temporal dynamic evolutionary process of information diffusion.

DISADVANTAGES

- The system is less effective due to lack of thinking, trust, and diffusion, the three psychological cognitive and behavioral states.
- The system doesn't effective since gradually lose the awareness of fraud information due to its forgetting psychology, it may be infected again by fraud information in the future.

3.2. PROPOSED SYSTEM

in the proposed system, the system put forward a novel dynamics model, called *SWIR*, which can accurately describe the dynamic process of fraud information diffusion. Importantly, for the sake of efficiently utilizing the limited resources and minimizing the losses of individuals, we establish the optimal control system to solve the optimal dynamic allocation problem of control strategies for fraud information diffusion. The main contributions of this paper are summarized as follows.

- 1) **Fraud Information Diffusion Model:** In consideration of the uncertain mental state of individuals and the transitional relationship of individuals in different states, we establish the *SWIR* model. It can more effectively describe the dynamic diffusion process.

of fraud information in MSNs. In addition, we theoretically analyze the stability of the *SWIR* model and the trend of fraud information diffusion.

2) Dynamic Allocation of the Control Strategies: In order to efficiently utilize limited control resources and minimize losses of individuals caused by fraud information, we propose two synergistic control strategies. We take the control resources consumption and the losses of individuals as the *total cost* constraint. Then, we formulate the optimal control problem to minimize the total cost, and model the control strategies as functions varying over time. Finally, based on the optimal control theory, the optimal distribution of the control strategies functions over time is derived.

ADVANTAGES

- The proposed system establishes an information diffusion model to accurately describe the dynamic diffusion process of fraud information in MSNs by considering the uncertain mental states of individuals.
- The system analyzes the trend of information diffusion and the stability of the dynamics model from a theoretical point of view and explores the theory of dynamic evolution of information diffusion model.

CHAPTER-4

SYSTEM REQUIREMENTS

To design an effective system for managing fraud detection propagation in mobile social networks (MSNs), it is essential to outline both functional and non-functional requirements. These requirements address the core capabilities the system must provide (functional) and the qualities it must possess to perform efficiently and effectively (non-functional).

4.1. Functional Requirements

1. **Real-Time Fraud Detection and Monitoring** :The system must continuously monitor user behavior, interactions, and network activities in real-time to detect fraudulent activities. This includes identifying abnormal behaviors, such as a sudden surge in messages or interactions with known fraudulent accounts. Machine learning algorithms, both supervised and unsupervised, should be employed to classify behaviors as normal or suspicious. Additionally, real-time analytics should be integrated to ensure that fraud is detected and mitigated promptly, preventing it from propagating further across the network.

2. **Behavioural Profiling and Anomaly Detection**:The system must create and maintain dynamic profiles for each user, which track their historical behavior, including their communication patterns, login times, and interactions. This profiling allows the system to detect deviations from typical behavior that may indicate fraudulent activities. It should leverage anomaly detection algorithms to spot outliers and flag users exhibiting suspicious behaviors.

3. **Fraud Propagation Analysis**:The system should incorporate fraud propagation models, such as the Susceptible-Infectious-Recovered (SIR) model or other epidemic spread models, to simulate and predict how fraudulent activities might spread through the social network. This functionality would enable the system to take preemptive actions by isolating or quarantining affected users or sections of the network before fraud spreads extensively.

4. **Automated Response and Mitigation**: Once fraudulent behavior is detected, the system must trigger automated responses. These responses may include suspending suspicious accounts, notifying administrators, issuing warnings to users, or blocking

interactions that seem to propagate fraud. The system should be able to distinguish between various levels of fraud severity and apply corresponding actions accordingly.

5. Reporting and Alerting: The system should provide an easy-to-use interface for administrators and security teams to monitor fraud detection results. This includes real-time dashboards, alert notifications, and detailed reports on fraudulent activities. Alerts should be customizable based on predefined thresholds (e.g., number of flagged activities in a set time period), and reports should provide insights into trends and patterns of fraud for auditing and compliance purposes.

4.2. Non-Functional Requirements

1. Scalability

Given the massive growth in mobile social network users, the system must be designed to scale efficiently. As the number of users and interactions increases, the system must handle the growing volume of data without compromising performance. This scalability requirement includes horizontal scaling to accommodate increasing user numbers and the ability to handle more data points as the network expands.

2. Real-Time Performance : Fraud detection in MSNs requires low-latency processing, as fraud can spread rapidly within social networks. The system must be able to perform real-time analysis on large amounts of data with minimal delay. This includes processing user interactions, running machine learning algorithms, and issuing alerts or mitigation actions as soon as fraudulent behavior is detected.

3. Privacy and Security: Since mobile social networks involve sensitive user data, the system must incorporate robust privacy-preserving mechanisms. This includes anonymizing data, ensuring encryption of sensitive information, and adhering to data protection regulations such as GDPR. Federated learning, which enables machine learning models to be trained on user devices without sharing raw data, could also be employed to maintain privacy while performing fraud detection.

4. Fault Tolerance and High Availability: The system must be resilient to fault and ensure high availability, meaning it should continue functioning even in the event of server failures or network issues. This includes implementing failover mechanisms, redundant data storage, and distributed computing frameworks to ensure that fraud detection operations are not interrupted.

5. **Adaptability:** Fraud tactics continually evolve, so the system must be capable of adapting to new threats. This involves regular updates to machine learning models based on new fraud patterns, as well as incorporating feedback from flagged incidents to improve detection accuracy. The system should also allow for manual updates or rule modifications when new fraudulent behaviors emerge.

6. **Efficiency and Resource Management:** Considering the resource constraints of mobile devices, the system must operate efficiently without draining battery life or overburdening device processing power. This includes optimizing algorithms for mobile environments and leveraging edge computing to perform heavy computations on servers or distributed nodes rather than on the mobile devices themselves.

7. **User-Friendly Interface:** Administrators, security personnel, and end-users must have access to an intuitive and user-friendly interface for interacting with the system. This includes a clear dashboard for monitoring fraud detection results, simple configuration options for setting thresholds, and easy-to-navigate alert systems to notify administrators of suspicious activities.

8. **Compliance with Legal and Ethical Standards:** The system must operate within the legal frameworks of the countries where it is deployed, ensuring compliance with regulations such as GDPR, CCPA, and other data protection laws. Ethical standards should also be considered to ensure that user data is handled responsibly and that fraudulent activities are detected without violating user privacy rights.

CHAPTER-5

SYSTEM STUDY

5.1. Feasibility Study

A The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ◆ Economical feasibility
- ◆ Technical feasibility
- ◆ Social feasibility

Economical feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social feasibility:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system

5.2. Feasibility Analysis

Feasibility analysis is a more detailed, in-depth exploration of each of the feasibility aspects identified in the study. It helps to determine whether the project is viable and provides the necessary data and insights to make an informed decision. The analysis is structured as follows:

1. **Technical Feasibility Analysis** :The technical analysis focuses on whether the tools, technologies, and infrastructure required to build the fraud detection system exist and can be effectively integrated. It includes an evaluation of the following:

- **Machine Learning Models**: Can the system effectively use supervised, unsupervised, and hybrid models to detect fraud? Will it need to be retrained periodically as fraud techniques evolve?
- **Real-Time Data Processing**: Is the system capable of analyzing massive amounts of data in real time? This may involve evaluating streaming data platforms, edge computing, or cloud solutions that provide the computational power necessary for real-time fraud detection.
- **Privacy-Preserving Technologies**: Given the need to protect user data, technologies like federated learning, differential privacy, and data encryption must be considered to ensure compliance with privacy laws and maintain user trust.

2. **Operational Feasibility Analysis** The operational analysis investigates how well the system can function within the environment of mobile social networks. Key factors include:

- **User Experience Impact:** How will the fraud detection system affect the performance and experience of the users in the social network? A system that consumes too many resources may result in slow app performance, which could degrade user satisfaction.

- **Administrator Workflow:** Will the system provide administrators with intuitive, actionable reports and alerts? Is it easy for administrators to respond to fraud alerts and adjust system parameters as needed?

- **Scalability and Integration:** How well can the system handle the growing number of users, data volume, and network traffic as mobile social networks expand? Integration with existing social platforms (e.g., Facebook, Instagram) and the use of APIs to track user behavior is crucial.

3. **Financial Feasibility Analysis** :Financial feasibility focuses on whether the costs of developing, deploying, and maintaining the fraud detection system are justifiable by the benefits it provides. The analysis would include:

- **Development Costs:** Assessing the costs for research and development, including the purchase of necessary software, hardware infrastructure, and hiring of skilled personnel (data scientists, engineers).

- **Maintenance Costs:** Continuous costs for maintaining the system, such as cloud hosting, monitoring, and data storage fees. This also includes costs for ongoing machine learning model training, bug fixes, and updates.

- **Return on Investment (ROI):** Estimating the long-term benefits, such as reduced losses from fraudulent activities, improved user trust, and compliance with legal requirements. The financial feasibility analysis should determine whether the financial investment in the system is likely to pay off in the form of reduced fraud, increased user retention, and regulatory compliance.

CHAPTER-6

SYSTEM DESIGN

6.1. System Architecture

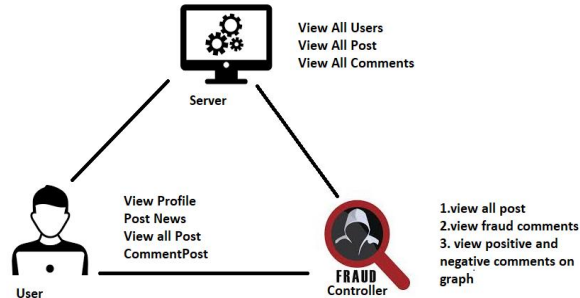


Fig 6.1 System architecture

The diagram represents the architecture of a **Fraud Detection System** within a mobile social network. The system has three primary components: the **User**, the **Server**, and the **Fraud Controller**. The **User** interacts with the system by performing actions such as viewing their profile, posting news, viewing all posts, and commenting on posts. The **Server** is the central hub, responsible for managing interactions, allowing users to access information about all users, posts, and comments. It acts as the communication bridge between the user and the fraud detection system. The **Fraud Controller** is tasked with detecting and analyzing fraudulent activities within the system. It can view all posts, specifically monitor fraudulent comments, and visualize the sentiments of comments (positive or negative) through graphs. By analyzing these interactions, the fraud controller helps identify harmful or suspicious content, ensuring that fraudulent activities, such as fake comments or spam, are detected and prevented. The fraud controller not only detects fraud but also helps visualize patterns and trends in comments, which can indicate broader fraudulent behavior. This architecture provides a robust system for maintaining the integrity of the social network by actively monitoring

user interactions and content for fraud detection. The fraud detection system also ensures that suspicious activities are flagged in real-time, allowing for quick intervention by administrators or automated mitigation actions. By leveraging the server and fraud controller, the system continuously monitors user behaviors, comments, and posts to identify potential threats before they spread. This proactive approach helps in maintaining a secure environment for users while reducing the risk of fraud and abuse within the network. Additionally, the system can generate reports and alerts for administrators to take necessary actions, ensuring that fraudulent content is quickly isolated and removed. The integration of sentiment analysis further enhances fraud detection by identifying negative or harmful patterns in user interactions.

6.2. UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.

6.2.1. USECASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

➤ Use case

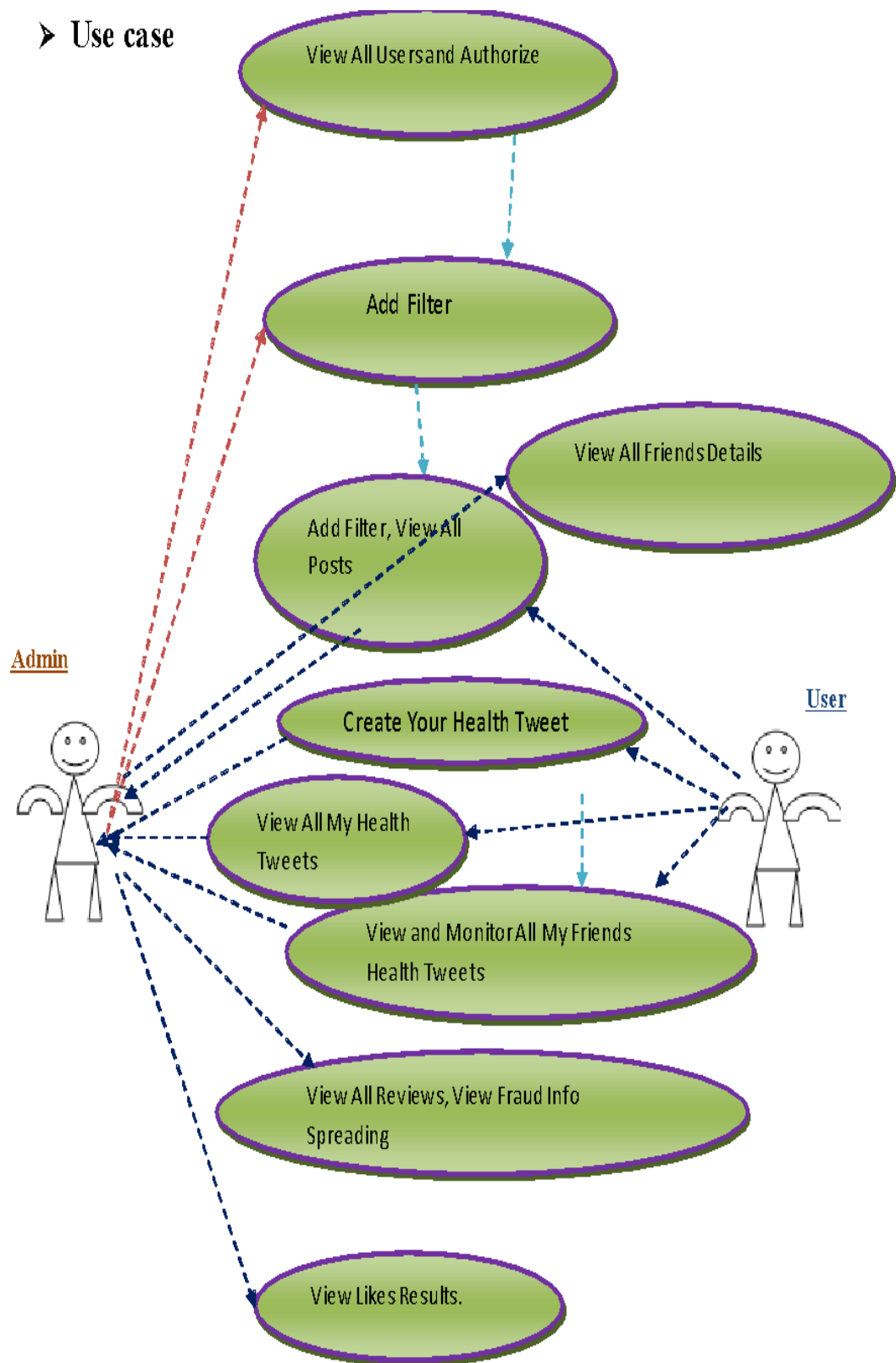


Fig 6.2.1 Use Case Diagram

6.2.2. CLASS DIAGRAM:

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class. Apart from this, each class may have certain "attributes" that uniquely identify the class.

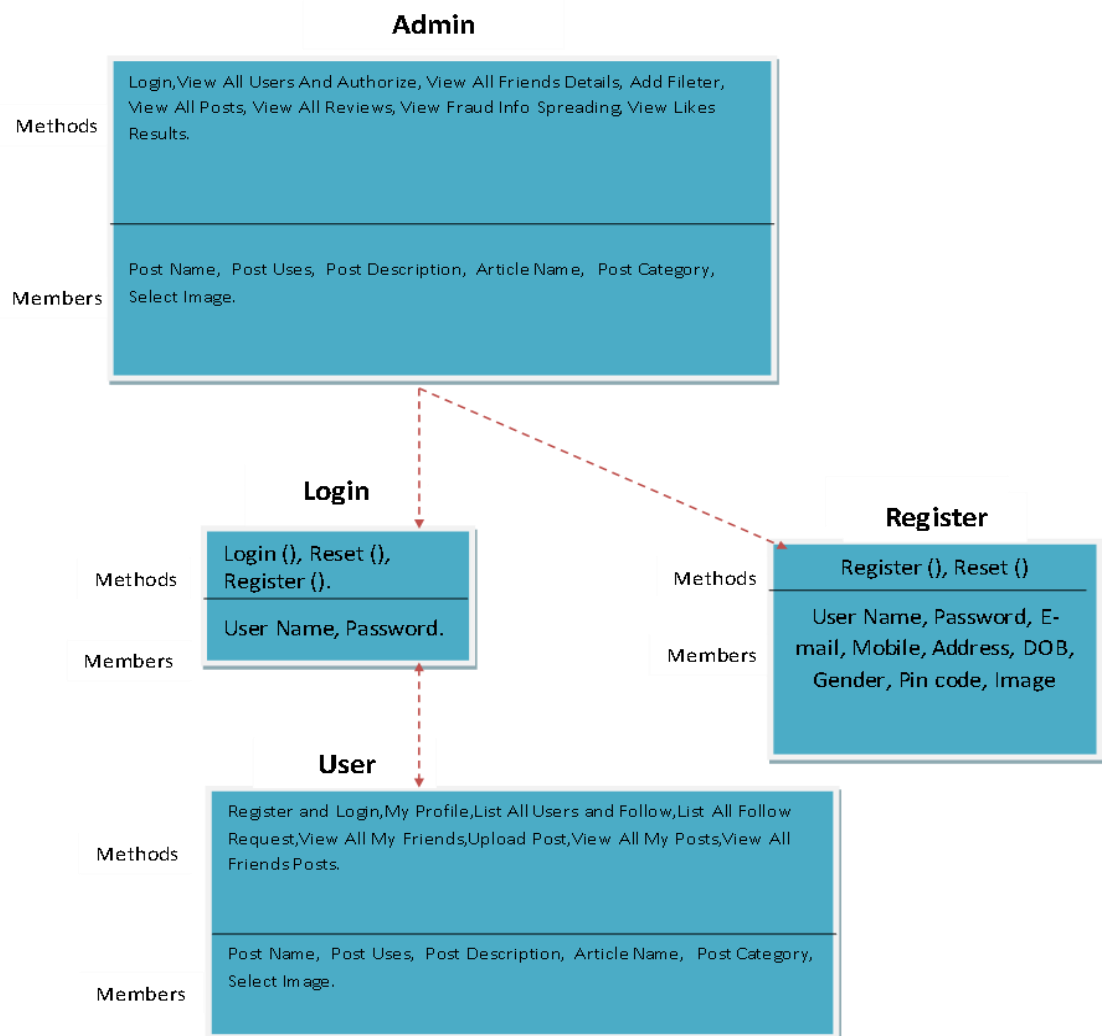


Fig 6.2.2 Class Diagram

6.2.3. SEQUENCE DIAGRAM:

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages".

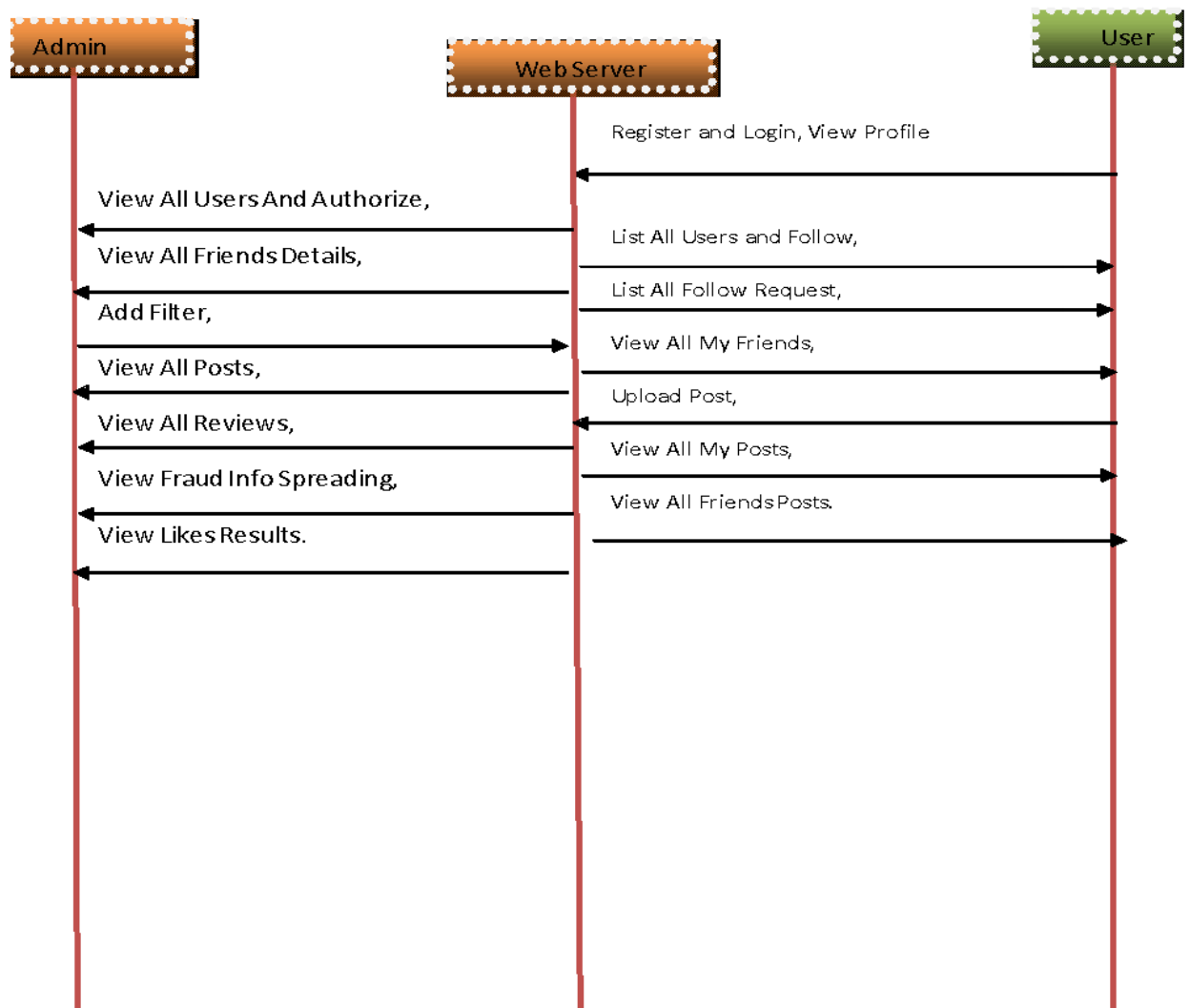


Fig 6.2.3 Sequence Diagram

6.2.4. COLLABORATION DIAGRAM:

A collaboration diagram groups together the interactions between different objects. The interactions are listed as numbered interactions that help to trace the sequence of the interactions. The collaboration diagram helps to identify all the possible interactions that each object has with other objects.

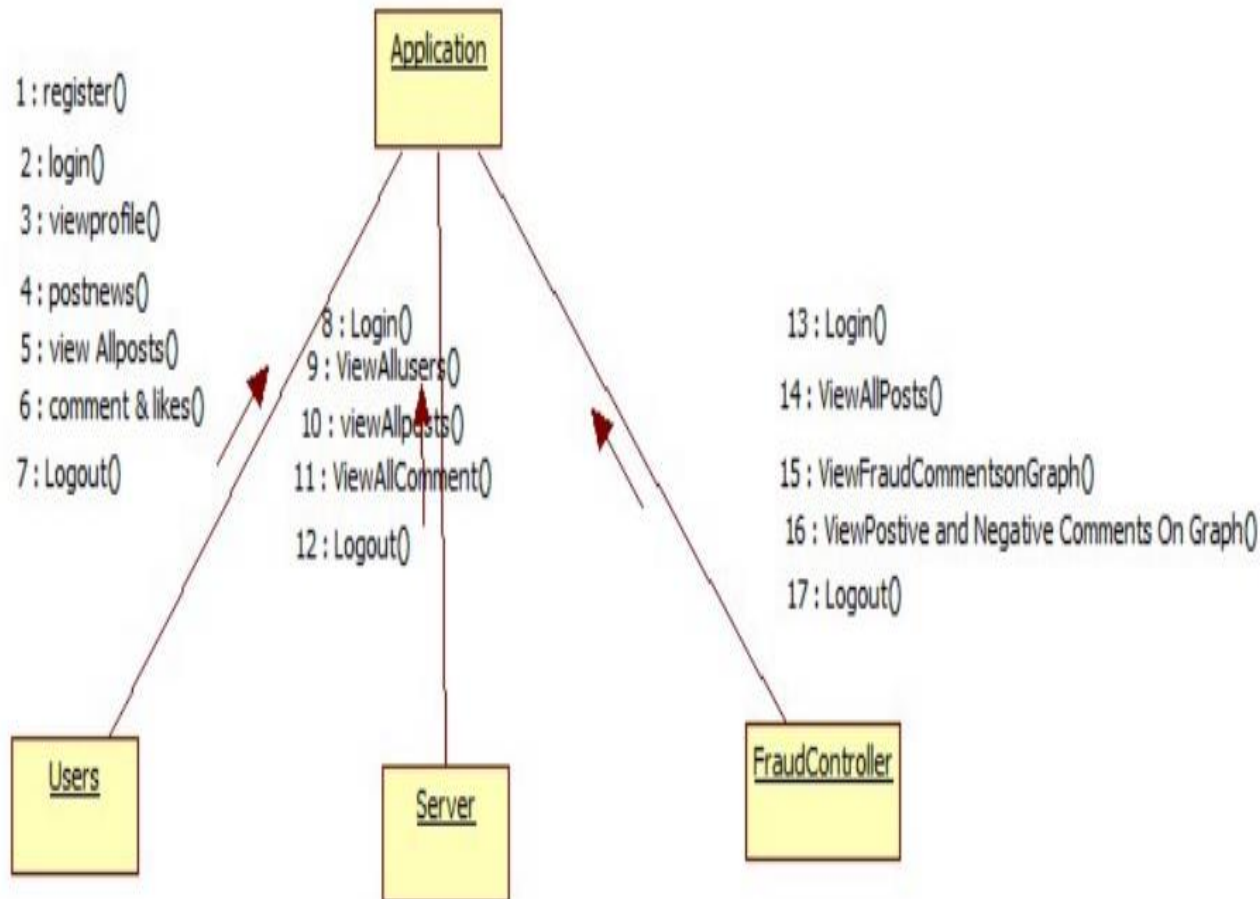


Fig 6.2.4 Collaboration Diagram

6.2.5.ACTIVITY DIAGRAM:

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states,and guard conditions.

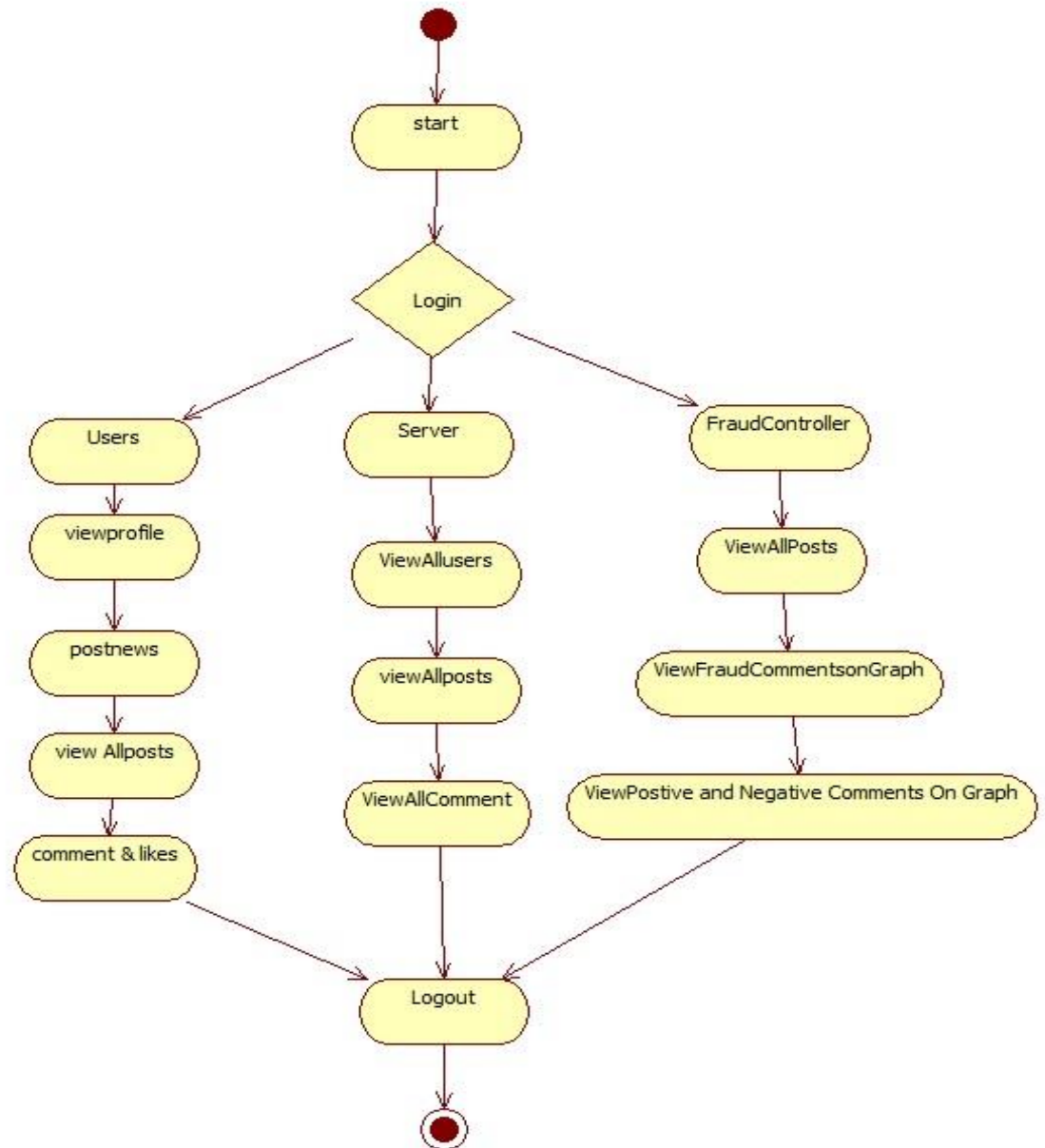


Fig.6.2.5.ActivityDiagram

CHAPTER 7

INPUT AND OUTPUT DESIGN

7.1 INPUT DESIGN

The input design connects information systems with their consumers. It includes the formulation of requirements and procedures for data preparation, which can be performed by inspecting the computer to read data from a written or printed document or by having people directly enter the data into the system. Consequently, input has been made to be as efficient as feasible while also being user-friendly. That way, the input is protected while also being accessible and private. Input Design considers the following factors: What kind of data is needed? What is the best way to code or organize the data? The conversation in which the operating staff is instructed on how to offer input is called the input dialog. What to do if the input validation fails and an error occurs

INPUT OBJECTIVES

To begin, you need to gather data. The term "design" refers to the process of taking a user-oriented description of an input and turning it into a computer-based system. In order to prevent data input errors and lead management in the appropriate direction for receiving reliable information from a computerized system, this design is essential.

Increase the efficiency of data entry by designing intuitive user interfaces. Input design's goal is to minimize the possibility of human error when entering data. Because of the design of the data entry panel, any data manipulation is feasible. Additionally, it's capable of presenting previously saved data. The system will check to see if the data entered is correct. Data can be entered on a screen. Users don't get lost in the shuffle since messages are provided at the appropriate time. Because of this, input design's major objective is to create a user-friendly layout

deciding on the aesthetic of the finished product :In order to be considered high-quality, a product must both meet the needs of its intended audience and make the information it

contains easily understandable to the general public. Any system's outputs are how other systems and users get their hands on the outcomes of processing. Production design dictates how the information is to be disseminated for immediate usage and hard copy output. It's here where the user gets most of their information from. To strengthen the connection between a system and its user, a more efficient and intelligent approach to the output design is employed. Computer output design must take several factors into mind, such as ensuring that each item of output is made in a way that the system is simple and effective to use. Analyzing computer output should be able to tell you exactly what you need to complete a project

Make a decision on the best way to show the facts

The process of putting together system-generated data to create documents and reports. The output form of an information system should accomplish one or more of the following objectives. Provide information on the organization's present or historical activities, state, or prospects for the future. the time in which things will happen.

Indicate the importance of noteworthy happenings, possibilities, problems, or warnings.
Begin a new procedure

7.2 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the

Requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the Future
- ❖ Trigger an action.
- ❖ Confirm an action

CHAPTER 8

IMPLEMENTATION

8.1 MODULES

The major modules of the project are

- 1.User
- 2.Server
- 3.Fraud controller

8.2 MODULE DESCRIPTION

1.User :

The Users module forms the foundation of user interaction with the platform. It begins with a streamlined registration process where users create their accounts by providing essential details, such as their name, email, and password. Once registered, users can log in to their accounts securely using their credentials. After successful login, they are greeted with a dashboard that offers multiple functionalities. One of the primary features is the ability to view and update their profile. This feature allows users to keep their information accurate and stay engaged with the platform. Additionally, users can post news articles or updates, contributing to the platform's dynamic content ecosystem. Each post can include titles, descriptions, and even multimedia elements like images or videos.

An important aspect of user interaction is the ability to engage with existing content through comments. Users can share their thoughts, opinions, or feedback on various posts, fostering a sense of community. The comments section allows for meaningful discussions while maintaining transparency and accountability. To ensure privacy and security, users can log out of their accounts with a single click, securely ending their sessions. This module is designed to create a user-friendly experience, balancing functionality and security to keep users engaged and active on the platform.

2.Server

The Server module serves as the administrative core, providing the tools and features required to oversee and manage the platform effectively. Unlike users, the server administrator does not need to register and can log in directly with predefined credentials. Once logged in, the server admin gains comprehensive control over the system. One of the primary features is the ability to view all registered users. This includes not only their basic information but also insights into their activity on the platform, such as posts created or comments made. This allows the admin to monitor user engagement and detect any unusual patterns of behavior. Another critical feature of the server module is its capacity to review all posts and comments shared by users. The admin can sort, filter, and even flag content that violates the platform's rules or guidelines. This ensures that the platform maintains a high standard of content quality and remains a safe space for all participants. The server module also simplifies administrative tasks with its intuitive interface, helping administrators manage the system efficiently. At the end of their session, administrators can securely log out, ensuring that sensitive data remains protected.

3.Fraud Controller

The Fraud Controller module is integral to the platform's security and integrity, focusing on identifying and addressing fraudulent or inappropriate content. With predefined credentials, the fraud controller can directly log in to the application and access a suite of powerful tools for content analysis. One of the standout features is the ability to analyze user comments and detect fraudulent activities. This analysis is visually represented on interactive graphs, allowing the fraud controller to spot patterns, trends, or suspicious behavior at a glance. This visualization provides actionable insights, enabling quick responses to potential issues.

Together, these modules—Users, Server, and Fraud Controller—operate in harmony to deliver a robust, interactive, and secure platform. The Users module promotes engagement and interaction, the Server module ensures smooth operation and content regulation, and the Fraud Controller module safeguards the platform against misuse. This modular design ensures that the platform is both user-centric and administratively efficient, creating an ecosystem where users can freely contribute while maintaining trust and secure

CHAPTER 9

SOFTWARE ENVIRONMENT

9.1 JAVA

Java technology is both a programming language and a platform. The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platformindependent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.

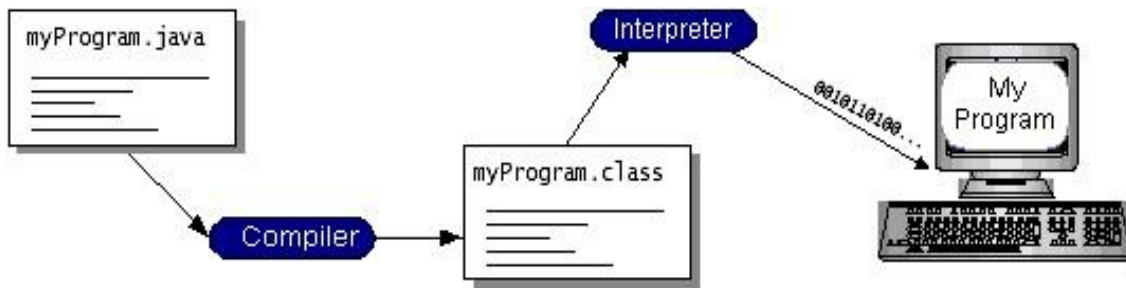


Fig 9.1.1 Java Interpreter

You can think of Java byte codes as the machine code instructions for the *Java* Virtual Machine (Java VM). Every Java interpreter, whether it's a development tool or a Web browser that can run applets, is an implementation of the Java VM. Java byte codes help make “write once, run anywhere” possible.



Fig 9.1.2 Java Compiler

The Java Platform

A platform is the hardware or software environment in which a program runs.

We've already mentioned some of the most popular platforms like Windows 2000,

Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The Java platform has two components:

- The Java Virtual Machine (Java VM)
- The Java Application Programming Interface (Java API)

You've already been introduced to the Java VM. It's the base for the Java platform and is ported onto various hardware-based platforms. The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as *packages*. The next section, What Can Java Technology Do? Highlights what functionality some of the packages in the Java API provide.

The following figure depicts a program that's running on the Java platform. As the figure shows, the Java API and the virtual machine insulate the program from the hardware.

What Can Java Technology Do

The most common types of programs written in the Java programming language are applets and applications. If you've surfed the Web, you're probably already familiar with applets. An applet is a program that adheres to certain conventions that allow it to run within a Java-enabled browser. However, the Java programming language is not just for writing cute, entertaining applets for the Web. The general-purpose, high-level Java programming language is also a powerful software platform. Using the generous API, you can write many types of programs. An application is a standalone program that runs directly on the Java platform. A special kind of application known as a *server* serves and supports clients on a network. Examples of servers are Web servers, proxy servers, mail servers, and print servers. Another specialized program is a *servlet*. A servlet can almost be thought of as an applet that runs on the server side. Java Servlets are a popular choice for

building interactive web applications, replacing the use of CGI scripts. Servlets are similar to applets in that they are runtime extensions of applications. Instead of working in browsers, though, servlets run within Java Web servers, configuring or tailoring the server.

How does the API support all these kinds of programs? It does so with packages of software components that provides a wide range of functionality. Every full implementation of the Java platform gives you the following features:

- **The essentials:** Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, and so on.
- **Applets:** The set of conventions used by applets.
- **Networking:** URLs, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) sockets, and IP (Internet Protocol) addresses.
- **Internationalization:** Help for writing programs that can be localized for users worldwide. Programs can automatically adapt to specific locales and be displayed in the appropriate language.
- **Security:** Both low level and high level, including electronic signatures, public and private key management, access control, and certificates.
- **Software components:** Known as JavaBeans™, can plug into existing component architectures.
- **Object serialization:** Allows lightweight persistence and communication via Remote Method Invocation (RMI).
- **Java Database Connectivity (JDBC™):** Provides uniform access to a wide range of relational databases.

The Java platform also has APIs for 2D and 3D graphics, accessibility, servers, collaboration, telephony, speech, animation, and more. The following figure depicts what is included in the Java 2 SDK.

JAVA DATABASE CONNECTIVITY

The JDBC API only defines interfaces for objects used for performing various database-related tasks like opening and closing connections, executing SQL commands, and retrieving the results. We all write our programs to interfaces and not implementations. Either the resource manager vendor or a third party Provides the implementation classes for the standard JDBC interfaces. These software implementations are called JDBC drivers. JDBC drivers transform the standard JDBC calls to the external resource manager-specific API calls. The diagram below depicts how a database client written in java accesses an external resource manager using the JDBC API and JDBC driver: Depending on the mechanism of implementation, JDBC drivers are broadly classified into four types.

TYPE1:

Type1 JDBC drivers implement the JDBC API on top of a lower level API like ODBC. These drivers are not generally portable because of the independency on native libraries. These drivers translate the JDBC calls to ODBC calls and ODBC sends the request to external data source using native library calls. The JDBC-ODBC driver that comes with the software distribution for J2SE is an example of a type1 driver.

TYPE2:

Type2 drivers are written in mixture of java and native code. Type2 drivers use vendors specific native APIs for accessing the data source. These drivers transform the JDBC calls to vendor specific calls using the vendor's native library. These drivers are also not portable like type1 drivers because of the dependency on native code.

TYPE3:

Type3 drivers use an intermediate middleware server for accessing the external data sources. The calls to the middleware server are database

independent. However, the middleware Server makes vendor specific native calls for accessing the data source. In this case, the driver is purely written in java.

TYPE4:

Type4 drivers are written in pure java and implement the JDBC interfaces and translate the JDBC specific calls to vendor specific access calls. They implement the data transfer and network protocol for the target resource manager. Most of the leading database vendors provide type4 drivers for accessing their data

JAVA SERVER PAGES (JSP)

INTRODUCTION:

Java Server Pages (JSP) technology enables you to mix regular, static HTML with dynamically generated content. You simply write the regular HTML in the normal manner, using familiar Web-page-building tools. You then enclose the code for the dynamic parts in special tags, most of which start with `<%` and end with `%>`

THE NEED FOR JSP:

Servlets are indeed useful, and JSP by no means makes them obsolete.

However,

- It is hard to write and maintain the HTML.
- You cannot use standard HTML tools.
- The HTML is inaccessible to non-Java developers.

BENEFITS OF JSP:

JSP provides the following benefits over servlets alone:

- It is easier to write and maintain the HTML: In this no extra backslashes, no double quotes, and no lurking Java syntax.
- You can use standard Web-site development tools:

We use Macromedia Dreamweaver for most of the JSP pages. Even HTML tools that know nothing about JSP can be used because they simply ignore the JSP tags.

- You can divide up your development team:

The Java programmers can work on the dynamic code. The Web developers can concentrate on the representation layer. On large projects, this division is very important. Depending on the size of your team and the complexity of your project, you can enforce a weaker or stronger separation between the static HTML and the dynamic content.

CREATING TEMPLATE TEXT:

A large percentage of our JSP document consists of static text known as template text. In almost all respects, this HTML looks just like normal HTML follows all the

Same syntax rules, and simply “passed through” to that client by the servlet created to handle the page. Not only does the HTML look normal, it can be created by whatever tools you already are using for building Web pages.

There are two minor exceptions to the “template text passed through” rule. First, if you want to have `<% Or %>` in the output, you need to put `<\% or %\>` in the template text. Second, if you want a comment to appear in the JSP page but not in the resultant document,

`<%-- JSP Comment -- %>` HTML comments of the form:

`<!--HTML Comment -->`

are passed through to the client normally.

TYPES OF JSP SCRIPTING ELEMENTS:

JSP scripting elements allow you to insert Java code into the servlet that will be generated from the JSP page. There are three forms:

1. **Expressions** of the form `<%=Java Expression %>`, which are evaluated and inserted into the servlet’s output.
2. **Scriptlets** of the form `<%Java code %>`, which are inserted into the servlet’s `_jspService` method (called by service).
3. **Declarations** of the form `<%! Field/Method Declaration %>`, which are inserted into the body of the servlet class, outside any existing method

USING JSP EXPRESSIONS:

A JSP element is used to insert values directly into the output. It has the following form:

`<%= Java Expression %>`

The expression is evaluated, converted to a string, and inserted in the page. This evaluation is performed at runtime (when the page is requested) and thus has full access to the information about the request. For example, the following shows the date/time that the page was requested.

Current time: `<%=new java.util.Date () %>`

PREDEFINED VARIABLES:

To simplify expressions we can use a number of predefined variables (or “implicit objects”). The specialty of these variables is that, the system simply tells what names it will use for the local variables in `_jspService`. The most important ones of these are:

- **request**, the `HttpServletRequest`.
- **response**, the `HttpServletResponse`.
- **session**, the `HttpSession` associated with the request
- **out**, the writer used to send output to clients.
- **application**, the `ServletContext`. This is a data structure shared by all servlets and JSP pages in the web application and is good for storing shared data.

Here is an example : Your hostname: `<%= request.getRemoteHost () %>`

TOMCAT

Tomcat 9.0 web server

Tomcat is an open source web server developed by Apache Group. Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Web Servers like Apache Tomcat support only web components while an application server supports web components as well as business components (BEAs Weblogic, is one of the popular application server). To develop a web application with jsp/servlet install any web server like JRun, Tomcat etc to run your application.

TERMINOLOGY:

Context – a Context is a web application.

\$CATALINA_HOME – This represents the root of Tomcat installation.

DIRECTORIES AND FILES:

/bin – Startup, shutdown, and other scripts. The *.sh files (for Unix systems) are functional duplicates of the *.bat files (for Windows systems). Since the Win32 command-line lacks certain functionality, there are some additional files in here.

/conf – Configuration files and related DTDs. The most important file in here is `server.xml`. It is the main configuration file for the container.

/logs – Log files are here by default.

9.2 SOURCE CODE

9.1.A_Add_Filter.jsp

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Admin</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript"
src="js/droid_sans_400-droid_sans_700.font.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<style type="text/css">
<!--
.style1 {font-size: 36px}
.style2 {color: #FFFFFF}
.style4 {font-weight: bold}
.style5 {
    color: #FF0000;
    font-size: 18px;
    font-weight: bold;
}
.style7 {color: #000000}
-->
</style>
</head>
<body>
<div class="main">
    <div class="header">
        <div class="header_resize">
            <div class="logo">
                <h1><a href="index.html"><span class="style1">Dynamic Control of Fraud
Information Spreading
in Mobile Social Networks</span></a></h1>
            </div>
            <div class="clr"></div>
            <div class="menu_nav">
                <ul>
                    <li><a href="index.html"><span>Home Page</span></a></li>
                    <li class="active"><a href="A_Login.jsp"><span>Admin</span></a></li>
                    <li><a href="U_Login.jsp"><span>Mobile User</span></a></li>
                </ul>
            </div>
            <div class="clr"></div>
            <div class="slider">
                <div id="coin-slider"> <a href="#"><span><big>Dynamic Control of Fraud Information Spreading
in Mobile Social Networks</big></span></a> <a href="#"><span><big>Dynamic Control of Fraud Information
Spreading
in Mobile Social Networks</big></span></a> <a href="#"><span><big>Dynamic Control of Fraud Information
Spreading
in Mobile Social Networks</big></span></a> </div>
                <div class="clr"></div>
            </div>
        </div>
    </div>
</div>
```

```

        </div>
        <div class="clr"></div>
    </div>
</div>
<div class="content">
    <div class="content_resize">
        <div class="mainbar">
            <p>&nbsp;</p>
            <p>&nbsp;</p>
            <h2>Add Filter Details...</h2>
            <p>&nbsp;</p>
            <form id="form1" name="form1" method="post" action="A_Add_Filter1.jsp">
                <p>&nbsp;</p>
                <table width="385" border="2">
                    <tr>
                        <td width="181" height="47" bgcolor="#FF0000"><span class="style2
style11"><strong>Select Filter Category </strong></span></td>
                        <td width="186"><select name="fcat">
                            <option>----Select----</option>
                            <option>Fraud</option>

                                </select>                                </td>
                    </tr>
                    <tr>
                        <td height="52" bgcolor="#FF0000"><span class="style2
style11"><strong>Enter Filter Name </strong></span></td>
                        <td><input type="text" name="fname" /></td>
                    </tr>
                    <tr>
                        <td height="52">&nbsp;</td>
                        <td><p>
                            <input type="submit" name="Submit" value="Add" />
                            <input type="reset" name="Submit2" value="Reset" />
                        </p></td>
                    </tr>
                </table>
                <p>&nbsp;</p>
                <p><a href="AdminMain.jsp"></a></p>
                <p class="style13 style5">Existing Filter Details .... </p>
            </form>

            <%@ include file="connect.jsp" %>
            <table width="379">
                <tr bgcolor="#99CCCC">
                    <td width="186" bgcolor="#FF0000">
                        <p align="center" class="style2"><strong>Filter Category</strong></p>
                    </td>
                    <div align="center"></div>
                </tr>
                <tr>
                    <td bgcolor="#FF0000">
                        <p align="center" class="style2"><strong>Filter Name </strong></p>
                    </td>
                    <div align="center"></div>
                </tr>
            </table>

            <%

```

```

String s0="",s1="",s2="",s3="",s4="",s5="",s6="";
int i=1,j=0,count=0,rank=0,k=0;

try
{
    String query="select * from filter ";
    Statement
st=connection.createStatement();
    ResultSet rs=st.executeQuery(query);
    while ( rs.next() )
    {
        s0=rs.getString(1);
        s1=rs.getString(2);

        %>
        <tr>
        <td height="33" valign="middle" bgcolor="#00FFFF">
        <div align="center" class="style4 style12 style14 style8 style7"
>
        <div align="center">
        <%out.println(s0);%>
        </div>
        </div></td>

        <td width="181" height="33" valign="middle" bgcolor="#00FFFF">
        <div align="center" class="style4 style12 style14 style9 style7"
>
        <div align="center">
        <%out.println(s1);%>
        </div>
        </div></td>
        </tr>
        <%

        }
        connection.close();
    }
    catch(Exception e)
    {
        out.println(e.getMessage());
    }

    %>

</table>

<p>&nbsp;</p>
<p>&nbsp;</p>
</div>
<div class="sidebar">

```


CHAPTER10

RESULTS

10. 1 SYSTEM TESTING

Testing

The eighth step is system testing.

Testing is a must in order to discover errors. Testing is the practice of looking for any and all flaws or vulnerabilities in a product. This method can be used to verify the performance of components, subassemblies, assemblies, and finished products. Testing software to see if it does what it's supposed to do.

The software system's specs and user expectations have no undesirable faults. There is a wide range of testing options. For each kind of test, there's a certain purpose for which it was created.

The methods of assessment

Each unit must be tested individually.

If you want to make sure your software works as expected and that your inputs and outputs are valid, you utilize unit testing. Ensure that all code paths and decision points are tested thoroughly. An application's software components are tested separately.. Each individual unit must be completed before integration may take place. These are structural tests, which demand an intrusive process and require knowledge of its construction. Unit tests are conducted at the component level to check a specific business process, application, or system configuration. Unit tests are one method of verifying that a business process adheres to its documented criteria.

Implementation and evaluation of results

If two or more pieces of software can actually work together as a single entity, an integration test is needed. The outcomes of screens and fields are more important in an

event-driven testing methodology. It is important to do integration tests in order to make sure that all of the components work together in a logical and consistent manner. Integration testing is used to detect the difficulties that arise when two or more components are combined.

TEST CASE DESIGN:

Black Box Testing

It is the process of testing software without having any understanding of the module being tested, its underlying structure, language, or design. For black box testing to be effective it must come from a clear source document, such as a specification or requirements document. The term "black box testing" refers to software testing in which the program under test is treated as a mystery. One cannot "see" inside. Tests are conducted only on input and outputs, not on the underlying software.

When it comes to the 8.2unit tests,

During the software development process, unit testing and coding may be accomplished at the same time. It is also possible to segregate unit testing from other testing.

It is imperative that strategies and tactics be put to the test.

Detailed functional tests will be written up for future reference during field testing.

The test's aims and objectives

There should be no mistakes in the data.

Only by clicking on the link supplied will you be able to view the requested pages.

Sending a message or entering data shouldn't necessitate any sort of wait time on your end.

The features will be put through their paces in testing.

Make that the data is in the correct format by performing an audit on it.

No more than one entry should be allowed in the database.

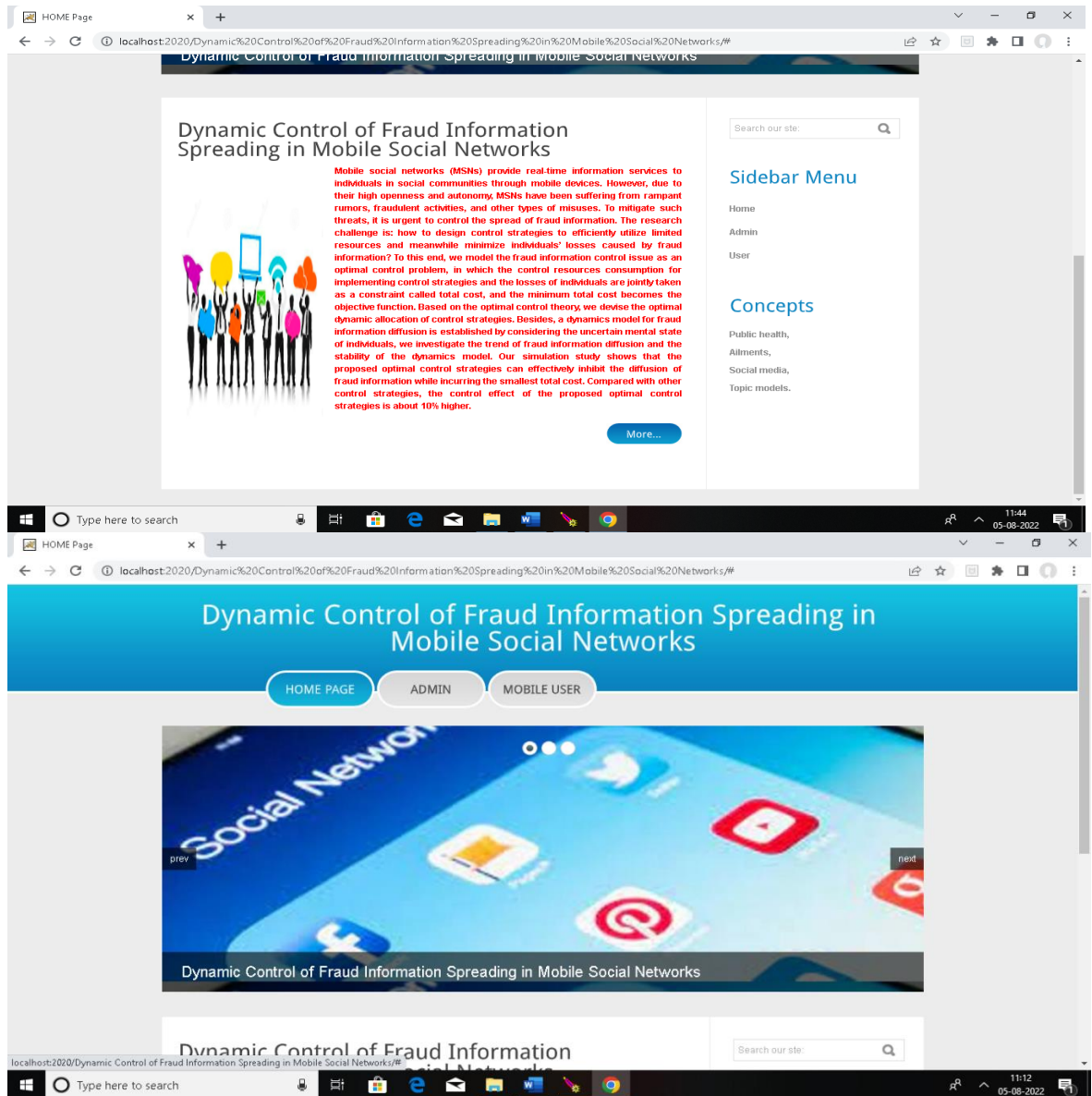
Every link needs to point to the appropriate page.

8.3 Integrity testing of the various parts

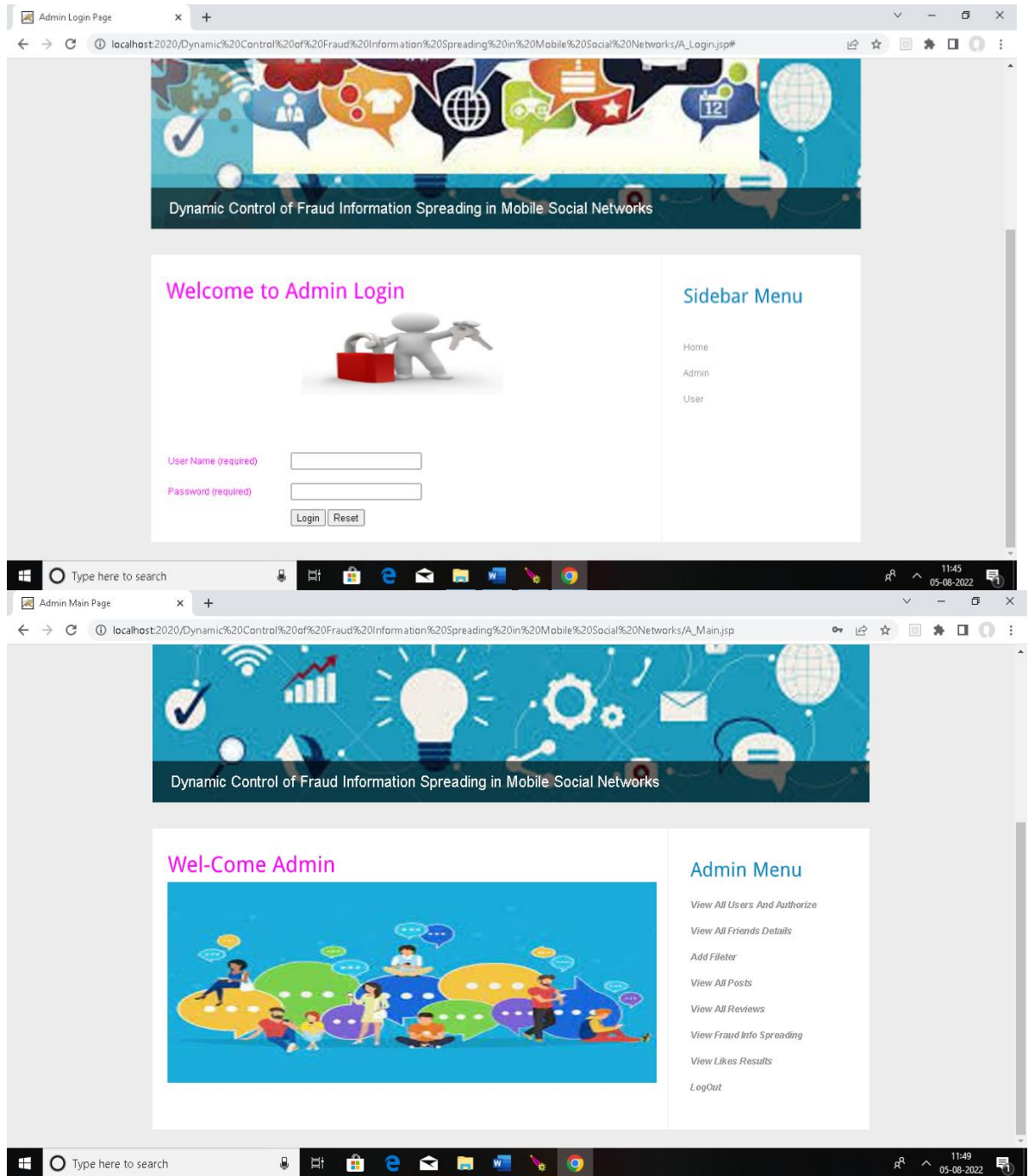
Software integration testing refers to the process of integrating software components one at a time to look for interface issues that could lead to problems.

In an integration test, the primary purpose is to ensure that all of the components of a system or company-wide software application interact with each other of the above-mentioned tests went perfectly. Everything as it should.

10.2 OUTPUT SCREENS




Screen 1 : Application Window



Screen 2 : Admin Login

User Registration Form



User Name :

Password :

Email :

Mobile :

DOB :

Gender :

Address :

Current Living Region :

Blood Group :


Company Name :

Choose Photo : No file chosen

Screen 3 :User Registration

Dynamic Control of Fraud Information Spreading in Mobile Social Networks

Welcome to User Login



User Name (required) :

Password (required) :

New User [Click Here To Register](#)

Sidebar Menu






- Home
- Admin
- User

Screen 4: User Login

Admin

localhost:2020/Dynamic%20Control%20of%20Fraud%20Information%20Spreading%20in%20Mobile%20Social%20Networks/A_View_All_Posts.jsp

VIEW ALL USERS POSTS !!!

| Id | Uploaded User | Post Name | Post Image | Post Uses | Post Description | Article Name | Post Category | Post Score | Post Date |
|----|---------------|-----------|---|-------------|--|--------------|----------------|------------|---------------------|
| 1 | m.vinay | be alert |  | nothing | evrything | something | World News | 0 | 29/07/2022 15:19:00 |
| 2 | m.vijay | vij |  | fraud msg | fraud | vinj19 | Social Message | 0 | 29/07/2022 15:22:09 |
| 3 | v.bhanu | function |  | | enjoy the day detailing when you have function | something | Entertainment | 0 | 30/07/2022 11:34:23 |
| 4 | v.bhanu | duplicate |  | nothing | due covid 19 exams postponed | something | World News | 0 | 01/08/2022 12:18:04 |
| 5 | m.vinay | covid |  | health care | covid 19 cases are increased | vin19 | World News | 0 | 04/08/2022 10:28:52 |

Sidebar Menu

- Admin Home
- Logout

Type here to search

12:36 05-08-2022

Screen 5: User Posts



Admin

localhost:2020/Dynamic%20Control%20of%20Fraud%20Information%20Spreading%20in%20Mobile%20Social%20Networks/A_View_Fraud_Info_Spreading.jsp

SOCIAL NETWORKS

Dynamic Control of Fraud Information Spreading in Mobile Social Networks

View Fraud Information Spreading !!!

| Id | Uploaded User | Post Name | Post Image | Post Uses | Post Description | Article Name | Post Category | Post Score | Post Date |
|----|---------------|-----------|---|-----------|------------------------------|--------------|----------------|------------|---------------------|
| 0 | m.vijay | vij |  | fraud msg | fraud | vinj19 | Social Message | 0 | 29/07/2022 15:22:09 |
| 0 | v.bhanu | duplicate |  | nothing | due covid 19 exams postponed | something | World News | 0 | 01/08/2022 12:18:04 |

[Back](#)

Sidebar Menu

- Admin Home
- Logout

Type here to search

12:42 05-08-2022

Screen 6: fraud information spreading

CHAPTER 11

CONCLUSION

The goal of this paper is to put forward the optimal control strategies to efficiently utilize limited control resources and minimize losses of individuals caused by the diffusion of fraud information. First, a novel SWIR dynamics model is proposed to describe the dynamic evolutionary process of fraud information diffusion in MSNs. Thereafter, this paper analyzes and proves the information diffusion trends and stability of the dynamics model. In particular, this paper proposes two synergistic control strategies to suppress the spread of fraud information, and derives the optimal dynamic allocation of the control strategies. Finally, we validate the efficiency of our proposed diffusion model and optimal control strategies in both synthetic datasets and real social network datasets. This paper can provide a theoretical basis and a feasible technical approach for the applications of controllable information diffusion based on MSNs, and further promote the development and application of information diffusion and optimal control technology in MSNs. In the future, we will further study the diffusion modeling and control of coupling of positive and negative information. In addition, we will also study the impact of users' social identity cognition on information diffusion

CHAPTER 12

REFERENCES

- [1] M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang, "Online task assignment for crowdsensing in predictable mobile social networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2306–2320, Aug. 2017.
- [2] L. Jiang, J. Liu, D. Zhou, Q. Zhou, X. Yang, and G. Yu, "Predicting the evolution of hot topics: A solution based on the online opinion dynamics model in social network," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.
- [3] Y. Lin *et al.*, "An on-demand coverage based self-deployment algorithm for big data perception in mobile sensing networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 220–234, May 2018.
- [4] Y. Wang, A. V. Vasilakos, J. Ma, and N. Xiong, "On studying the impact of uncertainty on behavior diffusion in social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 2, pp. 185–197, Feb. 2015.
- [5] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: A differential game approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1713–1728, Jul. 2019.
- [6] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, Mar. 2017.
- [7] L.-X. Yang, P. Li, X. Yang, Y. Wu, and Y. Y. Tang, "On the competition of two conflicting messages," *Nonlin. Dyn.*, vol. 91, no. 3, pp. 1853–1869, 2018.
- [8] R. Nash, M. Bouchard, and A. Malm, "Investing in people: The role of social networks in the diffusion of a large-scale fraud," *Soc. Netw.*, vol. 35, no. 4, pp. 686–698, 2013.
- [9] R. A. Raub, A. H. N. Hamzah, M. D. Jaafar, and K. N. Baharim, "Using subscriber usage profile risk score to improve accuracy of telecommunication fraud detection," in *Proc. IEEE CYBERNETICSCOM*, 2016, pp. 127–131.
- [10] J. Ma *et al.*, "Detecting rumors from microblogs with recurrent neural networks," in *Proc. IJCAI*, 2016, pp. 3818–3824.
- [11] (Aug. 2016). Tsinghua University Teachers Cheated 17 Million 600Thousand? The Original Liar Used This Psychological Routine! [Online]. Available: <http://www.bestchinanews.com/Domestic/2426.html>
- [12] M. Sahin, "Over-the-top bypass: Study of a recent telephony fraud," in *Proc. ACM CCS*, 2016, pp. 1106–1117.
- [13] K. Zhu and L. Ying, "Information source detection in the SIR model: A sample-path-based approach," *IEEE/ACM Trans. Netw.*, vol. 24, no. 1, pp. 408–421, Feb. 2016.

[14] Z. Chen, K. Zhu, and L. Ying, "Detecting multiple information sources in networks under the SIR model," IEEE Trans. Netw. Sci. Eng., vol. 3, no. 1, pp. 17–31, Jan./Mar. 2016.

[15] A. Y. Khrennikov, Information Dynamics in Cognitive, Psychological, Social, and Anomalous Phenomena, vol. 138. New York, NY, USA:Springer, 2013.

SitesReferred:<http://www.sourcefordgde.com>
<http://www.networkcomputing.com/> <http://www.ieee.org>
<http://www.almaden.ibm.com/software/quest/Resources/>
<http://www.computer.org/publications/dlib>