iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68186

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Suspicious Activity Reporting Portal

Mayuri S. Raut[1], Pratham P. Mohod[2], Harsh P. Rai[3], Prof. Akshda K. Dhakade[4]
[1, 2, 3]U.G. Students, [4]Assistant professor, Department of Computer Science & Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra

Abstract: ***Public procurement, a major sector of government spending, is highly vulnerable to corruption due to its complex and opaque vendor selection processes. To address this, a secure whistleblowing platform has been developed, allowing individuals to anonymously report sensitive information to authorities. The system features two panels: one for government authorities to manage reports and another for whistleblowers to submit tips. It includes robust security measures against malware, phishing, XSS, and SQL injection to ensure data integrity and confidentiality. By using decentralized storage, the platform enhances information security while reducing server costs. Through real-time testing, the system will be refined to meet all requirements, promoting transparency, accountability, and improved public service quality.***

Keywords: Cybercrime, Crime documentation, Real-Time, Anonymous reporting, Suspicious activity detection.

I. INTRODUCTION

In today's world, the rising crime rates present a significant challenge, despite the advancements in technology aimed at combating them. However, a major obstacle in solving crimes is the reluctance of witnesses to come forward due to fear of lengthy legal procedures, potential interrogations, or even retaliation. This project focuses on creating a platform that allows crime witnesses to anonymously submit crime tips, thereby promoting social responsibility without exposing them to risks. The objective of this application is to encourage more citizens to report criminal activities without the fear of being identified. By ensuring complete anonymity, the platform increases public participation in crime reporting. Additionally, the system incorporates a reward mechanism for anonymous tipsters, which serves as an incentive to encourage more individuals to share valuable information.

To enhance data security and reduce storage costs, the platform leverages decentralized storage solutions. This ensures that sensitive crime-related information is securely stored and protected from unauthorized access while also minimizing server expenses. The platform is particularly beneficial to crime investigators and undercover agents who rely heavily on insider information. It offers them a reliable channel to receive tips without compromising the safety of the informants. Overall, this project aims to create a secure, cost-effective, and trustworthy solution that empowers citizens to contribute to crime prevention efforts while preserving their anonymity.

II. LITERATURE REVIEW

With recent advancements in artificial intelligence (AI), machine learning (ML), mobile edge computing (MEC), and the Internet of Things (IOT), AI has emerged as a transformative technology. Traditionally, machine learning models required large volumes of data to be gathered and processed on centralized servers. However, with the rise of decentralized machine learning and MEC, it is now possible to train models directly on IOT devices. By utilizing MEC servers, IOT devices can offload complex training tasks, making AI deployment at the network edge more feasible and efficient. This approach reduces latency, enhances real-time processing capabilities, and minimizes the need for massive data transfers to centralized servers.

However, distributed edge intelligence also brings new challenges, particularly concerning data security and user privacy. To address these issues, blockchain technology is being explored as a potential solution. Blockchain offers a decentralized and immutable ledger, ensuring secure and transparent data management while preventing unauthorized access. By combining IOT, MEC, and blockchain , this approach enhances the security, efficiency, and reliability of AI applications at the network edge, making it a promising framework for future intelligent systems.[1]

Blockchain is a decentralized ledger known for its scalability, privacy, and immutable data records. It ensures trusted automated script execution through smart contracts. However, the rise of quantum computing poses a threat, as quantum algorithms could break current encryption methods. To combat this, researchers are developing quantum-resistant cryptography to secure blockchain networks against future quantum attacks.[2] The study in [1] explores the latest advancements in blockchain-based mobile edge computing (MEC), machine learning, and secure data sharing, along with an introduction to post-quantum blockchain.

With the rapid growth of web technology, massive volumes of data are being generated and shared online. The internet has become a hub for learning, exchanging ideas, and sharing opinions. Social media platforms such as Twitter, Facebook, and Google+ have gained immense popularity, allowing users to express views, engage in discussions, and share messages globally. Sentiment analysis of Twitter data has become a key research area, helping to interpret the unstructured and diverse opinions in tweets. This analysis classifies sentiments into positive, negative, or neutral categories, offering valuable insights into public opinion.[3]

The study in [2] presents a comprehensive survey and comparative analysis of existing opinion mining techniques, including machine learning and lexicon-based approaches, along with evaluation metrics. Various machine learning algorithms, such as Naive Bayes, Maximum Entropy, and Support Vector Machine (SVM), are applied to analyse Twitter data streams. Additionally, the research explores the challenges and practical applications of sentiment analysis on Twitter. This includes addressing issues like data sparsity, slang usage, and the dynamic nature of tweets, while highlighting its significance in areas such as marketing, trend prediction, and public opinion analysis.[4]

In the digital era, numerous documents in various Indian languages are available in digital format. To enable efficient retrieval, these documents need to be categorized based on their content. Text classification, a key area of text mining, addresses this challenge by automatically assigning documents to relevant categories. The study in [3] analyses text classification techniques applied to Indian language content. Since these languages pose unique challenges in natural language processing (NLP), specialized approaches are required. The research reveals that supervised learning algorithms, including Naive Bayes (NB), Support Vector Machine (SVM), Artificial Neural Network (ANN), and N-gram models, deliver superior performance for text classification tasks.[5]Researchers have long suggested that positive perceptions of the police increase citizens' willingness to cooperate with law enforcement. However, this assumption has rarely been tested empirically. The study in [6] examines the link between attitudes toward the police and victims' crime reporting behaviour. It also explores how victims' characteristics influence their decision to report crimes. Using field data from Ghana, the research reveals that victims with greater confidence in the police and higher satisfaction with police services are more likely to report sexual assault and robbery. Additionally, factors such as age, marital status and employment significantly influence victims' reporting behaviour. The study highlights both practical and theoretical implications of these findings.[6]

Non-fungible tokens (NFTs) are unique, indivisible blockchain-based tokens introduced in late 2017. While fungible tokens have facilitated innovations like Initial Coin Offerings (ICOs), the potential of NFTs remains less explored. The study in [8] addresses this gap by investigating the effectiveness of NFTs in event ticketing.Following a design science research approach, the authors design, build, and thoroughly evaluate a prototype NFT-based ticketing system. The study demonstrates how NFTs can tokenize digital goods, prevent fraud, and enhance control over secondary market transactions. It also provides general insights into the benefits and challenges of NFTs, offering valuable implications for researchers and practitioners. Lastly, the study proposes managerial recommendations for developing NFT-based applications and offers design principles to guide future research.[7]

III.ANALYSIS OF PROBLEM

A. Problem Statement

Solving crimes is an incredibly challenging task, and law enforcement agencies often encounter various obstacles. One of the most significant factors affecting their effectiveness is the ability of witnesses and informants to provide accurate and reliable information regarding a suspect's identity and actions. Without this essential input from individuals with knowledge of the crime, it becomes significantly harder to resolve cases. There are several reasons why people may be reluctant to report crimes. In many cases, individuals fear becoming entangled in lengthy legal procedures or facing unwanted attention. Others may avoid reporting more serious offenses, even if they were present at the scene, simply because they were only bystanders and do not wish to be involved. This hesitation to share information can hinder law enforcement’s ability to investigate and solve crimes effectively.

Many individuals prefer to avoid getting involved in legal proceedings, such as going to court or testifying, due to concerns about their safety or that of their families. To address this issue, a solution could be the implementation of a system that allows users to report crimes anonymously through a guest account. This feature would enable individuals to share details of criminal activities without revealing their personal identity. The system could include multiple access levels for effective management. A super admin account would have the authority to access crime reports from across India. Meanwhile, a state admin account would be responsible for monitoring reports specific to cities within their respective states. Additionally, there would be an agent (khabri) account, where authorized users could log in and provide confidential tips directly to the relevant admin. Lastly, a guest page would allow the public to share information anonymously without the need for login credentials. This setup would encourage more people to come forward with crime-related information while protecting their privacy.

B. Proposed Work

There are several reasons why people may be reluctant to report crimes, including:

- Lack of trust in the police: Many individuals hesitate to report incidents due to concerns that the police might investigate their own circumstances rather than focusing on the crime itself.
- Dealing with law enforcement is cumbersome: People often find the process of interacting with the police tedious, especially when they are repeatedly contacted for follow-ups, which can become a hassle.
- Fear of consequences: Even when law enforcement promises anonymity, individuals remain concerned that their names could still appear in records, making them vulnerable to potential risks.

To overcome these challenges, we propose a Tip-off System designed specifically for reporting crime-related activities. The system consists of four key modules:

- Guest Module: This allows users to anonymously upload crime details without revealing their identity.
- Super Admin Module: Enables access to crime reports from across the entire country.
- State Admin Module: Grants access to reports from specific cities within a particular state.
- Agent (Khabri) Module: Allows authorized agents to log in and provide confidential tips directly to the relevant admin. The agent also has the option to post messages publicly through the guest page without requiring a login.

This multi-level system ensures that people can report crimes safely and anonymously, promoting greater public participation in crime prevention.

C. Objectives

The primary objectives of our project are:

- Ensuring user anonymity: Protecting the identity of individuals who provide tips about crimes, allowing them to report without fear of exposure.
- Increasing citizen participation: Encouraging more people to share information by offering a safe and anonymous platform.
- Rewarding valid tips: Offering incentives or rewards to users who provide credible and useful information.
- Enhancing law enforcement insights: Enabling authorities to access detailed and organized reports, aiding in more effective investigations.
- Centralizing crime-related evidence and documentation: Creating a platform where proofs, documents, and related information can be easily stored and accessed.
- Minimizing paperwork: Streamlining the reporting and documentation process by digitizing records, reducing the need for physical paperwork.

IV. SYSTEM ARCHITECTURE

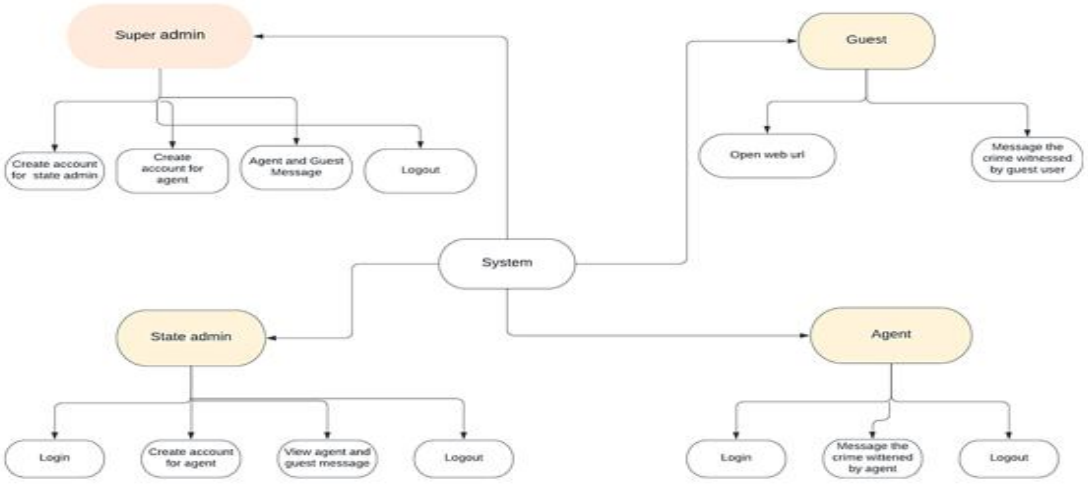


Figure 4.1: System Architecture

The Tip-off Project is designed to tackle the challenges associated with crime reporting, particularly for individuals who witness criminal activities but are reluctant to approach the police due to the fear of becoming involved in lengthy legal procedures. To address this issue, the project introduces a secure and anonymous reporting system, allowing people to share crime-related details without revealing their identity. The system consists of several modules, each serving a specific purpose. The Guest Account allows users to anonymously upload crime information, ensuring their privacy is protected. The Super Admin Acc**ount** grants access to crime reports from across the entire country, providing law enforcement with a comprehensive overview. Meanwhile, the State Admin Account offers access to reports from specific cities within a particular state, enabling more localized monitoring. Additionally, the Agent (Khabri) Account is designed for authorized agents who can log in and submit confidential tips directly to the relevant admin, ensuring streamlined communication. There is also a Guest Page where users can post public messages anonymously without needing to log in, further simplifying the process. By implementing this multi-level system, the Tip-off Project aims to encourage more people to come forward with valuable information while protecting their anonymity. This approach not only boosts public participation but also enhances law enforcement's ability to gather crucial insights, ultimately aiding in more effective crime prevention and investigation.

V. SYSTEM DESIGN

A. Data Flow Diagram Of Guest Module

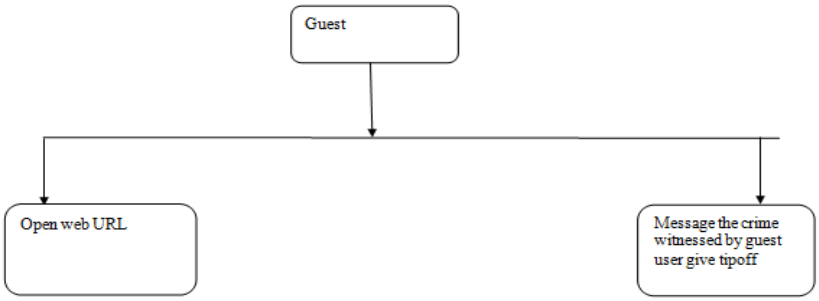


Fig 5.1: Guest Module DFD

The diagram illustrates the Guest Module workflow for a Suspicious Activity Reporting Portal. Here's a breakdown of the process:

1) Guest Node
- This represents the starting point, where a guest user (an anonymous individual) accesses the portal. Since it is a guest module, no login or registration is required, ensuring anonymity.

2) Open Web URL
- From the guest node, one possible action is to open the portal through a web URL. This allows the guest user to access the platform where they can report suspicious activity or crime details.

3) Message the Crime (Tip-off)
- The second action represents the option for the guest to report a crime they have witnessed.
- The guest user can submit a tip-off by describing the incident without revealing their identity. This information is then sent to the relevant authorities for investigation.

B. Data Flow Diagram Of Super Admin Module

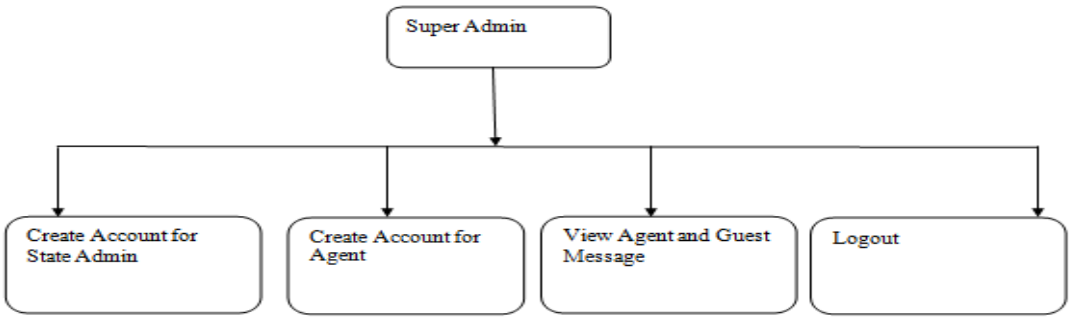


Fig. 5.2 : Super Admin Module DFD

The diagram represents the Super Admin Module Workflow for a Suspicious Activity Reporting Portal. Here's a detailed explanation of each component:

1) Super Admin Node
   - This is the main access point for the Super Admin, who has the highest level of authority in the system.
   - The Super Admin is responsible for managing accounts, monitoring reports, and overseeing the entire system.
2) Create Account for State Admin
   - This option allows the Super Admin to create and manage accounts for State Admins.
   - State Admins have localized access, meaning they can view reports related to specific cities or regions within their state.
3) Create Account for Agent
   - The Super Admin can create and manage agent accounts (Khabri accounts).
   - Agents are authorized users who can submit crime tips and communicate directly with the relevant State Admin.
4) View Agent and Guest Messages
   - This functionality allows the Super Admin to access and review messages submitted by both agents and guest users.
   - The Super Admin can monitor the tips, assess their credibility, and forward them to the appropriate law enforcement authorities.
5) Logout
   - This option allows the Super Admin to end their session and securely log out of the portal.

C. *Data Flow Diagram Of State Admin Module*

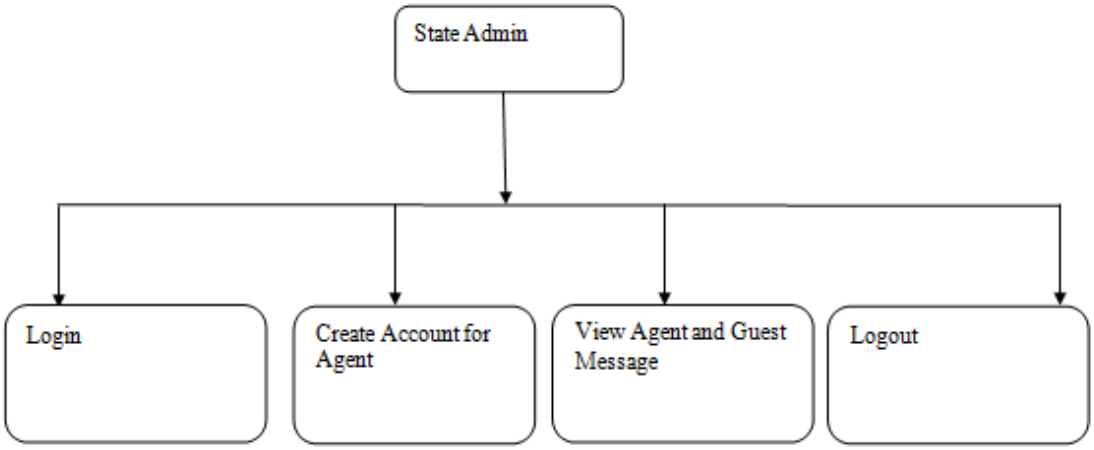


Fig. 5.3 : State Admin Module DFD

The diagram illustrates the State Admin Module Workflow for a Suspicious Activity Reporting Portal. Here's a detailed explanation of each component:

1) State Admin Node
   - This is the main access point for the State Admin, who has administrative control over a specific state.
   - The State Admin manages agent accounts, views reports, and monitors suspicious activity messages related to their region.
2) Login
   - The State Admin logs into the system using their credentials to access the portal.
   - Upon successful login, they gain access to crime reports and other administrative functionalities.
3) Create Account for Agent
   - This option allows the State Admin to create and manage agent (Khabri) accounts.
   - Agents are authorized users who can submit confidential tips to the relevant admin.
   - By creating multiple agent accounts, the State Admin ensures broader coverage and efficient reporting from different regions.

4) View Agent and Guest Messages
- This functionality allows the State Admin to access and review crime tips submitted by both agents and guest users.
- The State Admin can analyze the messages, verify their authenticity, and forward them to law enforcement for investigation.

5) Logout
- This option ends the current session, ensuring the State Admin securely logs out of the system, preventing unauthorized access.

D. Data Flow Diagram Of Agent(Khabari) Module

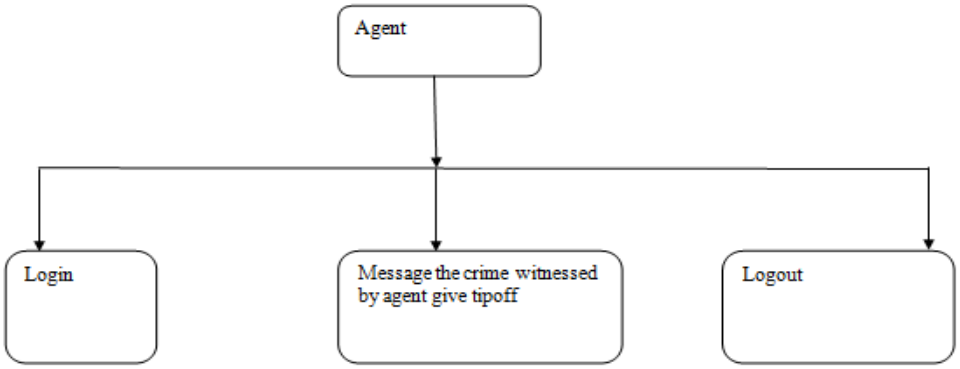


Fig.5.4 : Agent Module DFD

The diagram illustrates the Agent (Khabri) Module Workflow for a Suspicious Activity Reporting Portal. Here's a detailed explanation of each component:

1) Agent Node
- This is the main access point for the Agent, who plays a key role in reporting suspicious activities.
- Agents have authorized access, allowing them to submit tips directly to the relevant admin.

2) Login
- The agent logs into the system using their credentials.
- Once authenticated, they gain access to the tip-off submission feature.

3) Message the Crime Witnessed (Tip-off)
- After logging in, the agent can report any suspicious or criminal activity they have witnessed.
- They submit a tip-off message with details of the incident, which is sent to the respective State Admin or Super Admin for further investigation.
- This module ensures that agents can directly communicate with the admin, streamlining the reporting process.

4) Logout
- The Logout option allows the agent to securely end their session.
- This ensures that no unauthorized person can access their account or submit false reports.

VI. TESTING

Once the software is fully developed, it is deployed in a test environment where the testing team evaluates the functionality of the entire system. This phase is essential to verify that the application meets the customer's requirements and performs as expected. The significance of testing in the software development lifecycle cannot be overlooked. It allows the team to validate both the functional and non-functional aspects of the project, ensuring quality and reliability.

Testing also helps identify whether newly introduced features unintentionally disrupt existing functionality. By catching such issues early, the team can address them before they affect the final product. Early-stage testing makes it easier to detect and fix hidden errors, reducing the cost and complexity of corrections later on. Through thorough testing, major software defects are eliminated, making the final product more robust and competitive.

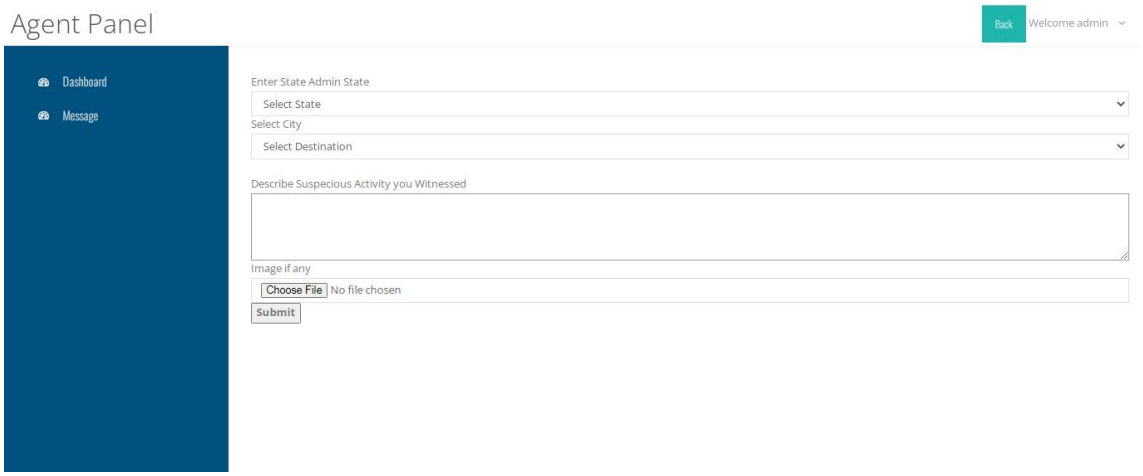
There are various types of software testing, each serving a specific purpose:

1) Acceptance Testing: Ensures that the entire system behaves as intended and meets the client's requirements.
2) Integration Testing: Verifies that different software components or modules function correctly together.
3) Unit Testing: Evaluates individual units of code to confirm they perform as expected. A unit refers to the smallest testable part of an application.
4) Functional Testing: Simulates real-world business scenarios to confirm the application meets functional requirements. Black-box testing is commonly used for this purpose.
5) Performance Testing: Assesses how the software handles different workloads. For example, load testing measures how the system performs under real-life traffic conditions.
6) Regression Testing: Checks whether newly added features affect the existing functionality. Sanity testing can be performed as a quick verification of surface-level functions when there is limited time for a full regression test.
7) Stress Testing: Determines the system's breaking point by applying extreme workloads, helping identify its failure threshold.
8) Usability Testing: Evaluates how easily a customer can navigate and use the application to complete tasks effectively.

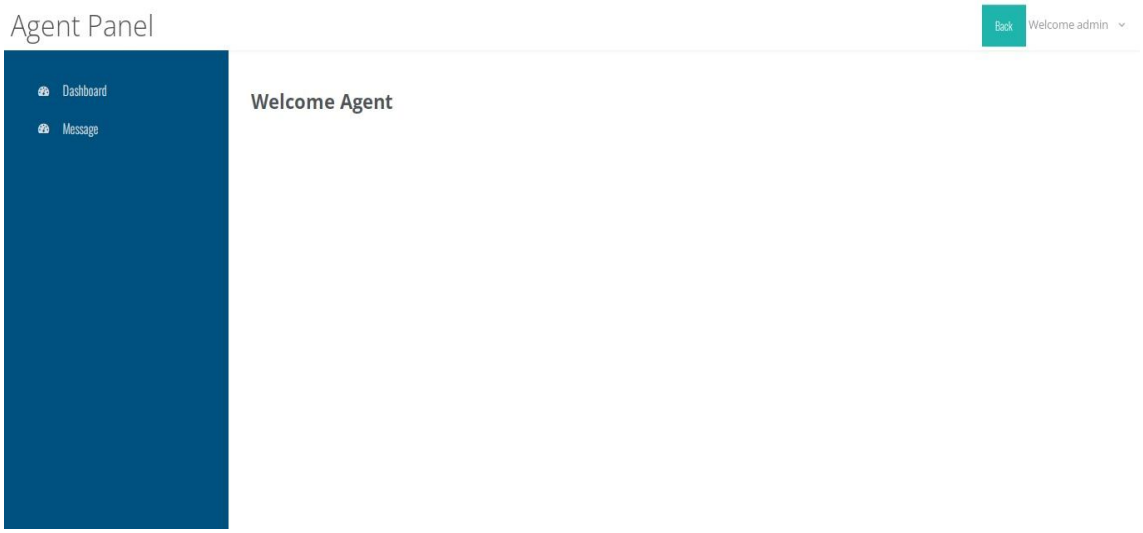
Validating core requirements is crucial during testing. Additionally, exploratory testing helps uncover unpredictable scenarios that could lead to software failures. Even simple applications can require a broad range of tests to identify potential defects. A test management plan helps prioritize the most valuable types of tests based on available time and resources. Optimizing testing efforts by running the fewest tests that detect the largest number of issues enhances the effectiveness of the testing process.

VII. RESULTS

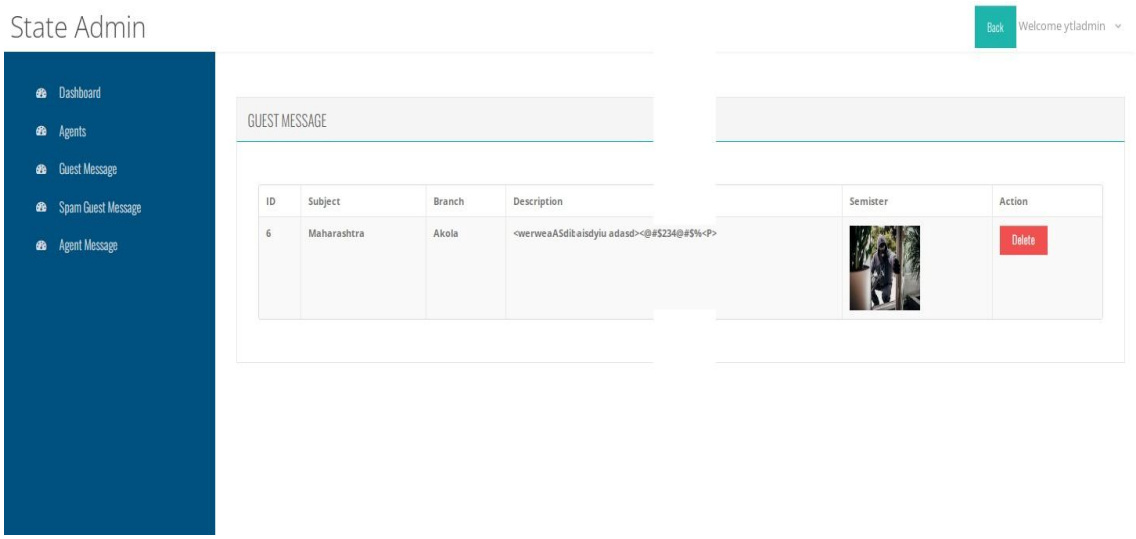
Screenshot 7.1: Home page



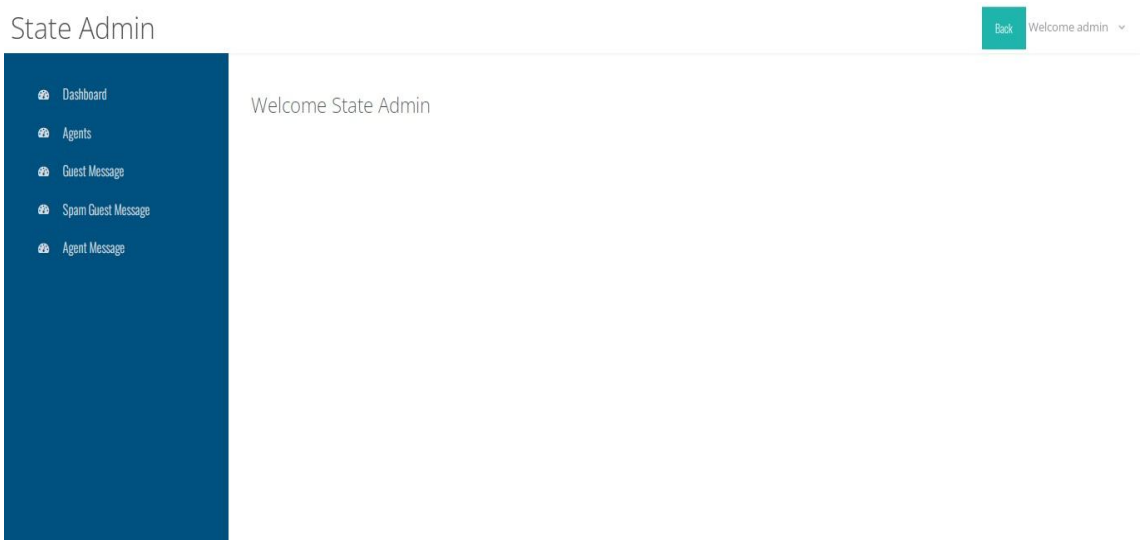
Screenshot 7.2: Form in Agent Panel



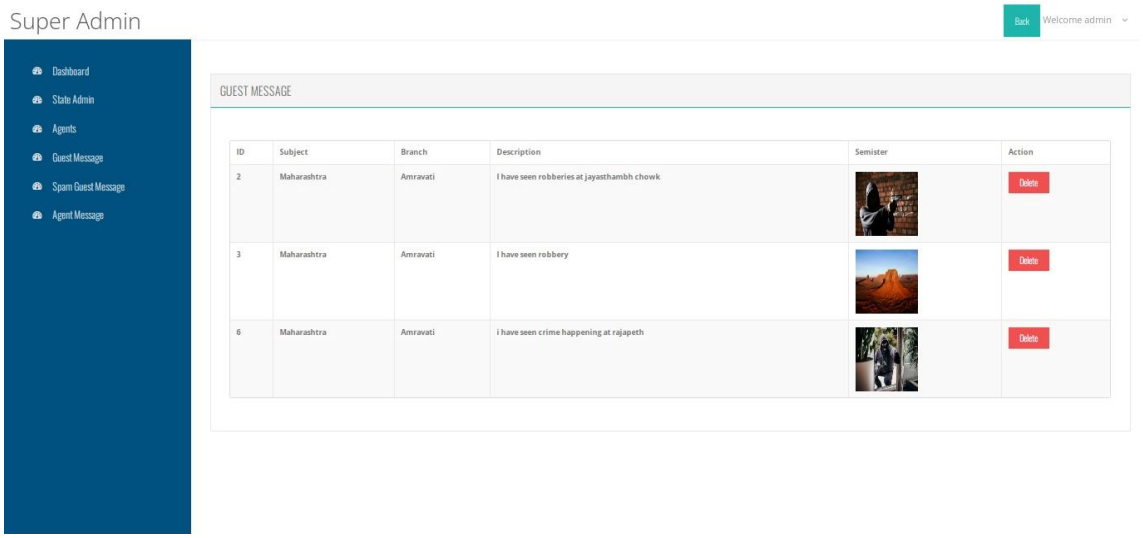
Screenshot 7.3: Agent Panel Dashboard



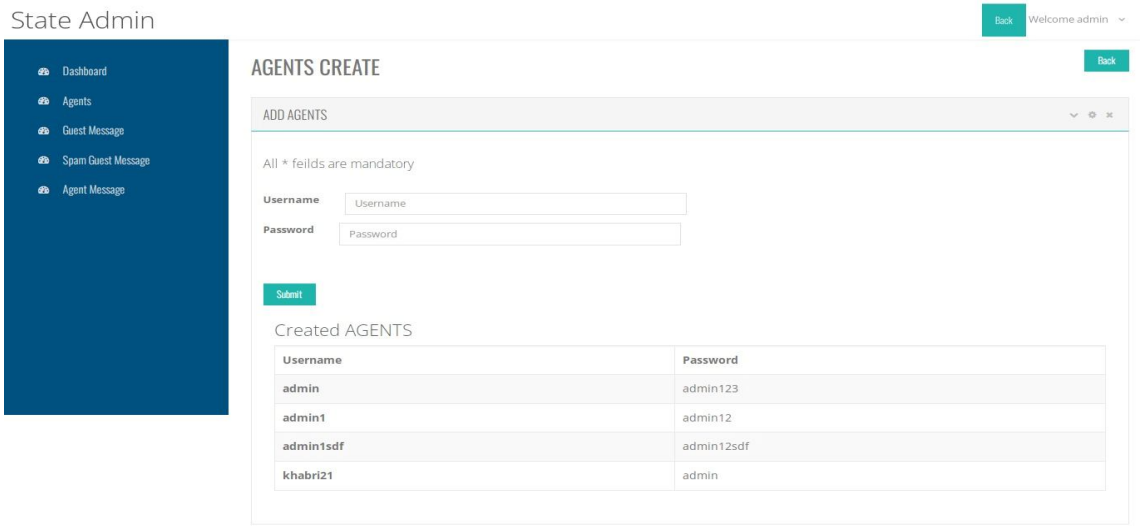
Screenshot 7.4: Guest message



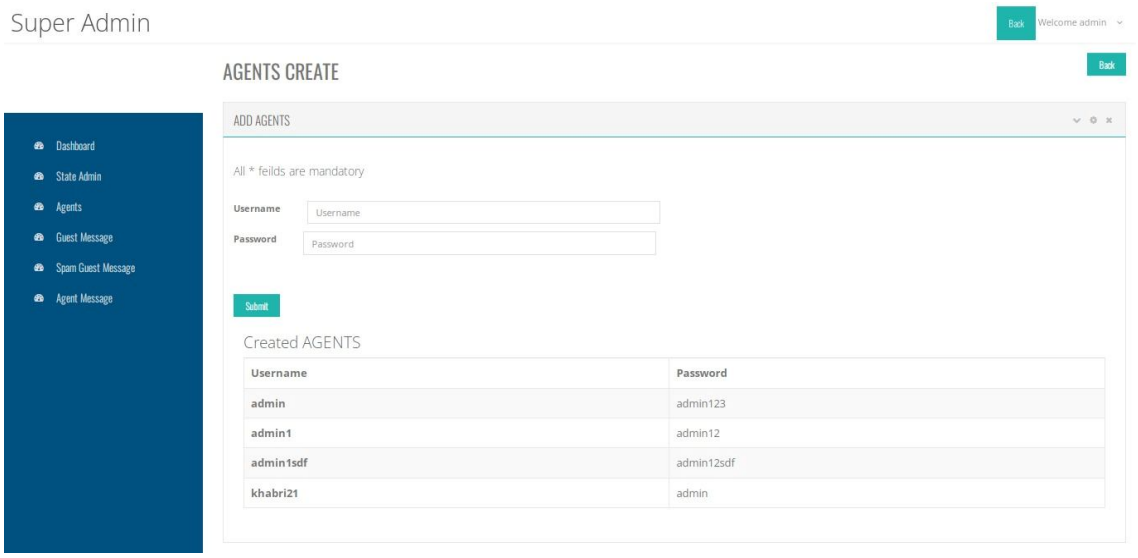
Screenshot 7.5: State Admin page



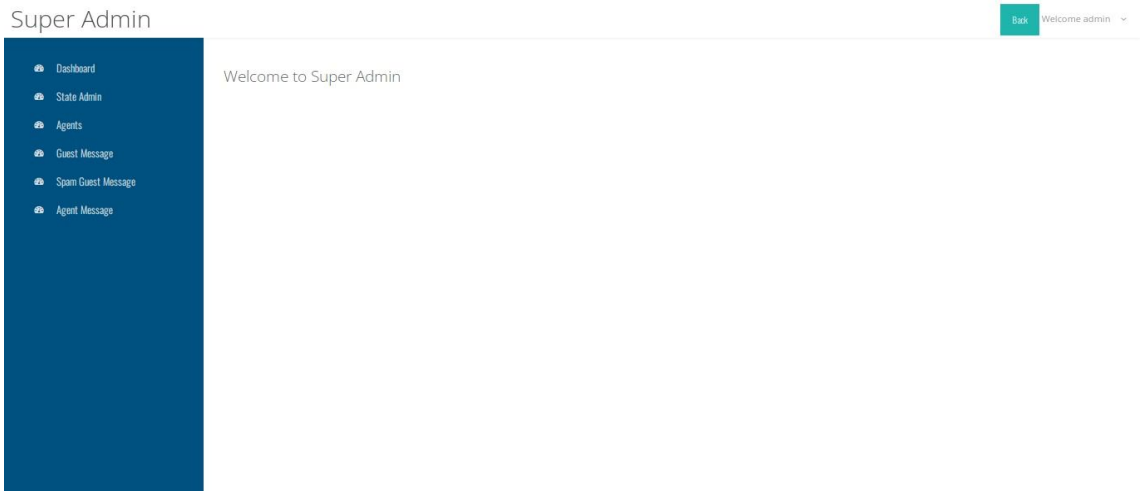
Screenshot 7.6: Guest Message in Super Admin



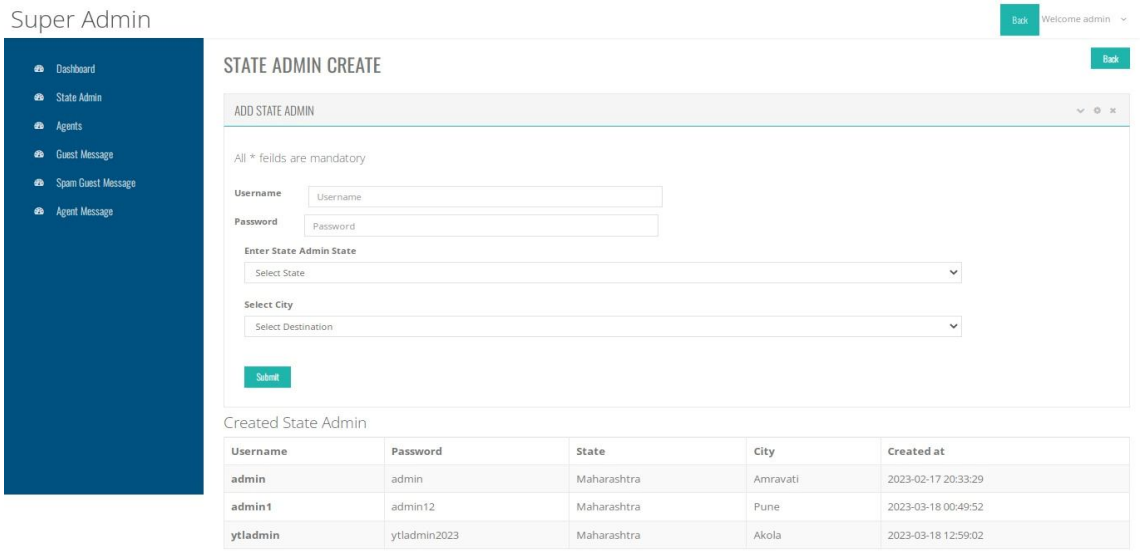
Screenshot 7.7: Agent Create form in state admin



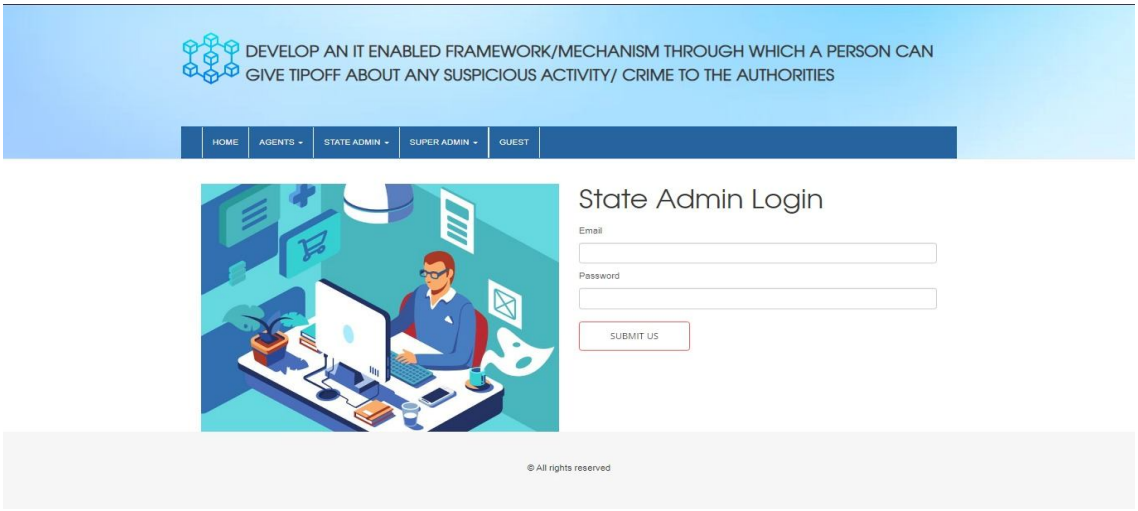
Screenshot 7.8: Agent Create form in state admin



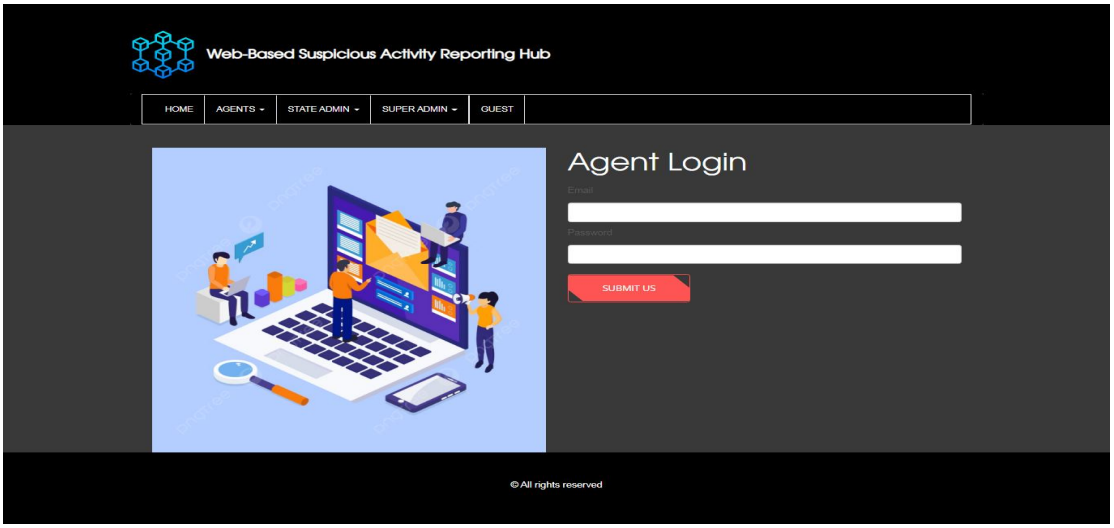
Screenshot 7.9: dashboard of super admin



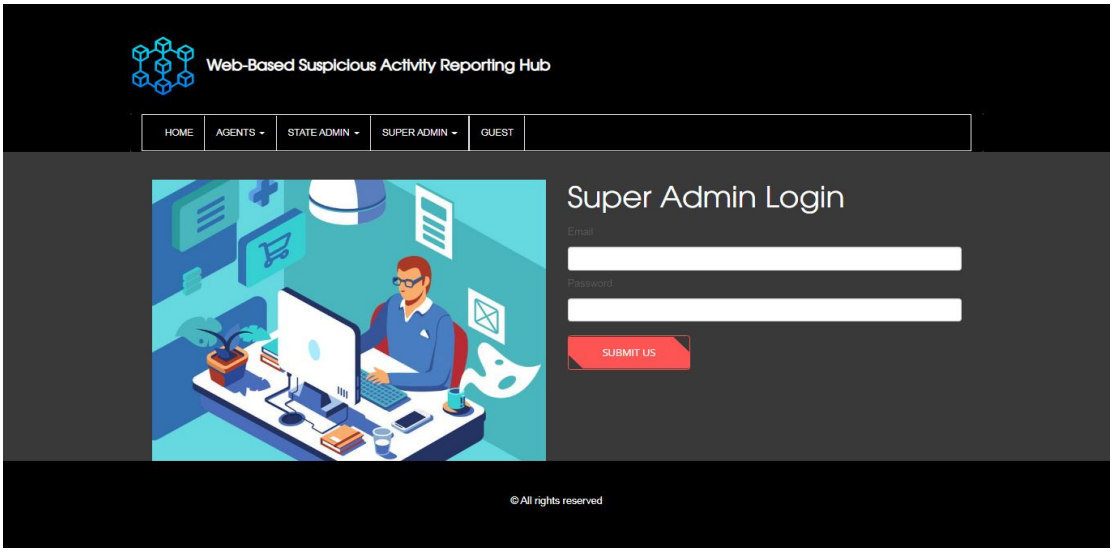
Screenshot 7.10: state admin addition form in super admin panel



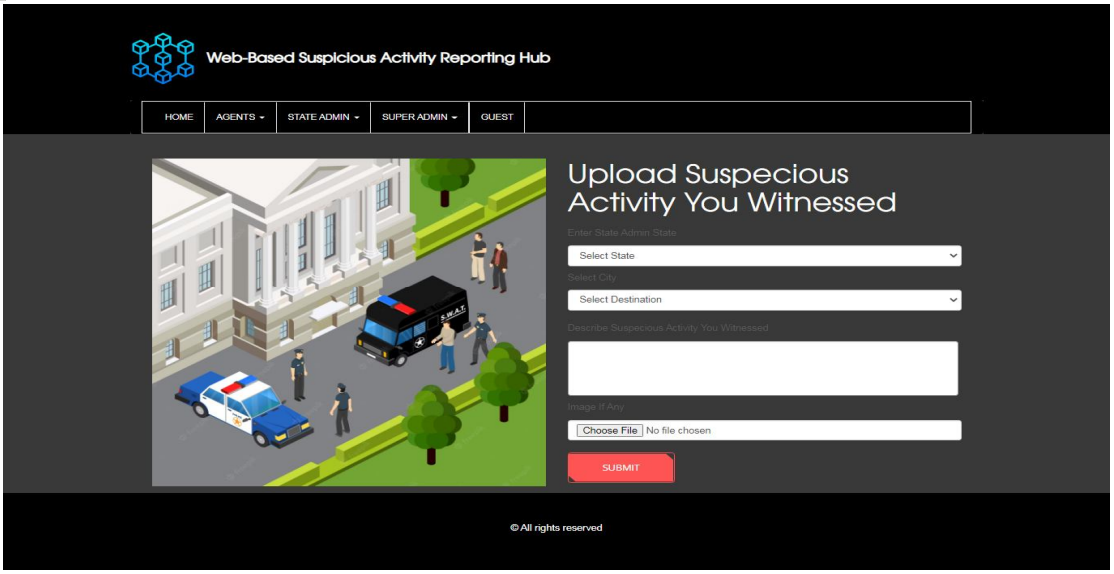
Screenshot 7.11: Authentication form of state admin



Screenshot 7.12: Authentication form of Agent

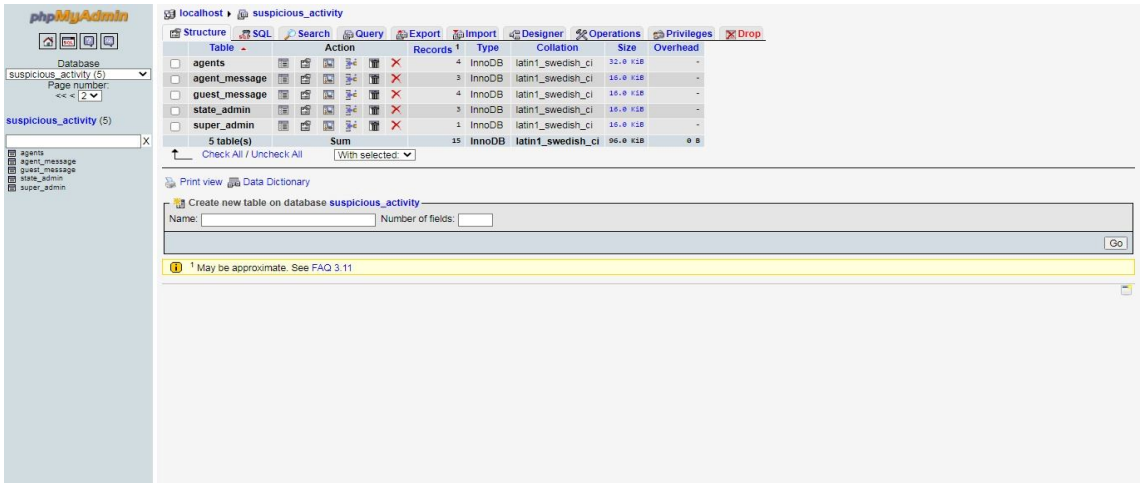


Screenshot 7.13: Authentication form of super admin

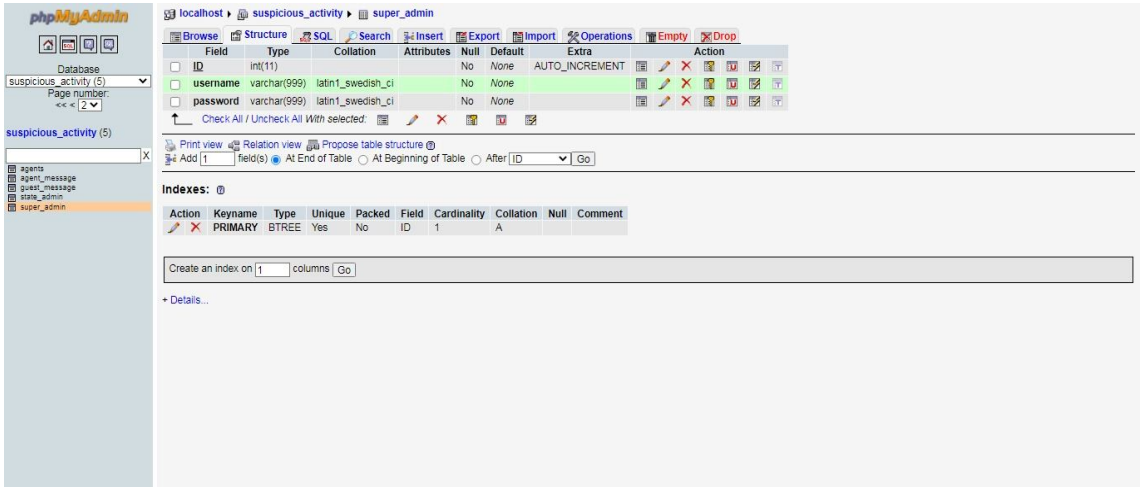


Screenshot 7.14: suspicious activity upload form

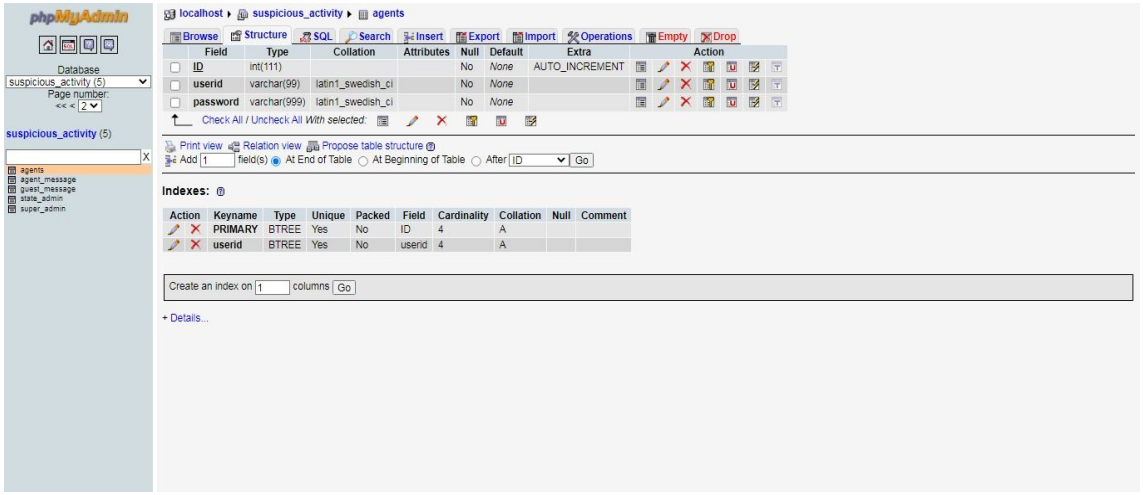
Screenshot 7.15: Database Tables



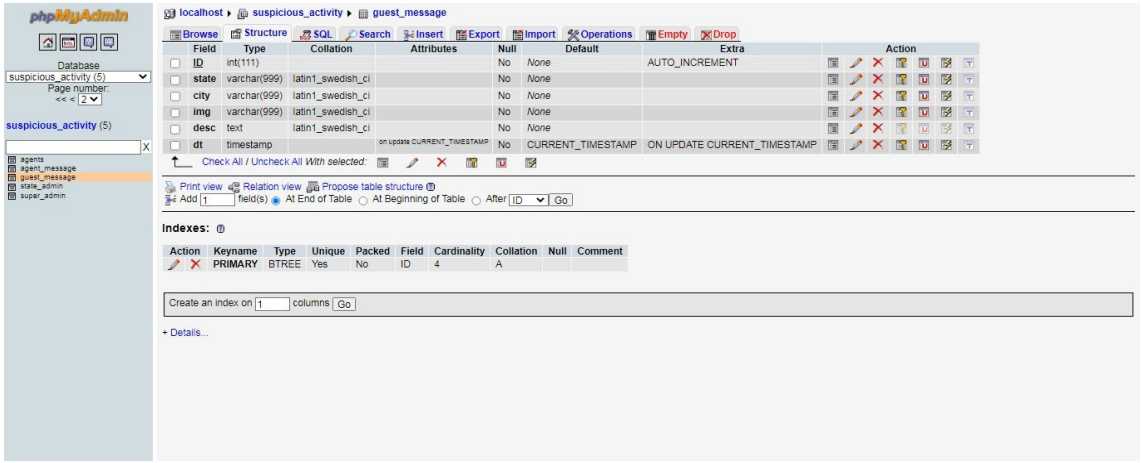
Screenshot 7.15: Database Tables



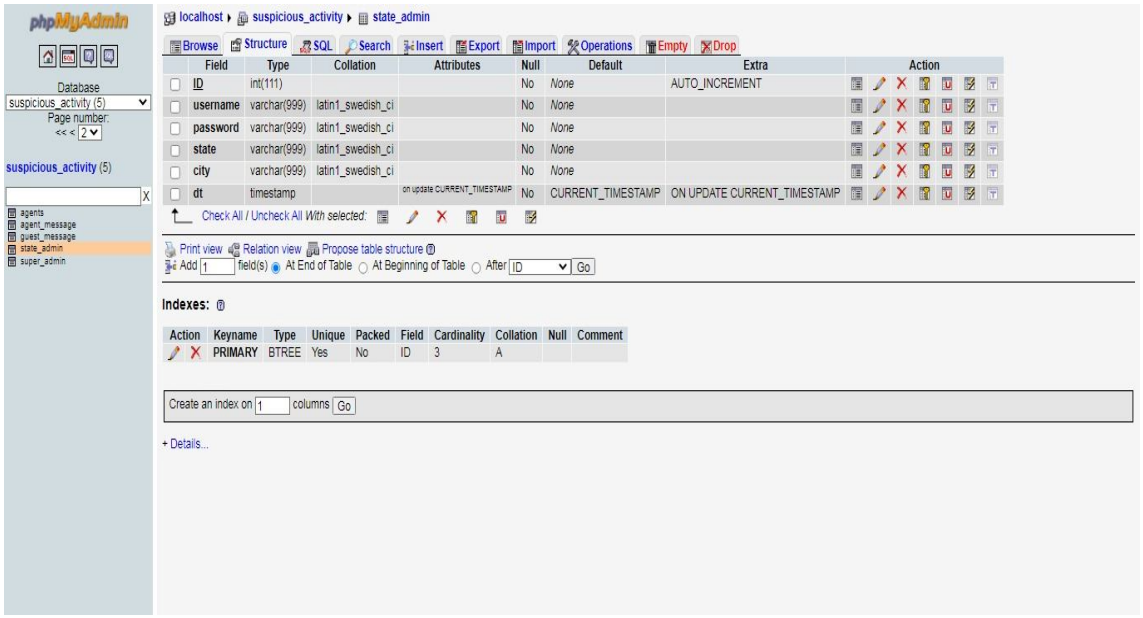
Screenshot 7.16: table super admin



Screenshot 7.17: Table Agent



Screenshot 7.18: Table Guest Message



Screenshot 7.19: table State Admin

VIII. CONCLUSION & FUTURE SCOPE

The key takeaway from our implementation is the importance of providing a secure and anonymous platform for crime reporting. While victims are typically expected to report crimes, witnesses often play a crucial role in uncovering valuable information. However, many witnesses hesitate to come forward due to fear of exposure or retaliation. Our system aims to prioritize witness protection by enabling them to share information anonymously.

Since not every tip-off is guaranteed to be genuine, implementing an algorithm to distinguish between authentic and false reports would significantly enhance police investigations. Insider information, when verified, holds substantial value in solving crimes. We believe that every individual deserves the right to be heard, and true justice is only possible when witnesses can share their accounts without fearing external threats. By leveraging modern technology, it is entirely feasible to build a reliable and anonymous crime tip-off system that encourages public participation in crime prevention.

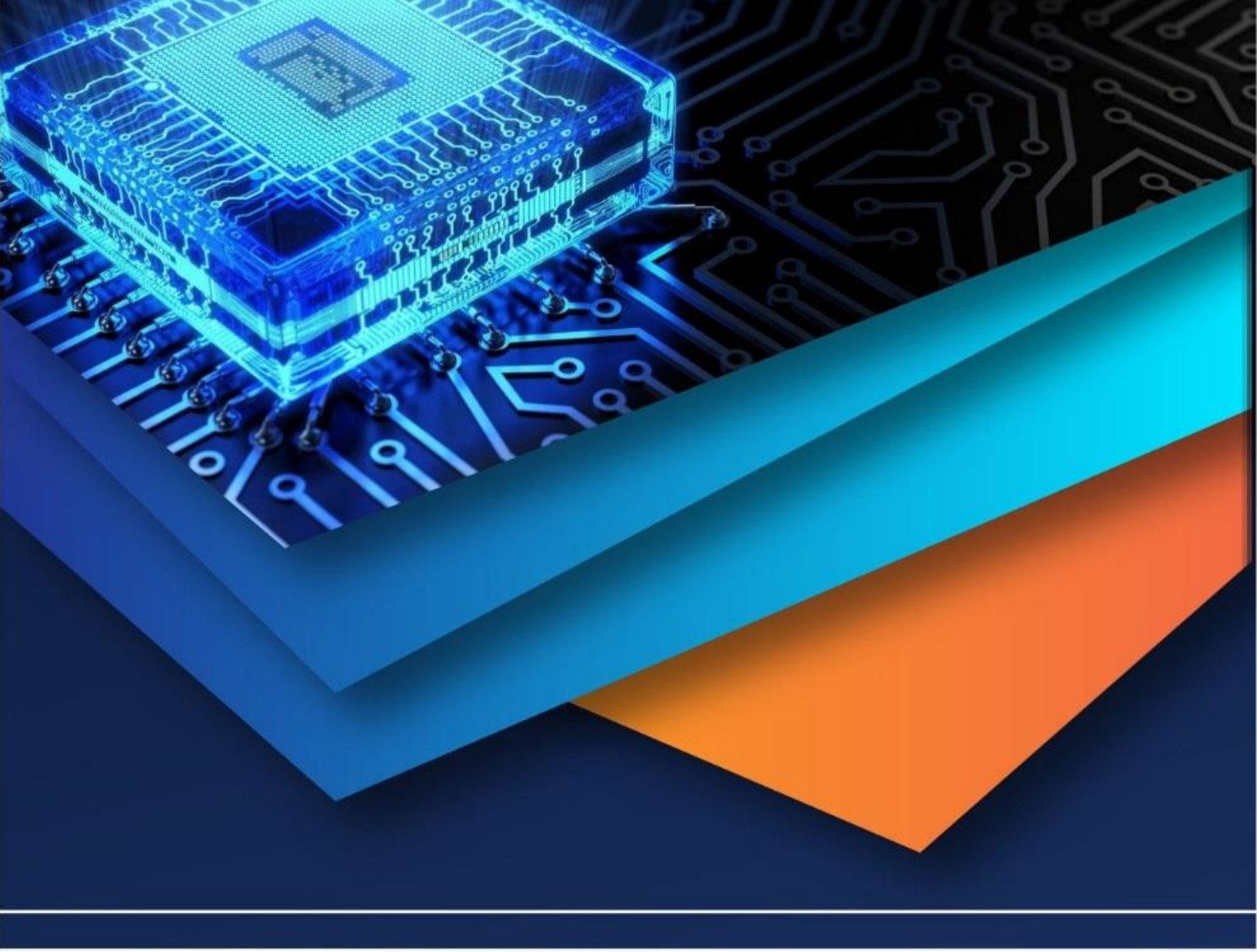
Through this research and development, we strive to address all critical aspects of crime reporting and contribute to creating a safer society with this innovative solution.

A. Potential Future Enhancements

- Support for Students in Unconventional Career Paths: The platform could be extended to provide guidance and resources for students pursuing non-traditional careers, helping them navigate unique professional journeys.
- Student Talent Management: The system could include performance evaluation-based talent management to identify and nurture student skills effectively.
- Online Exam Functionality: Adding an online examination module would enable institutions to conduct assessments remotely, increasing accessibility and flexibility.
- Online Resume Builder: Incorporating a resume-building feature would help students and job seekers create professional resumes easily, enhancing their employability.
- Online Classes: The platform could be expanded to include virtual classrooms, enabling remote learning and providing access to educational resources from any location.

REFERENCES

[1] “Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing” - Paper published on March 12th, 2021 by Yao Du, Shuxiao Miao, Zitian Tong, Victoria Lemieux &Zehua Wang - https://www.intechopen.com/online-first/75695
[2] “Sentiment Analysis of Twitter Data: A Survey of Techniques” - Published in April 2016 by Vishal A. Kharde& S.S. Sonawane – https://arxiv.org/ftp/arxiv/papers/1601/1601.06971.pdf
[3] “A Study of Text Classification Natural Language Processing Algorithms for Indian Languages” - Published in July 2015, by JasleenKaur and Dr.Jatinderkumar R. Saini - https://www.researchgate.net/publication/281965343_A_Study_of_Text_Classification_Natural_Language_Processing_Algorithms_for_Indian_Languages
[4] “Ethereum | Whitepaper” - Published in 2013 by VitalikButerin - the Founder of Ethereum - https://ethereum.org/en/whitepaper/
[5] “An anonymous platform for tip-offs on market manipulation” - Article published on 1st October, 2014 by Sachin P Mampatta https://www.businessstandard.com/article/markets/now-an-anonymousplatform-for-tip-offs-on-market-manipulation114100100577_1.html
[6] “Crime Reporting Behavior: Do Attitudes Toward the Police Matter?” - Published in February 2016 by Francis D. Boateng - https://www.researchgate.net/publication/295855033_ Crime_Reporting_Behavior_Do_Attitudes_Toward_the_Police_Matter
[7] “Why do more than 90% thefts in India’s metro cities go unreported” - Article published on 27th September, 2017 by Avanti Durani and NehaSinha - https://www.hindustantimes.com/india-news/why-domore-than-90-thefts-in-india-s-metro-cities-gounreported/story-FR6WZKAZiqzTRgN7LCilLI.html
[8] “NFTs in Practice - Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application” - Published in December 2019 by Ferdinand Regner, André Schweizer& Nils Urbach - https://www.researchgate.net/publication/336057493_NFTs_in_Practice_-_NonFungible_Tokens_as_Core_Component_of_a_Blockchain-based_Event_Ticketing_Application
[9] “NFTs: Digital things and their criminal lives” - Published on 19th August, 2021 by Simon Mackenzie &DiānaBērziņa – https://journals.sagepub.com/doi/abs/10.1177/1741659 0211039797?journalCode=cmca
[10] “Anonymous reporting: Why companies should allow it” - Article published by Moritz Homann on 7 th December, 2021 – https://www.integrityline.com/engb/expertise/blog/anonymous-reporting-companies/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY