iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78045

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 14 Issue III Mar 2026- Available at www.ijraset.com

Cyber Crime Management System

Aryan Navnath Dumbre[1], Sujal Navnath Pagire[2], Akshay Dnyandev Lokhande[3]
Computer Engineering Department, Samarth Polytechnic Belhe

Abstract: ***Cybercrime has become a major challenge in the digital era due to the increasing use of internet services, online transactions, and digital communication platforms. Crimes such as phishing, identity theft, hacking, online fraud, and cyber harassment are rapidly increasing worldwide. Traditional methods for reporting cybercrime are often inefficient, time-consuming, and lack transparency in tracking complaint status. To overcome these limitations, a web-based Cyber Crime Management System is proposed to provide a secure and efficient platform for reporting and managing cybercrime incidents. The system allows users to register, submit complaints, upload supporting evidence, and track complaint progress through a web interface. Administrators can monitor complaints, manage users, update complaint status, and analyze reported incidents. The system is implemented using HTML5, CSS3, Bootstrap, and JavaScript for the frontend, while Python with the Flask framework is used for backend development. SQLite database is used for efficient data storage. Security features such as SHA256 password hashing, session management, input validation, and secure file handling are implemented to ensure data confidentiality and system security. The implementation of this system improves accessibility, transparency, and efficiency in cybercrime complaint management.***

Keywords: Cyber Crime, Complaint Management System, Flask Framework, Web Application, SQLite Database, Cyber Security.

I. INTRODUCTION

The rapid growth of internet technologies has significantly improved communication, online services, and digital transactions. However, the increasing dependence on digital platforms has also led to a rise in cybercrime activities. Cybercriminals exploit security vulnerabilities in networks and applications to perform illegal activities such as financial fraud, identity theft, phishing attacks, hacking, and cyber harassment. Traditional cybercrime reporting methods usually require victims to visit police stations to file complaints manually. This process is often time-consuming and inconvenient. Additionally, victims often face difficulties in tracking the progress of their complaints. These limitations highlight the need for an efficient digital platform that allows users to report cybercrime incidents quickly and easily. A Cyber Crime Management System provides an online platform that enables users to register complaints and track their status without visiting physical offices. It also allows administrators to manage complaints effectively and monitor cybercrime incidents. The objective of this project is to design and implement a web-based Cyber Crime Management System that simplifies complaint registration, improves complaint tracking, and enhances communication between users and administrators. The system uses modern web technologies and security mechanisms to ensure reliable and secure operation.

.

II. LITERATURE REVIEW

Cybercrime has become a major issue in the digital era due to the rapid growth of internet services and online transactions. Many researchers have proposed web-based systems and security frameworks to improve cybercrime reporting and management. In research conducted by William Stallings, cyber security principles and network protection techniques were discussed to prevent cyber attacks such as hacking, phishing, and identity theft. The study highlights the importance of implementing strong authentication mechanisms, encryption, and secure communication protocols in web-based systems to protect user data.

A web-based crime reporting system was proposed by M. A. Hossain and S. Islam, which allows users to report crimes online and track the status of their complaints. The system improves accessibility and reduces the need for manual paperwork. However, the system lacked advanced security mechanisms and proper evidence management features.

Another study focused on developing a secure complaint management system using modern web technologies such as Python and lightweight frameworks. The use of frameworks such as Flask enables developers to build scalable web applications with simplified routing, request handling, and session management.

Research related to web application security by OWASP highlights common vulnerabilities in web systems such as SQL Injection, Cross-Site Scripting (XSS), and insecure authentication. Implementing security measures such as password hashing, input validation, and session management can significantly reduce these vulnerabilities.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Another important aspect discussed in recent studies is database management for web applications. Lightweight databases such as SQLite are widely used in web-based systems because they provide efficient data storage without requiring a separate server. SQLite is suitable for small and medium-scale applications due to its simplicity and reliability.

III.PROPOSED SYSTEM

The proposed Cyber Crime Management System is designed to provide a secure web-based platform for reporting and managing cybercrime complaints. The system follows a **Three-Tier Web Architecture** consisting of client tier, application tier, and database tier.

A. Client Tier

The client tier represents the user interface of the system. It is developed using HTML, CSS, Bootstrap, and JavaScript. This layer allows users to interact with the system through a web browser.
Users can perform actions such as:

1) Registering an account
2) Logging into the system
3) Submitting cybercrime complaints
4) Uploading supporting evidence
5) Viewing complaint details
6) Tracking complaint status

B. Application Tier

The application tier contains the backend logic implemented using Python and the Flask framework. It processes user requests and performs operations such as authentication, validation, and database communication.
The application tier handles the following tasks:

1) User authentication and session management
2) Complaint processing and storage
3) Evidence file handling
4) Request validation
5) Communication with the database

C. Database Tier

The database tier uses SQLite to store application data securely. The database contains multiple tables including users and complaints.
The Users Table stores user credentials and authentication data.
The Complaints Tabl**e** stores complaint details such as description, status, and timestamps.
The database structure maintains relationships between users and their submitted complaints.

IV.SYSTEM IMPLEMENTATION

The Cyber Crime Management System is implemented as a web application using the Flask framework. The frontend interface is designed using HTML, CSS, and Bootstrap to provide a responsive layout. JavaScript is used to enhance interactivity and perform client-side validation. The backend application handles request processing, authentication, and complaint management using Python and Flask. The Flask framework also manages routing, session handling, and integration with the SQLite database. The system consists of several functional modules including:

1) User Management Module: Handles user registration, login authentication, and session management.
2) Complaint Management Module: Allows users to submit cybercrime complaints and track their progress.
3) Evidence Handling Module: Supports secure file upload and validation for storing supporting evidence.
4) Admin Module: Provides administrative control to monitor complaints, manage users, and update complaint status.

Security features such as SHA256 password hashing, input validation, and file upload restrictions are implemented to protect the system from cyber attacks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

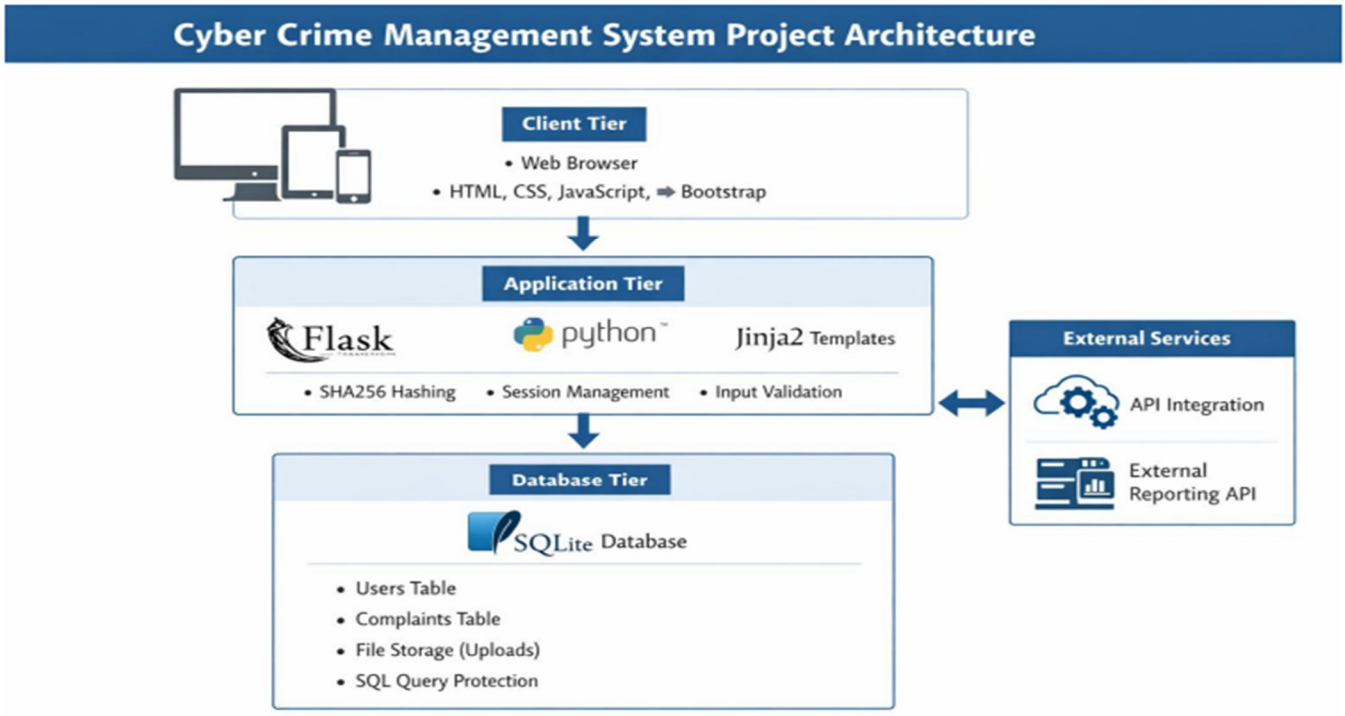


Fig. System Achitecture Digram

V. RESULT AND ANALYSIS

The implementation of the Cyber Crime Management System provides a simple and efficient platform for managing cybercrime complaints. Users can easily register on the platform and submit complaints using a structured form. The system allows users to upload evidence files such as screenshots or documents related to cybercrime incidents. Users can also track the progress of their complaints through the web interface. Administrators have access to a dashboard where they can view all complaints, update complaint status, and monitor user activity. This improves transparency and helps administrators manage complaints more efficiently. The use of Flask and SQLite ensures lightweight performance and easy deployment of the system. The implemented security mechanisms protect user data and prevent common web security vulnerabilities. Overall, the system improves accessibility and efficiency in reporting cybercrime incidents and provides better communication between users and administrators.

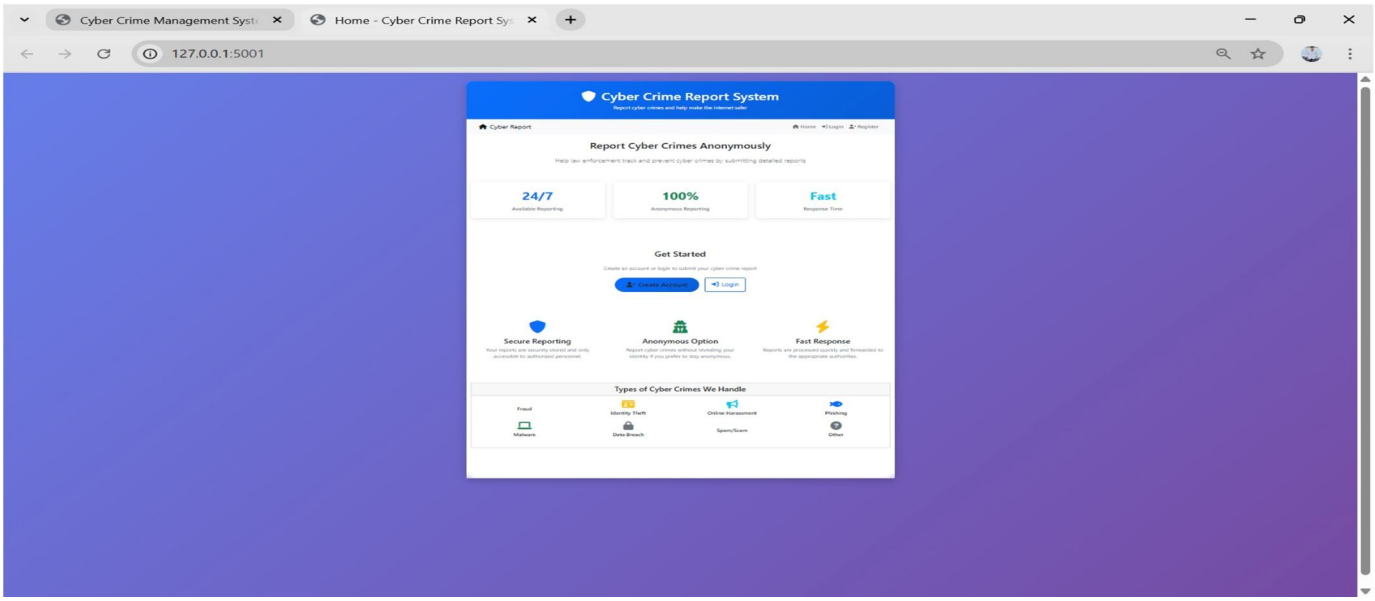


Fig Home Page

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

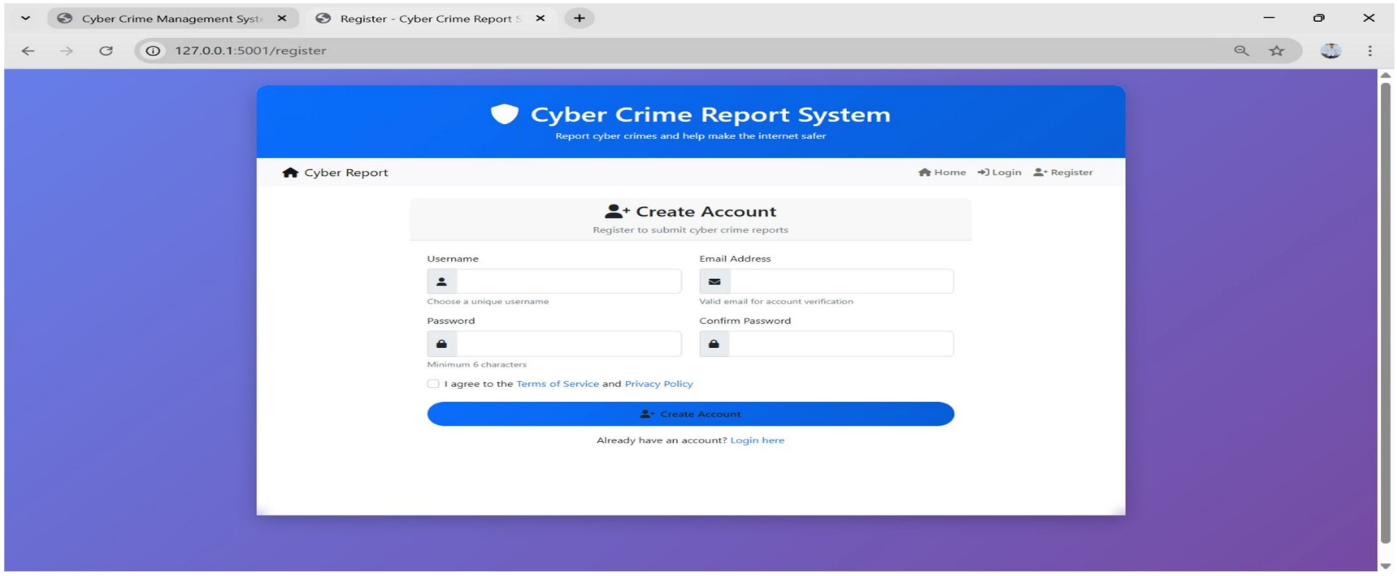


Fig User Account registration

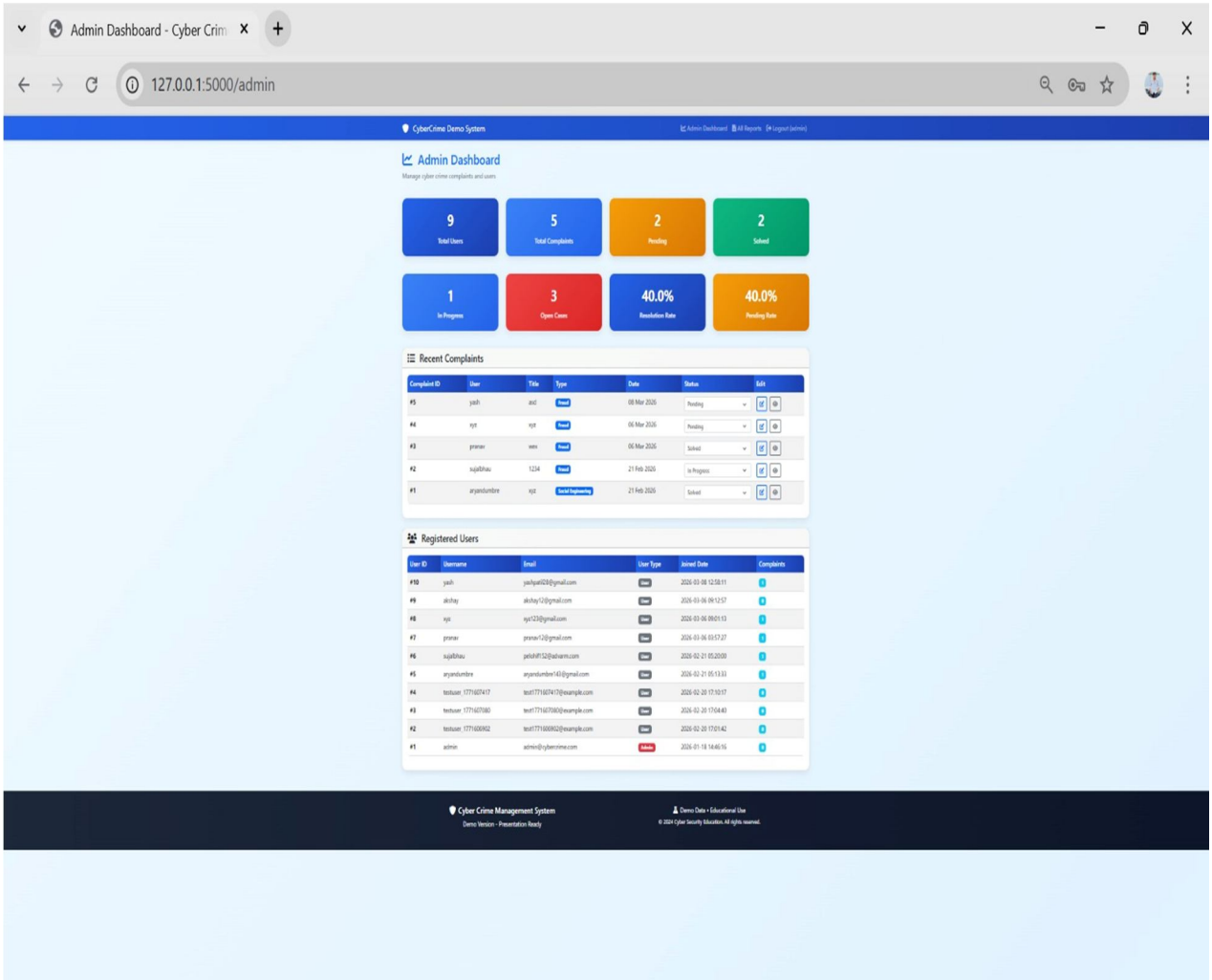


Fig. Dashbord

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

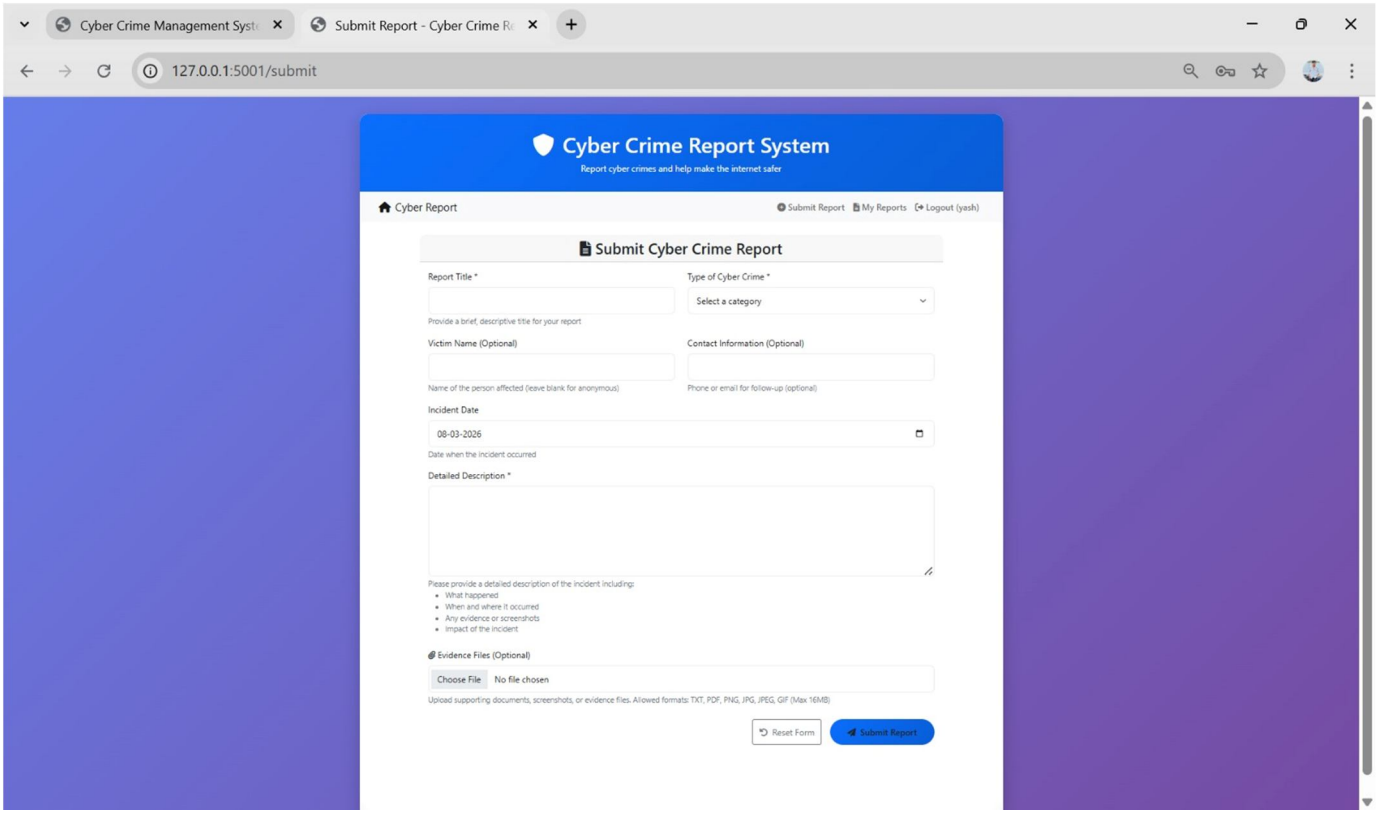


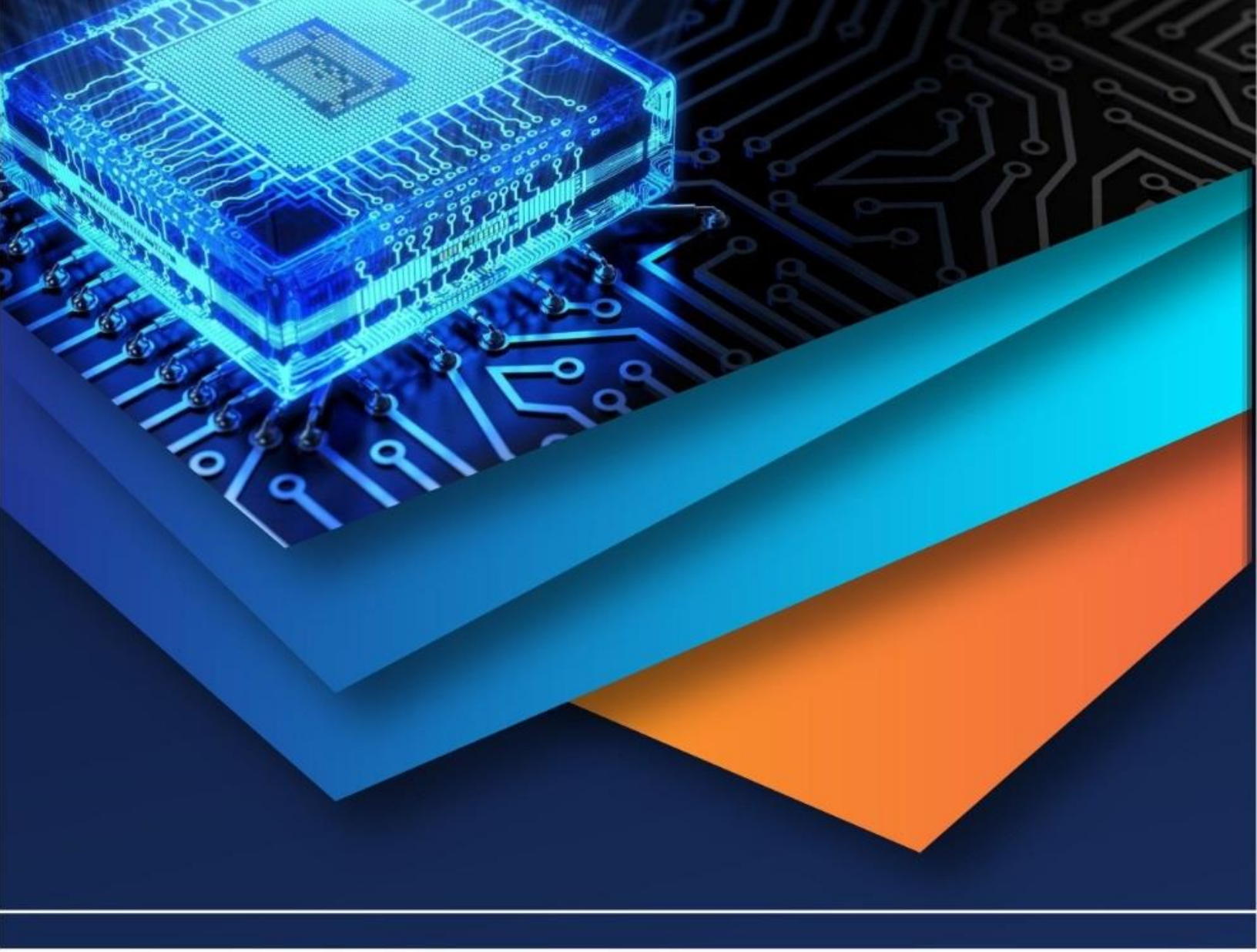
Fig. Submit cyber-crime Report

VI. CONCLUSION

The Cybercrime has become a serious problem in modern digital society. Efficient reporting and management systems are required to address cybercrime incidents effectively. The Cyber Crime Management System provides a secure and user-friendly web platform for reporting cybercrime complaints and managing them efficiently. The system simplifies the complaint submission process and allows administrators to monitor cases effectively. The integration of modern web technologies and security mechanisms ensures reliable system performance. Future enhancements may include mobile application support, integration with government cybercrime portals, real-time notifications, and advanced analytics for detecting cybercrime patterns.

REFERENCES

[1] William Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson Education, 2017.
[2] M. A. Hossain and S. Islam, "Web-Based Crime Reporting System for Efficient Crime Management," International Journal of Computer Applications, vol. 179, no. 24, pp. 12–18, 2018.
[3] Flask Documentation, Pallets Projects. Available: https://flask.palletsprojects.com
[4] SQLite Documentation. Available: https://www.sqlite.org
[5] OWASP, OWASP Top 10 Web Application Security Risks, 2021.
[6] Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, 2nd ed., Prentice Hall, 2002.
[7] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2015.
[8] Kevin Mitnick and William L. Simon, The Art of Deception: Controlling the Human Element of Security, Wiley Publishing, 2011.
[9] Joseph Migga Kizza, Guide to Computer Network Security, Springer, 2017.
[10] Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison-Wesley, 2011.
[11] National Institute of Standards and Technology, Guide to Computer Security Log Management, NIST Special Publication 800-92, 2012.
[12] European Union Agency for Cybersecurity, Cybersecurity Threat Landscape Report, 2020.
[13] International Telecommunication Union, Global Cybersecurity Index Report, 2021.
[14] IEEE, "Cyber Security and Digital Forensics Research Publications," IEEE Digital Library.
[15] OWASP, OWASP Top 10: Web Application Security Risks, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)