CyberPeace editor@cyberpeace.net

THE CYBERPEACE JOURNAL

Supported by United Service Institution of India

Academic Partner Shah & Anchor Kutchhi Engineering College

Cyber Rakshak Portal

Srushti Patil
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
srushti.17380@sakec.ac.in

Kashan Rizvi
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
kashan.17321@sakec.ac.in

Palash Thakkar
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
palash.17404@sakec.ac.in

Pallavi Sawale
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
pallavi.sawale@sakec.ac.in

***Abstract*— This paper provides a thorough review of a cybercrime reporting system that aims to improve law enforcement's response to cybercrimes and expedite the reporting process. Advanced technologies like blockchain are incorporated into the system to store data securely, artificial intelligence is used to automatically detect threats, and victims may easily report incidents thanks to an intuitive user interface. The principal aim is to furnish a centralized forum whereby individuals and businesses can anonymously report cyber events while guaranteeing the security and integrity of the information. In order to facilitate effective data analysis and research, the system also attempts to standardize the data collection procedure. The suggested solution, which combines real-time monitoring and data analytics, helps to discover new threats and accelerates and increases the accuracy of cybercrime investigations.**

Keywords — Cyber crime Reporting System, Cybercrime Data Standardization , Dashboard, Reporting and Analytics, Centralized Cybercrime Registry.

I. INTRODUCTION

An efficient Cyber Crime Reporting System is becoming more and more necessary as cyber dangers continue to grow on a global scale. Timely responses and comprehensive investigations may be hampered by the inefficiencies, delays, and lack of uniformity that plague traditional ways of reporting cybercrimes. This article investigates the creation of a resilient system that combines cutting-edge technologies and creative approaches to overcome these difficulties. The system utilizes artificial intelligence for threat identification and analysis along with blockchain technology to handle safe data, with the goal of improving the precision and effectiveness of cybercrime reporting and response.

Hacker is a term commonly applied to a "Computer user who intends to gain unauthorized access to a computer system." [7]. The suggested solution offers a centralized platform that makes it simple to submit incident reports and guarantees the integrity and confidentiality of sensitive data. It provides tools like multi-factor authentication, anonymized reporting, and real-time monitoring to help cybersecurity experts and law enforcement agencies recognize and respond to cyber threats more successfully. Additionally, the system is positioned as a crucial weapon in the fight against cybercrime because of its capacity to standardize data collecting and interface with current digital forensics technologies, providing a holistic solution to enhance the state of cybersecurity overall.

II. PURPOSE

This research paper's goals are to:

A. *Provide a Secure and Efficient Cybercrime Reporting Framework:* Construct a system that makes it easier for users to submit incident reports and streamlines the reporting process overall.

B. *Improving Data Security and Integrity:* To safeguard confidential data and preserve the accuracy of reported data, use cutting-edge security techniques like end-to-end encryption and blockchain technology.

C. To encourage more people to come forward without fear of reprisals, facilitate anonymous reporting of cybercrimes by providing avenues for victims and witnesses to do so.

D. *Integrate AI for Threat Detection:* To increase the speed and accuracy of threat identification and response, use artificial intelligence and machine learning to automatically assess and categorize reported incidents.

E. *Standardize Data collecting and Analysis:* To guarantee consistency and dependability and support more efficient investigations and data-driven decision-making, establish standardized procedures for data collecting and reporting.

F. *Boost Law Enforcement Coordination:* Establish a centralized platform that facilitates cooperation between cybersecurity experts and law enforcement organizations, improving resource allocation and coordination in the battle against cybercrime.

G. *Encourage Real-Time Monitoring and reaction:* To swiftly address new risks and lessen possible harm, enable real-time monitoring of reported occurrences and dynamic reaction capabilities.

III. OBJECTIVES

This research article aims to create and assess a Cyber Crime Reporting System that tackles the existing shortcomings in cybercrime reporting and investigation. By utilizing cutting-edge technologies like blockchain for data integrity and artificial intelligence for automated threat analysis, this system seeks to give people and companies a safe and easy-to-use platform for reporting cyber incidents. The project aims to improve overall response tactics, shorten the time needed for threat identification, and increase the efficiency and accuracy of cybercrime reporting by creating this system.

The report additionally attempts to enhance cooperation between cybersecurity experts and law enforcement organizations, as well as standardize the data collection method. The system's goal is to promote more thorough and prompt reporting of cyber events by including real-time monitoring elements and guaranteeing anonymous reporting. In the end, it all comes down to building a stronger and more efficient cybersecurity infrastructure that can better handle and mitigate the increasing dangers that come with cyberspace.

IV. METHODOLOGY

In order to guarantee the Cyber Crime Reporting System's efficacy, security, and usability, a methodical approach is employed during the development process. First and foremost, acquiring needs and analyzing them are crucial procedures. In this phase, the reporting system's goals and scope are defined, literature and current systems are reviewed, and stakeholder interviews are conducted. Having well-defined requirements aids in the establishment of features like case management, incident reporting, user authentication, and integration with law enforcement.

Second, building a strong architecture and user interface is the main goal of the design process. System architects and designers lay out the database schema, system components, and technical infrastructure based on the requirements that have been acquired. To enable smooth reporting and communication between users and administrators, design considerations include data security safeguards, encryption standards, access limits, and user-friendly interfaces. Alignment with industry standards and stakeholder expectations is ensured through prototyping and iterative design reviews.

Thirdly, the methodology's testing and implementation phases are crucial. The concept is translated into code by developers, who also incorporate security features and protocols including automated case assignment, real-time incident reporting, and progress tracking. Extensive testing guarantees that the system fulfills performance criteria and functions dependably under various conditions. This includes unit testing, integration testing, and user acceptance testing. It is possible to make improvements and modifications prior to the final release thanks to ongoing input from testers and stakeholders.

To sum up, the process of creating a Cyber Crime Reporting System project includes gathering requirements, designing the system, and going through rigorous phases of implementation and testing. The goal of this methodical approach is to provide a safe, intuitive environment that improves the ability to report cybercrimes, streamlines incident handling and encourages cooperation amongst relevant parties in the effective defense against cyberattacks.

V. LITERATURE SURVEY

A. *Current State of Cyber Crime Reporting*

- Overview: This section discusses the various platforms and systems that are currently in use by governments, private companies, and law enforcement agencies in order to report cybercrimes.
- Problems: Draw attention to the difficulties in reporting cybercrimes, including underreporting, a lack of uniform reporting guidelines, and problems with jurisdictional limits.

B. *Techniques and Frameworks for Technology:*

- Online Resources: Analyzing digital tools and platforms, such as mobile apps, web portals, and automated reporting systems, that are used for reporting cybercrimes.
- Technologies Involved: Examine how blockchain technology preserves immutable records, how artificial intelligence finds patterns, and how data analytics analyzes trends in cybercrime reporting.

C. *Concerns for Law and Ethics Legal Frameworks:*

- A summary of the rules and frameworks that control the reporting of cybercrimes in various jurisdictions, including mandatory reporting requirements, cross- border data exchange procedures, and data protection legislation.
- Ethical Issues: Talk about ethical issues such as privacy concerns, the possibility of reported data

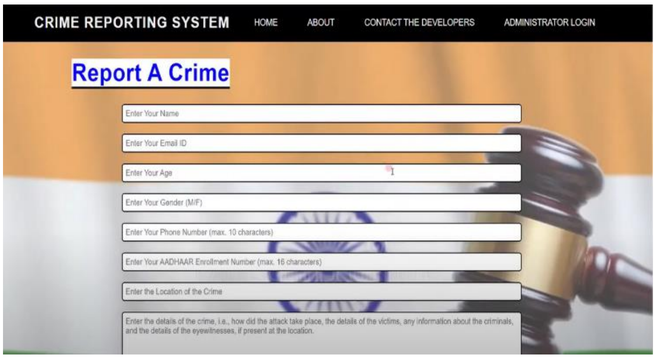
being misused, and the necessity of maintaining victim confidentiality and protection.

D. *Campaigns for Public Awareness and Engagement:*

- An analysis of public service announcements and educational activities that aim to increase public awareness of the value of reporting cybercrimes.
- Engagement Strategies: Examine tactics including user-friendly reporting interfaces, anonymity choices, and victim support services to see if they can motivate more victims and witnesses to report cybercrimes.

VI. RESULT.

While there have been notable developments in the creation and implementation of digital reporting systems, the "Cyber Crime Reporting System" research indicates that substantial obstacles still need to be overcome in order to achieve thorough and efficient cybercrime reporting. According to the study, despite the systems' increasing sophistication, there are still problems with underreporting because of ignorance or fear of retaliation, varying legal frameworks between countries, and technological constraints on data collecting and analysis. The utilization of cutting-edge technology such as blockchain and artificial intelligence has demonstrated potential to improve the dependability and effectiveness of reporting systems. Nonetheless, ethical worries about victim identity protection and data privacy remain major obstacles.



Enter Your Name

Enter Your Email ID

Enter Your Age

Enter Your Gender (M/F)

Enter Your Phone Number (max. 10 characters)

Enter Your AADHAAR Enrollment Number (max. 16 characters)

Enter the Location of the Crime

Enter the details of the crime, i.e., how did the attack take place, the details of the victims, any information about the criminals, and the details of the eyewitnesses, if present at the location.

Fig: 4.1

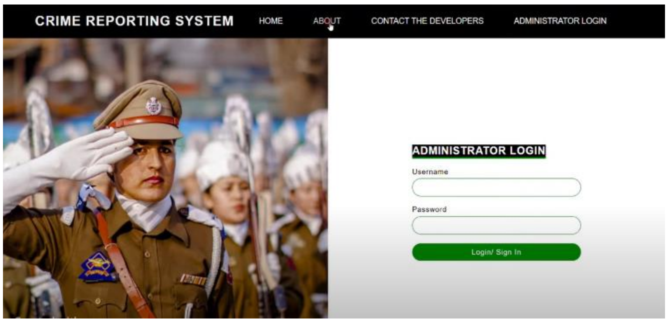
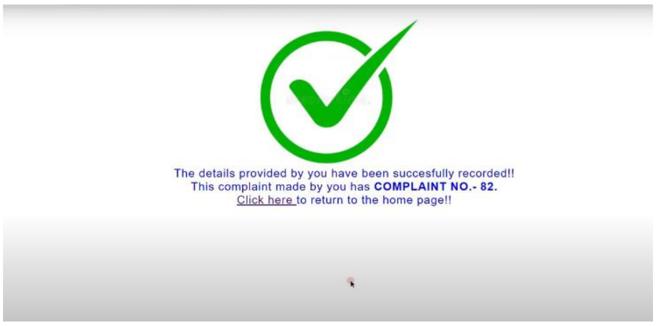


Fig: 4.



The details provided by you have been succesfully recorded!!
This complaint made by you has **COMPLAINT NO.- 82.**
Click here to return to the home page!!

Fig: 4.3

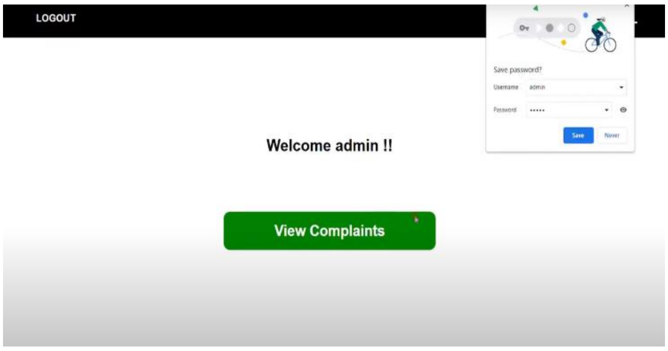
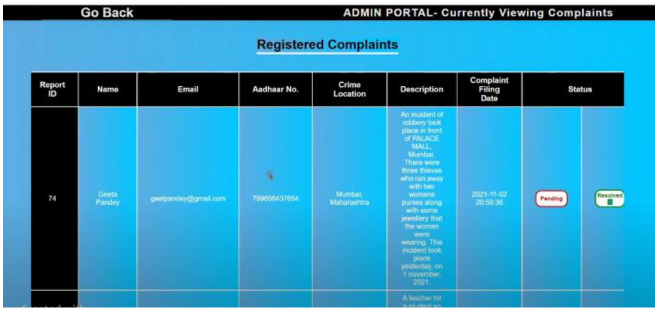


Fig: 4.4



Report ID	Name	Email	Aadhaar No.	Crime Location	Description	Complaint Filing Date	Status	
74	Geeta Pandey	geetpandey@gmail.com	789656437654	Mumbai, Maharashtra	An incident of robbery took place in front of PALACE MALL, Mumbai. There were three thieves who ran away with two womens purses along with some jewellery that the women were wearing. This incident took place yesterday, on 1 november, 2021.	2021-11-02 20:59:36	Pending	Resolved
					A teacher hit a student so			

Fig : 4.5.

VII. FUTURE SCOPE.

A. *Advanced Reporting Systems Real-time Reporting and Analysis:*

AI and machine learning may be used in future systems to detect and report cyber problems in real-time. This would enable more precise threat classification and speedier responses.

Automated Threat Detection: By integrating automated detection systems with enhanced threat information feeds, it may be possible to recognize and report new risks. Tracking System are very flexible and can be integrated with various technologies [8].

B. *Better User Experience Interfaces that are easy to use:*

Upcoming systems may concentrate on enhancing the user experience by simplifying the incident reporting process for non-technical users.

Multilingual help: The system might provide multilingual help to suit users from across the world, opening it up to a larger audience.

C. Integration of the Legal and Law Enforcement Systems Cooperation with the Police:

Investigative speed and efficacy may be increased by strengthening data exchange and cooperation between law enforcement and reporting systems.

Legal Frameworks and Compliance: In order to promote cross-border collaboration in the fight against cybercrimes, future systems may be created in accordance with international laws and regulations.

D. Security and Privacy of Data Safe Reporting Channels:

One of the main priorities will be to guarantee the integrity and confidentiality of the data that is reported. Sensitive data may be protected via sophisticated encryption and secure pathways in future systems.

Whistle blower Protection and Anonymity: Giving victims the option to report anonymously can help them come forward without worrying about being retaliated against.

VIII. CONCLUSION .

The "Cyber Crime Reporting System" report concludes by emphasizing how vital it is to take an effective and all-encompassing approach to combating the growing threat of cybercrimes. The study sheds light on the difficulties that today's reporting systems must overcome, such as gaps in the legal system, technological constraints, and problems with public knowledge and involvement. Notwithstanding these difficulties, integrating cutting-edge technology like blockchain and artificial intelligence has enormous potential to improve the security, efficacy, and accuracy of cybercrime reporting. In addition, it is clear that international coordination and worldwide standardization are required to provide a coordinated and successful response to cyber attacks.

AKNOWLEDGEMENT

To everyone who helped to successfully complete this cybersecurity research paper, I would like to extend my sincere gratitude. Throughout this journey, your help, support, and advice have been priceless. Above all, I would want to express my gratitude to my committed Guide, Ms. Pallavi Sawale, for her constant assistance, knowledgeable counsel, and insightful to I want to start by expressing my gratitude to my committed Guide, Ms. Pallavi Sawale, for her steadfast support, knowledgeable advice, and insightful comments. The direction and caliber of this work have greatly benefited from your mentoring. I also want to express my gratitude to Palash Thakkar, Srushti Patil, and Kashan Rizvi, who made up my research team, for their excellent work ethic, boundless devotion, and innumerable hours of ideation, investigation, and content evaluation. This Research paper has been made truly exceptional by your dedication to perfection. I am appreciative of Shah & Anchor Kutchhi engineering college.

REFERENCES.

[1] National Crime Record Bureau (NCRB): https://ncrb.gov.in/en Provides data and reports on cybercrime in India, highlighting the significance of improved reporting mechanisms.

[2] Council of Europe: Budapest Convention on Cybercrime: https://www.coe.int/en/web/cybercrime An international treaty promoting cooperation in the fight against cybercrime, emphasizing the importance of effective reporting systems.

[3] Cybersecurity &amp; Infrastructure Security Agency (CISA): https://www.cisa.gov/ U.S. government agency offering resources and guidance on cybercrime reporting, which can be adapted for the Indian context.

[4] OWASP Top 10: (https://owasp.org/www-project-top-ten/) A well-recognized standard for web application security, providing valuable insights for securing.

[5] PHP Manual: (https://www.php.net/manual/en/index.php) The official documentation for PHP, a crucial resource for understanding the development process for the Cyber Rakshak portal.

[6] MySQL Documentation: (https://dev.mysql.com/doc/) The official documentation for MySQL, a relational database management system essential for data storage in Cyber crime Reporting System. the Cyber Rakshak portal.

[7] https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY .

[8] https://ijcrt.org/papers/IJCRT2106568.pdf by the United Nations Office on Drugs and Crime

[9] Enhancing Cyber Crime Reporting Systems: Best Practices and Guidelines" by the International Association of Chiefs of Police (IACP)