International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 01 | January - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

CrimeBook: Where Reporting Crime Anonymously is Easier

KSHITIJ KUMAR SINGH, PRINCE MISHRA

Department of CSE Presidency University Bengaluru, India

Abstract

Our project focuses on the development of an advanced anonymous crime reporting system aimed at empowering individuals to report crimes without fear of reprisal. Utilizing a user-friendly website, we have created a platform that allows users to submit anonymous crime reports and receive updates on the progress of their submissions. The primary objectives are to boost crime reporting rates, enhance community engagement, and minimize law enforcement response times. Extensive research indicates that our anonymous reporting system has been highly effective in achieving these goals.

Acknowledging the potential challenges associated with anonymous reporting, including the risk of false reports and the imperative to safeguard user privacy, our project employs state-of-the-art Blowfish cipher encryption to secure personal data. This encryption methodology ensures that sensitive information remains confidential and is only accessible to authorized personnel. Our innovative approach not only addresses the crucial need for a secure and anonymous reporting mechanism but also establishes a transparent and efficient communication channel between the community and law enforcement agencies. By encouraging citizens to play an active role in crime prevention without compromising their safety, our system contributes to the creation of a safer and more secure community environment.

In addition to the technological aspects, our project places a strong emphasis on user education and awareness. Through outreach programs, we aim to educate the community about the benefits and responsible use of the anonymous reporting system. This proactive approach fosters trust between law enforcement and citizens, further reinforcing the collaborative effort to maintain public safety. While our research and implementation have yielded positive outcomes, we remain committed to ongoing improvement and adaptation. Regular updates and user feedback mechanisms are integrated into the system to ensure continuous refinement and responsiveness to emerging challenges. By fostering a culture of accountability and collaboration, our project stands as a model for leveraging technology to address complex societal issues while prioritizing user safety and privacy.

1. Introduction

The act of reporting crimes plays a pivotal role in cultivating safer communities, yet the prevalent reluctance among individuals to share information, fueled by the fear of retaliation, presents a formidable challenge. In response to this concern, our innovative solution proposes the implementation of an anonymous crime reporting system, providing a secure platform for reporting incidents while ensuring the anonymity of the reporter. Leveraging the MERN Stack (MongoDB, Express, React, Node), this project endeavors to establish a dedicated website tailored to anonymous crime reporting, aiming to assuage concerns related to potential reprisals. The core objective of this system is threefold: to elevate crime reporting rates, foster increased community engagement, and diminish law enforcement response times. Robust empirical research substantiates the efficacy of anonymous reporting in achieving these pivotal goals. However, the introduction of anonymous reporting also brings forth specific challenges, notably the potential for false reports and the indispensable need to safeguard user privacy.

To address and mitigate these challenges, our project incorporates comprehensive measures that not only ensure the legitimacy and credibility of reports but also prioritize the protection of user privacy. A noteworthy aspect of our approach involves the utilization of Blowfish cipher encryption to secure personal data. This advanced encryption methodology serves the dual purpose of mitigating the risk of false reporting and safeguarding user privacy. In essence, our project emerges as a comprehensive and innovative solution, providing a secure and confidential avenue for individuals to report crimes. By addressing the challenges associated with anonymous reporting, our system contributes significantly to the creation of safer communities, fostering a culture of trust and cooperation between the public and law enforcement agencies.

2. Literature Survey

Prof. Nawale S.K et al.'s research [1] proposes the development of an Online Crime Reporting System as a comprehensive software solution to manage police station operations efficiently. This system aims to streamline the handling of crime files and operational activities within police stations, allowing for better control and monitoring. Currently, many police station tasks are managed manually, but the proposed system suggests automating these processes through computerized operational structures. The system comprises modules such as Login for Individuals and Administrators, View Complaint Status,

Access Case Record Information, Check Most Wanted Criminals List, Trending City Crime Information, and Safety Recommendations, particularly for vulnerable individuals such as girls and vendors. This initiative proves beneficial in automating complaint recording, maintaining malpractice records, user management systems, and overall administration of police stations.

S. Selvakani et al.'s study [2] emphasizes the inevitability of crime in human activities and advocates for its meticulous monitoring. Recognizing that society cannot be entirely free from criminal elements, the research proposes a crime reporting system model based on three specific modes:

- reporting system,
- post-investigation reporting system,
- and recording reporting system.

The framework comprises three essential modules: an information gathering module, a reporting and control module, and an information utilization module. Future work on this crime exposure framework could focus on enhancing accessibility, awareness, and usability, potentially through portable delivery methods.

In the study conducted by Nnadimma et al. [3], the researchers address the societal need for a robust crime reporting mechanism in an ideal legal-governed society. Traditionally, reporting crimes involved physically visiting law enforcement offices, leaving little room for anonymity. However, with technological advancements, various reporting methods have emerged, ranging from Telegram and specialized radio communications to web and mobile applications. The proposed project seeks to create a comprehensive web platform that caters to all crime types, accessible to the public and featuring suggestive (Find Entities), interpretive, and informative elements. Importantly, the platform ensures anonymity for individuals reporting crimes, aligning with the evolving landscape of technology- enabled crime reporting.

Ashwani Sharma et al.'s research [4] introduces the concept of an Online Crime Reporting System, presenting it as a comprehensive application that encompasses the entire case management system. The primary objective of this project is to streamline and enhance the management of all activities within a police station. By leveraging computer technology, the system facilitates the reporting of crimes and the efficient management of various tasks within the police station. Noteworthy features include the tracking of complaint details, most wanted criminals, and police station information. The current manual processes within police stations can be replaced with computerized systems, ensuring ease and efficiency. The project integrates modules such as User and Admin Login, Complaint Registration, Complaint Status View, Criminal Record Management, Case History Details Management, Most Wanted Criminal List Management, City Crime Latest News, and Safety Tips, particularly focusing on women and sellers. This initiative proves instrumental in automating police station records, including complaints, criminal records, administrative processes, and user and police management systems.

In a study conducted by Tzay-Farn Shih et al. [5], a Cloud-Based Crime Reporting System with Identity Protection is proposed. This innovative system incorporates digital signatures, symmetric and asymmetric keys, as well as digital certificates to enable secure reporting of illegal events. The proposed approach manages criminal conduct reports from the reporting stage to the issuance of rewards, ensuring data integrity, safety, anonymity, and non-repudiation of informants. Additionally, it prevents case and report erasure, fraudulent reports, and safeguards against abusive system usage. This approach provides a practical and secure platform for reporting and combating crime, addressing administrative issues such as lost or deleted cases and mitigating the risk of malicious system usage.

Non-repudiation emerges as a crucial aspect within this proposed solution. All information signed by system users is securely stored on the system server, eliminating the possibility of users disputing the authenticity of records in case of disagreements. This comprehensive and secure approach ensures the credibility, integrity, and efficiency of the crime reporting system, aligning with the evolving needs of law enforcement and the community.

- The possibility that reported cases would be forgotten or delayed as a result of outside interference. The suggested approach is therefore outfitted with an automatic upward reporting mechanism to prevent reported cases from being suppressed if they are not accepted within a set amount of time.
- That the reward process may allow for the identification of informers. As there is no record to monitor the identity of a person making a report, the suggested scheme incorporates a precautionary method to ensure that managers or databases are not leaked. This is necessary because the system must preserve the privacy of informers in all actions.
- The identity of the informant could be revealed if the reported information is intercepted or released. Consequently, it is crucial to guarantee total transmission confidentiality.

In its entirety, an online reporting system must conform to a set of essential standards, encompassing authentication, anonymity, integrity, non-repudiation, prevention of case erasure, avoidance of informer identity disclosure during award procedures, safeguarding informant privacy, and averting interception of reported information.

Eugene F. Ferraro of Morrison, CO (US) [6] introduces a study proposing an anonymous reporting system tailored for reporting and tracking occurrences, accidents, and related incidents. The system is initiated by a provider for an institutional participant or client, allowing numerous individual users to access it. The most common implementation involves a web-based interface with an integrated website. Notably, the interface incorporates an anonymizer to safeguard the identity of

© 2024, IJSREM | www.ijsrem.com

each user. Users are presented with the option to submit a report, and the system assigns a random number identifier to each report to maintain complete anonymity.

A select group of recipients and one or more administrators linked to the participant or client receive the reports. Administrators, while ensuring anonymity, can request additional comments or communicate regarding the report using the assigned access number. This system is particularly well-suited for implementation in institutional or corporate settings, providing a secure and confidential avenue for reporting incidents while preserving the anonymity of users. The study emphasizes the importance of these features in enhancing the functionality and effectiveness of online reporting systems in various organizational contexts.

- The subscriber makes arrangements with the system provider for the installation of the incident reporting system.
- The subscriber informs its constituents of the reporting system's existence and publishes the channels through which the constituents can report occurrences, such as phone numbers and email addresses.
- To report an occurrence anonymously, the reporting party (witness/user) may make a phone call or use the Internet. A special anonymous identifier is supplied to the reporter to be used for any future reporting or conversation.
- The system's anonymizer ensures, within bounds, the anonymity of both the submitter and the report's content. Witnesses are able to create one or more anonymous accounts for reporting and following up on reports. These accounts may also serve as personalities, enabling follow-up inquiries and other conversations.
- The information is acquired and compiled by the supplier, who then sends reports to the subscriber so they can classify the data and review the outcomes of earlier inputs.
- The system offers a framework for comparing and utilising earlier reports, enabling the subscriber to supplement earlier reports, include fresh submissions, and see the outcomes of earlier submissions.

Overall, the system offers a straightforward and anonymous way for people to report worrying situations while retaining complete confidentiality. The system offers a low-cost and practical mechanism for subscribers to classify and track reported incidents, as well as safe and organised handling of participant information and identities.

Riya Lohan et al. [7] This study asserted that as a society becomes more populous and complex, the range of antisocial activities that must be controlled by the government through the armed forces and other agencies, especially the Police Force, increases. The incident-based system covers a far larger range of offences and reports on the circumstances surrounding the crime, the victim, and the criminal. Because there is no direct alternative to reporting crimes through phone, messaging, or potentially face-to-face, which can be problematic if the reporter wants to protect their anonymity, the current mechanism for doing so faces a number of difficulties. A prototype crime reporting system consists of four reporting forms: a complaint or dispatch reporting form, a criminal event report form, a follow-up investigation report form and an arrest report form. The system's three functional modules are data collecting, report administration and control, and data utilization. Future enhancements to the crime reporting system could concentrate on boosting mobile accessibility, utilization, and awareness.

The following steps were taken in order to report crimes:

1. The FIR form is completed by the victim or volunteer.
2. Police check the reliability of the information source.
3. If all goes as planned, the police continue theirinquiry.
4. If the report is accurate in every way, the police reject it and mark it as a fake.
5. An immediate use document.
6. Repetition of stages 2 through 4.

A.M. Archana and others [8] This study suggested that the user could submit any online photographic evidence and the victims could submit a case through a website under one of numerous divisions. Users will be able to hit a "SOS" button to send their location to the closest police station using the "SOS" feature. For accident victims, there will be a separate component so that FIRs can be filed immediately and treatment may start straight away. Under the current setup, users' information will be kept private, and only complaints will be transmitted to the nearest police station. The server side will immediately transfer the user's complaint number, and the concepts of cookies and IP addressing will be used to pinpoint the location and the real person. In order to resolve the location issues, the police station's server is crucial. It will seek up the address using the IP address before forwarding the message to the police station from which it was sent.

A website from which users can submit a First Information Report (FIR) against the offender under several categories will be part of the "Online Crime Report" plan. If the FIR has been filed and the necessary actions have been performed, the user will be informed by the admin (from the police), who manages the main website. Victims can lodge a FIR through a number of website sections. The user may send any images they may have found online. Through a criminal database, the police will always have access to the information. Under this strategy, user information will remain private, and only complaints will be forwarded to the neighborhood police station. The number of user complaints are automatically forwarded by the server, and the concepts of cookies and IP addressing have been utilized to identify the location and the in the realm of online reporting systems, strict adherence to a set of foundational standards is imperative. These standards encompass critical aspects such as authentication, anonymity, integrity, non-repudiation, prevention of case erasure, avoidance of informer identity disclosure during award procedures, safeguarding informant privacy, and averting the interception of reported information.

In a study by Eugene F. Ferraro from Morrison, CO (US) [6], a novel approach to anonymous reporting systems is presented, specifically designed for reporting and tracking various incidents like occurrences and accidents. The initiation of this system is facilitated by a provider for an institutional participant or client, enabling a multitude of individual users to seamlessly access it. The predominant implementation involves a web-based interface with an integrated website. A notable feature of this interface is the incorporation of an anonymizer, ensuring the preservation of each user's identity. Users are provided with the flexibility to submit reports, and the system, in turn, assigns a unique random number identifier to each report, preserving the complete anonymity of the user.

Reports are disseminated to a selected group of recipients and one or more administrators associated with the participant or client. The administrators, while upholding the principle of anonymity, can solicit additional comments or communicate pertinent information related to the report using the assigned access number. This system stands out as particularly well-suited for implementation in institutional or corporate settings, offering a secure and confidential channel for reporting incidents while prioritizing user anonymity.

3. Legal framework

1. The Indian Evidence Act of 1872 stands as a crucial legal avenue for CrimeBook, offering a legitimate pathway for electronic evidence within defined parameters. This legal framework has the potential to confer credibility upon CrimeBook's submissions, rendering them acceptable evidence in a court of law.

Expanding on this, the Indian Evidence Act of 1872 has been a cornerstone in shaping the admissibility of electronic evidence, ushering in a new era where CrimeBook's role becomes more pronounced. The Act, while permitting electronic evidence, imposes specific restrictions, providing a nuanced perspective on the acceptance of such materials in legal proceedings. The careful navigation of these restrictions becomes pivotal for CrimeBook to establish a solid foundation for its submissions within the legal domain.

2. The Information Technology Act of 2000 emerges as a pivotal piece of legislation addressing the complex landscape of cybercrime and data privacy concerns. CrimeBook finds itself compelled to adhere to the provisions outlined in this statute, necessitating the implementation of robust data security measures. This imperative ensures not only the safeguarding of user data on the platform but also guarantees compliance with regulatory standards.

Delving deeper into the Information Technology Act of 2000, CrimeBook's compliance extends beyond a mere legal obligation. The act mandates a comprehensive approach to data security, obliging CrimeBook to deploy advanced measures that fortify its defenses against potential cyber threats. By aligning with this legal framework, CrimeBook not only enhances its own security posture but also contributes to the broader efforts in maintaining the integrity of digital interactions within the cyber realm.

3. The Witness Protection Scheme of 2009 holds considerable significance within the operational framework of CrimeBook. This scheme, designed to safeguard witnesses, becomes a distinctive feature that can foster a conducive environment for anonymous reporting on the platform. The assurance of witness protection becomes a catalyst in bolstering CrimeBook's effectiveness, as individuals are more likely to step forward with valuable information when guaranteed safety.

Expanding on this, the Witness Protection Scheme of 2009 plays a pivotal role in shaping CrimeBook's reputation as a reliable platform for confidential reporting. The assurance of anonymity and protection for those willing to provide critical information contributes not only to the platform's credibility but also serves as a powerful incentive for individuals to become proactive contributors to the fight against crime. In essence, this scheme becomes a cornerstone in building trust and cooperation within the CrimeBook community, establishing it as a formidable ally in the pursuit of justice.

4. References

[1] Jadhav Prachi Ashok,Tikone Anjali Balasaheb, Prof.Nawale S.K. on "Online Crime Reporting System", International Journal of Research Publication and Reviews,Vol 3, no 11, pp 2432-2435 November 2022

[2] S. Selvakani, K. Vasumathi, M. Harikaran on "Web Based Online Crime Reporting System using Asp.Net", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

[3] Nnadimma, Chisom ejike on "Design and implementation of an online crime reporting system" report submitted to the school of postgraduate studies,university of lagos in information technology january, 2018

[4] Ashwani Sharma, Bhuvanesh Kumar Sharma, Avdesh Bhardawaj "Design of a Novel Online Crime Reporting System" by International Conference on Engineering Technology and Science (ICETS'16)

[5] Tzay-Farn Shih , Chin-Ling Chen , Bo-Yan Syu and Yong- Yuan Deng on "A Cloud-Based Crime Reporting System with Identity Protection" mdpi.com/journal , Published: 18 February 2019.

[6] Eugene F. Ferraro, Morrison, "ANONYMOUS REPORTING SYSTEM " United States Patent Ferraro , Patent No.: US 9,135,598 B2

[7] Riya Lohan and Mr. Mahesh Singh "An Online Crime Reporting System" AITM Engineering College, Palwal Volume-4, Issue-6, June-2015 • ISSN No 2277 – 8160

[8] ArchanaM, Durga S and Saveetha K "Online Crime Reporting System" Special Issue Published in Int. Jnl. Of Advanced Networking Applications (IJANA)

© 2024, IJSREM | www.ijsrem.com DOI: 10.55041/IJSREM28167