JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybercrime Reporting Portal For Judiciary Law Using Smart City

[1]Prof.Thenmalar R, [2]Victoria Mary S, [3]Manoj Kumar B, [4]Swarnambika L

[1]Assistant Professor, [2]UG Student, [3]UG Student, [4]UG Student
[1]Department of Computer Science and Engineering,
[1]RVS College of Engineering and Technology, Coimbatore, India

Abstract : Taking care of cybercrime has become essential to contemporary urban administration in the age of swift digital transformation and the rise of smart cities. This project suggests creating a cybercrime reporting portal that is specifically tailored for smart city ecosystems and integrated with judicial law. The site makes it possible for citizens to report cybercrimes in a quick, safe, and effective way while making sure that the judicial system's legal framework is tightly incorporated into the procedure. In order to help law enforcement and judicial authorities handle cases quickly, the system makes use of smart city technologies like real-time data processing, geolocation monitoring, secure identification verification, and AI-based categorization. In the quickly changing digital world of today, the widespread use of the internet has resulted in a notable increase in cybercrimes, which can range from financial fraud and data breaches to identity theft and online harassment. As smart cities develop with interconnected infrastructures and integrated technology, maintaining digital safety becomes a top concern for municipal governance. This project suggests creating and deploying a cybercrime reporting portal that complies with legal requirements and is especially suited . The proposed site serves as a centralized, easily navigable digital platform that eliminates the need for citizens to physically attend police stations or courts in order to report cybercrime incidents. A cybercrime reporting portal that is integrated with judicial law and intended for smart city infrastructure is presented in this proposal. The portal's capabilities, which include geolocation tagging, AI-based crime classification, real-time tracking, and automatic case sending to cyber cells and judicial authorities, allow users to safely report cybercrimes online. Transparency, prompt action, and effective legal processing are all encouraged. The system also raises awareness and improves digital literacy by providing materials on user rights and cyber regulations. In an effort to create a more secure and intelligent digital society, the portal connects citizens, law enforcement, and the court by utilizing smart city technologies and digital governance principles.

Index Terms - Packet Sniffing, Network Security, IPTV Security, Cyber Threats, Intrusion Detection, Network Packet, Data Privacy, Unauthorized Access Prevention, Office Network Security.

I. INTRODUCTION

+ As a result of smart city projects and the quick development of technology, cybercrimes have grown to be a significant issue for both authorities and citizens. Many people cannot access traditional ways of reporting such crimes, and they are frequently delayed and ineffective. This project presents a cybercrime reporting portal that is tailored for smart city settings and integrated with the legislation. The portal provides users with a safe and practical means of reporting occurrences, monitoring the status of their cases, and obtaining legal advice. The system makes use of intelligent technologies like geo-tagging, real-time updates, and AI-based classification to guarantee a quicker response and improved communication between the public, law enforcement, and the courts. It seeks to improve legal transparency, public confidence in the legal system, and digital safety. As cities become smarter and more connected, cybercrime has also grown in complexity and frequency. There is a growing need for a modern, efficient, and accessible system to report and manage such digital threats. This project proposes a Cybercrime Reporting Portal designed to operate within a smart city framework, ensuring integration with judicial law and digital governance. The portal allows users to file complaints online, track case progress, and receive legal support. With features like AI-based analysis, geo-location, and automated case forwarding, it enhances transparency, accountability, and coordination between citizens, law enforcement, and the judicial system.

II. RELATED WORK

TITLE: Deep Learning Approach for Intelligent Intrusion Detection System
AUTHORS: R. Vinaya kumar , M. Alazab , K. Soman, P. Poornachandran, A. Al- Nemrat
PUBLICATION: IEEE Access,2019.

DESCRIPTION:

Deep learning's use to intrusion detection in cybersecurity systems is examined in this work. In smart surroundings, such as IoT devices and city infrastructures, it illustrates how neural networks can successfully detect and stop cyberattacks.

TITLE: Smart Cities Enabled Intrusion Detection System for IoT-Networks Using Machine Learning
AUTHORS: F. Farivar, M. S. Haghighi, A. Jolfaei
PUBLICATION: IEEE Access, 2019

DESCRIPTION:

A machine learning-based intrusion detection system tailored for Internet of Things networks in smart cities is proposed in this research. Through real-time detection of anomalous behaviours and possible threats, it focuses on enhancing the security of connected devices.

TITLE: Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review

AUTHORS: Elsaeidy, I. Elgendi, K.S. Munasinghe, D. Sharma

PUBLICATION: IEEE Access, 2023

DESCRIPTION:

In this research, incident response methods and cyber resilience techniques in smart cities are reviewed. In order to improve urban security systems, it pinpoints the best ways to guarantee the uninterrupted functioning and speedy restoration of city services after a cyberattack.

TITLE: Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey

AUTHORS: CytiD. Pera kovic B.B. Gupta

PUBLICATION: IEEE Access, 2021

DESCRIPTION:
The cybersecurity and forensic methods that are essential for safeguarding smart city infrastructures are reviewed in this study. It discusses methods for data integrity and cyber threat protection for urban digital systems, including detection, prevention, and investigative techniques.

III. EXISTING SYSYEM

I . Portal for Reporting Cybercrimes in India
The Ministry of Home Affairs launched this service, which enables people to report online harassment, identity theft, and financial fraud, among other cybercrimes. It provides a simple way to register concerns and monitor the progress of inquiries. For case monitoring and real-time data interchange, it isn't deeply integrated with smart city infrastructure.
II. E-Government Platforms (India and Worldwide)
E-governance systems have been adopted by numerous nations, including India, in an effort to improve public services. These tools make it easier to submit documents, obtain services, and report online. These platforms make things more accessible, but they are not usually completely connected with judicial systems for smooth legal processes, and they have limited use in reporting cybercrimes.
III. Description of Cyber Forensic Systems: In order to anayze digital evidence from devices such as computers, cell phones, and Internet of Things devices, law enforcement organizations employ sophisticated forensic systems. Despite having extensive data recovery and evidence processing capabilities, these systems are frequently cut off from citizen reporting portals and do not have real-time connectivity with smart city judicial operations.

IV. PROPOSED SYSTEM:

The proposed system is a Smart City-integrated Cybercrime Reporting Portal that bridges the gap between citizens, law enforcement agencies, and the judiciary. It enables users to securely report cybercrimes through an online platform with real-time features such as AI-based crime categorization, geo-tagging of incidents, and automated case forwarding to relevant cyber cells and judicial bodies.

4.1 An intelligent and secure user interface

It will offer citizens a user-friendly and secure platform for reporting cybercrimes. By logging in with a government-verified identity, like Aadhaar, users may guarantee permitted access. The primary design objectives will be accessibility for all citizens, especially those with limited technology skills, simplicity, and multilingual support.

4.2 Crime Categorization Using AI

Based on user input, content type, and keywords, the system will automatically analyse and categorize the cybercrime using AI algorithms after a complaint has been filed. This makes it possible to evaluate cases more quickly, prioritize risks that are considered serious, and accurately route cases to the relevant cybercrime cell or judicial body.

4.3 Case Monitoring and Alerts in Real Time

From registration through inquiry and legal action, the system will follow each complaint in real time. The legal process will be more transparent and trustworthy as a result of citizens receiving updates on the status of their cases via email or SMS.

4.4 Connecting to Smart City Infrastructure

IoT sensors, centralized data hubs, and surveillance systems are some of the smart city components that the portal will interface with. Automatic location tagging, quicker evidence gathering, and a comprehensive understanding of the digital risks threatening cities are all made possible by this. Rapid response and cyber safety

4.5 Legal Assistance and Judicial Process

The system will also have legal materials including user rights, sanctions, cyber law rules, and advice on being safe online. Every legitimate report will join the formal legal process swiftly and effectively thanks to its integration with judicial systems, which will advance cases for legal examination.

4.6 Data Security and Privacy Measures:

Strong cybersecurity and data privacy measures will be put in place by the suggested system to safeguard user data, including case-related data. National data protection rules will be adhered to by the portal, and all data will be encrypted from beginning to end. The implementation of multi-factor authentication (MFA),

.

V. RESEARCH METHODOLOGY

Using a methodical and planned approach, the research methodology for this project combines qualitative and quantitative techniques to guarantee the successful creation and validation of the suggested cybercrime reporting system.

..

5.1 Analysis Of Requirements

In order to comprehend current cybercrime reporting platforms, smart city technology, and legal procedures, a thorough investigation was carried out. Surveys, discussions with experts, and examination of existing platforms such as the National Cyber Crime Reporting Portal were used to gather data.

5.2 Design Of Systems

To design the architecture of the proposed system, tools from the Unified Modeling Language (UML) were used. Data flow diagrams (DFD), entity-relationship diagrams (ERD), and flowcharts were developed to illustrate modules including judicial integration, AI-based classification, and user registration.

5.3 Technology Stack Selection

Cloud services, PHP/Python, JavaScript, HTML/CSS, and MySQL were among the technologies chosen for their scalability, security, and ability to integrate with smart city infrastructure. For geotagging and classification, location-based APIs and AI libraries were selected.

Parameter	**Description**
Module Success Rate	(successful modules/total modules)*100
Vulnerabilities Detected	Detected Issues-Fixed Issues
User Satisfaction Score	(Positive feedback/Total Responses)*100
System Response Time	Total Response Time/Number of requests

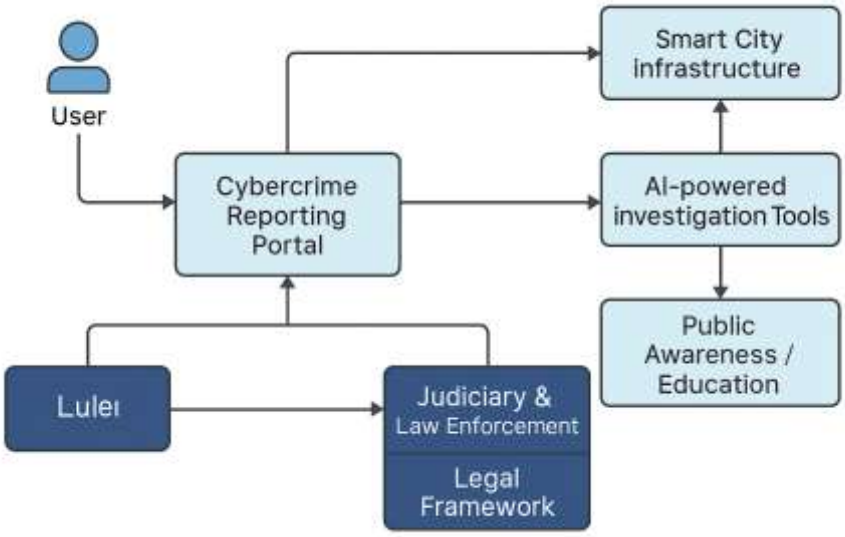
5.4 Implementation and Testing

A prototype of the portal was developed and tested in a simulated smart city environment. Various test cases were performed including functional testing, security testing, and usability testing to ensure the system works reliably under different scenarios.

5.5 System integration and Scalability

The suggested system is made to easily interface with the centralized data hubs, IoT devices, and surveillance cameras that are already part of the smart city infrastructure. Because it makes use of cloud-based technologies and open-source APIs, scalability as cities expand and the number of users increases is simple. Because of the system architecture's modularity, new features or security protocols can be implemented without interfering with already-existing services. The system's detection and reporting capabilities can be enhanced by incorporating machine learning models as cybercrimes change, guaranteeing its long-term efficacy.

VI. BLOCK DIAGRAM



A web portal or mobile app allows citizens to report cybercrimes through the Cybercrime Reporting Portal, a system integrated with smart cities. After gathering complaint information, such as location and proof, it employs artificial intelligence (AI) to classify the offense, give a priority, and route it to the appropriate law enforcement agency. While officers handle issues through a specialized dashboard, significant matters are sent to the courts via an e-Court system so that prompt legal action can be taken. Additionally, a Smart City Analytics Hub that records crime trends and produces insights for improved policymaking is connected to the platform. By facilitating real-time data sharing and automation, this system supports the judiciary and law enforcement while guaranteeing the prompt, transparent, and effective treatment of cybercrimes.

TECHNIQUES:

Blockchain For Evidence Integrity: Blockchain is a decentralized ledger technology that can be used to securely store and timestamp cybercrime evidence, such as screenshots, IP logs, emails, and chat histories. Once data is added to the blockchain, it cannot be altered or deleted, ensuring it remains tamper-proof.

Application in the System:

When a user reports a cybercrime, all related data and documents are hashed and stored on the blockchain.

Law enforcement and judiciary can access this immutable record to verify that evidence has not been tampered with.

AI-Based Case Categorization and Prioritization

Artificial Intelligence (AI) algorithms can automatically analyze incoming reports to categorize them and prioritize them based on severity or risk to public safety.

Combining Smart Surveillance with IoT

Internet of Things (IoT) gadgets and intelligent monitoring systems are essential for spotting questionable online activity in a smart city setting. Smart cameras, sensors, and automated traffic systems are examples of equipment that are able to identify and record anomalous digital activity, such as hacking attempts, unauthorized access, or tampering with vital infrastructure. Authorities can act swiftly by automatically sending the gathered data to central computers for reporting and analysis. The efficacy of reporting cybercrimes is improved by this real-time identification, which also helps stop serious threats before they become more serious.

Blockchain for Safe Evidence Management

In cybercrime cases,

the validity and integrity of digital evidence are among the main issues. Blockchain technology provides a tamper-proof way to store and validate data, which addresses this issue. When a cybercrime is reported, cryptographic hashes on the blockchain can be used to store evidence like screenshots, transaction logs, and IP addresses. This data is extremely dependable for use in legal proceedings since once it is entered, it cannot be altered. As a result, there is less possibility of fraud and manipulation and courts and investigators will be able to trust the evidence.

Processing Cases Automatically with Artificial Intelligence

Because AI automates case classification, analysis, and prioritization, it greatly increases the effectiveness of cybercrime management. Artificial intelligence (AI) systems determine the sort of crime, evaluate its urgency, and forward it to the proper authorities by analyzing the content of cybercrime complaints using machine learning and natural language processing. As a result, there is less manual labor required, reaction times are accelerated, and urgent cases are given prompt treatment. Furthermore, AI can assist in anticipating patterns and trends in cybercrime, hence bolstering proactive law enforcement tactics.

Jurisdictional Dashboard and Electronic Case Monitoring

To better monitor and handle cybercrime crimes, legal authorities should use a centralized judicial dashboard. Real-time updates on the status of each case are available on this dashboard, including information on court sessions, evidence logs, and investigation status. Using electronic case monitoring,

RESULT

Improved Reporting Efficiency: By allowing users to electronically register cybercrime concerns, the portal lowers the delays brought on by manual paperwork and in-person reporting. Faster Crime Categorization:

With AI-assisted classification, cybercrime cases are categorized quickly and accurately, allowing for faster prioritization and redirection to relevant departments. Improved Law Enforcement Coordination:

Real-time dashboards and automated updates help officers track case progress, assign tasks, and manage digital evidence efficiently. Seamless Judiciary Integration:

Through e-Governance connectivity, cases are forwarded to judicial systems automatically, reducing processing time and enhancing transparency. Enhanced Public Trust:

Users receive status updates and legal notifications, improving accountability and increasing public confidence in digital governance.

VII. CONCLUSION

E-Government systems for legal processing and artificial intelligence for criminal classification greatly improve the effectiveness, precision, and speed of cybercrime handling in smart cities. These methods facilitate smooth communication between the public, law enforcement, and the courts as well as automated case analysis and priority-based routing. Thus, in addition to enhancing public safety, the Cybercrime Reporting Portal also promotes an open and technologically advanced legal system.

VIII. FUTURE WORK

1. Predictive Analytics Integration: Make use of AI to predict patterns in cybercrime and facilitate preventative measures.
2. IoT and Surveillance System Linkage: For active monitoring, link the gateway to real-time city sensors and surveillance.
3. Blockchain for Evidence Security: Make use of blockchain technology to guarantee tamper-proof digital evidence storge.
4. Multilingual AI Chatbot Support: Use intelligent, multilingual chatbots to guide users.

IX. REFERNCE

1. Ministry of Home Affairs, Government of India – Cybercrime Reporting Portal
https://cybercrime.gov.in
2. National Crime Records Bureau (NCRB), India – Crime in India Reports
https://ncrb.gov.in
3. Ahmed, M., & Pathan, A. S. K. (2021). Security of Smart Cities: Challenges and Solutions. Springer.
ISBN: 9783030663851
4. Saini, H. S., Rao, Y. S., & Panda, T. C. (2012). Cyber-Crimes and Their Impacts: A Review. International Journal of Engineering Research and Applications, 2(2), 202-209.
5. Sharma, M., & Kaushik, A. (2020). AI-based Cybercrime Detection and Reporting Framework. Journal of Cyber Security Technology, 4(3), 157–173.
DOI: 10.1080/23742917.2020.1713513