EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

Department of CSE - (IoT & CSBT)
Jnana Prabha, Bidarahalli, Virgo Nagar Post, Bengaluru,
Karnataka - 560049

Synopsis on

"My City My Safety: Anonymous Crime Reporting System"

Domain: - Cyber Security, Blockchain, Machine Learning & Web Development

Team Members: -

M Prem Venkat (1EP22IC029)

Nisha K (1EP22IC035)

Niveditha C (1EP22IC036)

Syeda Saniya Khazi (1EP22IC054)

Abstract: -

SecureTip addresses the reluctance of witnesses to report crimes by providing a secure platform. Utilizing AES encryption for user-server communication, Blockchain for tamper-proof data storage, and Tensorflow CNN for accurate tip analysis, SecureTip ensures anonymity and reliability. Users can submit tips, including multimedia, with assurance of confidentiality. The system, built on Django, facilitates efficient data processing and load balancing, presenting tips in a tabular format with ML predictions. IPFS manages multimedia data securely. Authorities access a comprehensive dashboard, anonymized user lists, and training options for ML algorithms, ensuring prompt response to reported activities. SecureTip enables users to report suspicious activities anonymously, mitigating fears of reprisal. The integration of encryption, Blockchain, and ML ensures data security and accurate analysis. The system fosters trust between authorities and the community, enhancing crime prevention efforts.

Keywords: -

Blockchain, Crime Reporting, Anonymity, Security, Decentralization, Smart Contracts, Cryptography, Law Enforcement.

Introduction: -

The reluctance of witnesses to report suspicious activities due to fears of retaliation or privacy breaches. This innovative platform addresses the critical need for a secure and anonymous channel for individuals to provide crucial information to law enforcement agencies.

In today's digital age, traditional reporting methods often fall short in ensuring the confidentiality and integrity of reported data. With SecureTip, we introduce a paradigm shift by leveraging cutting-edge technologies such as AES encryption, Blockchain, and Tensorflow CNN. These technologies work seamlessly together to create a robust and secure environment where users can submit tips with confidence, knowing that their identity and information are protected.

By harnessing the power of AES encryption, SecureTip safeguards communication between users and the server, preventing unauthorized access to sensitive data. The integration of Blockchain technology ensures tamper-proof storage of tip details, guaranteeing the integrity of reported information. With its user-friendly interface and comprehensive features, SecureTip empowers individuals to play an active role in crime prevention without fear of repercussions.

Literature Survey: -

- K-Anonymity for Privacy Preserving Crime Data Publishing in Resource Constrained Environments:
  https://ieeexplore.ieee.org/document/6844743
- Toward an mPolicing solution for Namibia: Leveraging emerging mobile platforms and crime mapping:
  https://www.researchgate.net/publication/262166703_Toward_an_mPolicing_solution_for_Namibia_Leveraging_emerging_mobile_platforms_and_crime_mapping
- When crime reporting goes high-tech: An experimental test of computerized citizen response to crime:
  https://www.sciencedirect.com/science/article/abs/pii/0047235295000437
- Feature Based Training for Crime Detection using Deep Learning Techniques:
  https://ieeexplore.ieee.org/document/10369315
- Deep Convolutional Generative Adversarial Networks for Crime Scene Object Detection:
  https://ieeexplore.ieee.org/document/10250517

Existing System: -

Existing surveillance systems often rely on manual monitoring, which is labor-intensive and prone to human error, especially given the volume of data and the rarity of suspicious activities compared to routine occurrences. Traditional surveillance methods are inadequate in efficiently identifying potential threats such as gun-based crimes and abandoned luggage, which pose significant risks to human safety. With the advent of intelligent surveillance systems, various technological approaches have been introduced, but many still fall short in terms of accuracy and real-time detection capabilities. Current solutions often lack the advanced analytical power needed to effectively discern critical threats from ordinary activities. This inadequacy necessitates the development of more sophisticated systems that leverage deep learning and computer vision to enhance the detection and response to high-risk situations in surveillance footage

Proposed System: -

The proposed system, SecureTip, revolutionizes crime reporting by offering a secure platform for anonymous tip-offs. Employing cutting-edge technologies, including AES encryption for secure communication and Blockchain for tamper-proof data storage, SecureTip ensures confidentiality and integrity of user information. Multimedia files can be uploaded alongside tips, enhancing reporting accuracy. Powered by Django, the system facilitates efficient data processing and presentation, with tips displayed in a tabular format, including ML predictions. IPFS securely stores multimedia data, enhancing overall system security. For authorities, SecureTip provides a comprehensive dashboard for managing reported activities, training ML algorithms for accurate analysis, and accessing anonymized user lists. By enabling safe and anonymous reporting, SecureTip bridges the gap between witnesses and authorities, fostering community trust and enhancing crime prevention efforts.

Requirements Specification: -

- **Hardware Requirements:**

1) **Operating System:** Windows Only
2) **Processor:** i5 and above
3) **Ram:** 8GB and above
4) **Hard Disk:** 25 GB in local drive

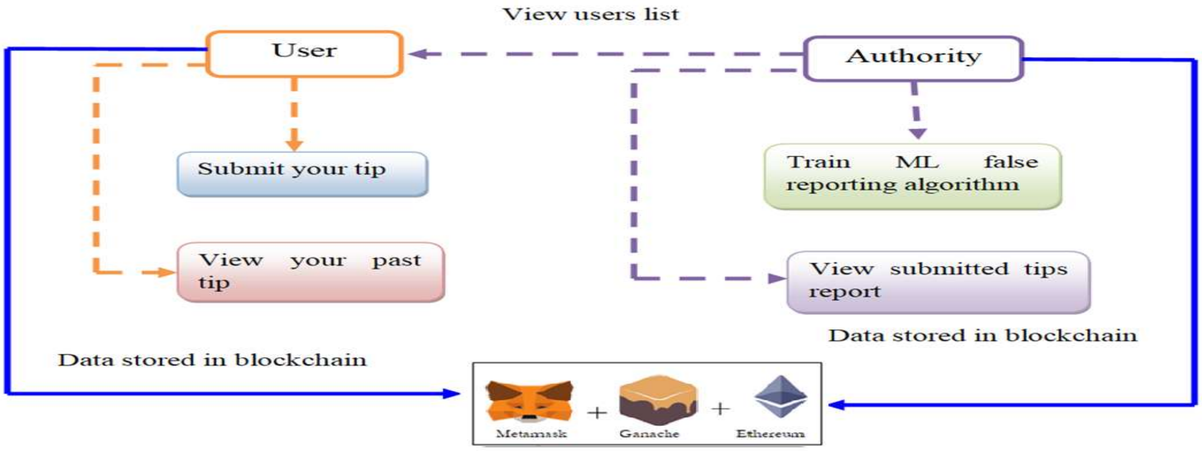
- **Software Requirements:**

1) PYTHON IDLE (3.7.0)
2) Node JS
3) Visual Studio Community Version
4) Ganache
5) **Metamask:** Chrome extension
6) **Languages Back-end:** Python, Java Script, Solidity
7) **Languages Front-end:** HTML, CSS, JS, Boot Strap
8) **Framework:** Flask

Methodology: -

- **Blockchain Setup:** Deploy a private/public blockchain network for secure crime reporting.
- **Smart Contracts:** Develop contracts to handle report submission, verification, and status tracking.
- **Anonymous Reporting:** Utilize Cryptographic techniques for anonymity.
- **Data Security:** Encrypt sensitive data before storing on-chain.
- **Access Control:** Implement role-based access for law enforcement to decrypt reports.
- **User Interface:** Build a web/mobile application for easy reporting and tracking.
- **Testing & Deployment:** Security audits, stress tests, and final deployment.

System Architecture:-


View users list
User
Authority
Submit your tip
Train ML false reporting algorithm
View your past tip
View submitted tips report
Data stored in blockchain
Data stored in blockchain
Metamask
+
Ganache
+
Ethereum

Expected Results: -

- Secure and anonymous crime tip-offs.
- Immutable crime records preventing data manipulation.
- Increased public trust in crime reporting.
- Faster and more reliable response from law enforcement.

Conclusion: -

This blockchain-based system provides a secure and anonymous way to report suspicious activities while ensuring the integrity of submitted reports. By leveraging decentralization, cryptographic security, and smart contracts, the system enhances trust in law enforcement and promotes a safer society. A secure crime tip-off system enhances public participation in crime prevention while addressing safety and privacy concerns. By leveraging encryption, blockchain, and AI, we can create a more reliable and effective reporting mechanism that empowers citizens and supports law enforcement agencies.

References: -

- **Burke Mark-John and Kayem Anne V.D.M., (2014) “K-Anonymity for Privacy Preserving Crime Data Publishing in Resource Constrained Environments.”** In the 8th International Symposium on Security and Multinodality in Pervasive Environments, (SMPE 2014), Victoria, Canada - May 13-16, 2014
- **Jensen, K. L., Iipito, H. N., Onwordi, M. U. and Mukumbira, S. (2012). “Toward an mPolicing solution for Namibia: leveraging emerging mobile platforms and crime mapping.”** In Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference (pp. 196-205). ACM.
- **Lasley, J.R. and Palombo, B.J. (1995). “When crime reporting goes high-tech: An experimental test of computerized citizen response to crime.”** Journal of Criminal Justice, 23(6), pp. 519-529.
- **P. Mahalakshmi, S. Thenmalar, "Feature Based Training for Crime Detection using Deep Learning Techniques", 2023** International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), pp.1-4, 2023.
- **Uma N, "Deep Convolutional Generative Adversarial Networks for Crime Scene Object Detection", 2023** Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), pp.616-620, 2023.