EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institute, Affiliated to VTU, Belagavi) Jnana Prabha, Bidarahalli, Bengaluru-49
Approved by AICTE, New Delhi & Government of Karnataka Accredited by NBA (CSE, ECE & ISE) and NAAC with **A** Grade

Project Presentation
On
"My City My Safety: Anonymous crime reporting Network"

By

M Prem Venkat (1EP22IC029)
Nisha K (1EP22IC035)
Niveditha C (1EP22IC036)
Syeda Saniya Khazi (1EP22IC054)

Under the Guidance of

Dr. Nanda Ashwin
Professor & HOD

Department of
CSE – (IoT & CSBT)

www.eastpoint.ac.in

Contents

Introduction

Crime reporting is crucial for public safety, but traditional methods often fall short in ensuring the confidentiality and integrity of reported data. This innovative platform addresses the critical need for a secure and anonymous channel for individuals to provide crucial information to law enforcement agencies. 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. Additionally, Tensorflow CNN enhances the accuracy of tip analysis, enabling law enforcement to effectively prioritize and respond to reported activities.

With its user-friendly interface and comprehensive features, SecureTip empowers individuals to play an active role in crime prevention without fear of repercussions. By fostering trust and cooperation between the community and law enforcement, SecureTip heralds a new era of collaborative crime-fighting efforts, ultimately leading to safer and more secure communities.

Literature Survey

- Burke Mark-John and Kayem Anne V.D.M., (2014) “K-Anonymity for Privacy Preserving Crime Data Publishing in Resource Constrained Environments”. https://ieeexplore.ieee.org/document/6844743

- Jensen, K. L., Iipito, H. N., Onwordi, M. U. and Mukumbira, S. “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

- Lasley, J.R. and Palombo, B.J. “When crime reporting goes high-tech: An experimental test of computerized citizen response to crime”. https://www.sciencedirect.com/science/article/abs/pii/0047235295000437

- P. Mahalakshmi, S. Thenmalar, "Feature Based Training for Crime Detection using Deep Learning Techniques“. https://ieeexplore.ieee.org/document/10369315

- Uma N, "Deep Convolutional Generative Adversarial Networks for Crime Scene Object Detection". https://ieeexplore.ieee.org/document/10250517

Proposed Method

The proposed method, 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.

Objectives

- The main goal of this project is to build a more secure, faster, and highly trustworthy platform for reporting suspicious activities to crime-prevention authorities. The system focuses on protecting the identity of the person submitting the tip, preventing tampering of information, and verifying the authenticity of the data being submitted.
- To achieve this, the project uses AES encryption to fully safeguard the reporter's personal information. This ensures that any sensitive details remain hidden during transmission, so no unauthorized party can intercept or reveal the identity of the person providing the tip.
- Utilizing blockchain to store the tips on a blockchain, so no one can change them, ensuring that the information stays accurate and trustworthy.
- Integrating Tensorflow CNN to automatically check if the information provided is true.
- Employing IPFS for a system to store things like images or videos linked to the tips, making sure they are easy to access.

Motivation

- The motivation behind this project comes from the growing need for a safe and trustworthy way for citizens to report suspicious activities.
- In many cases, people hesitate to approach authorities because they fear exposure, retaliation, or misuse of their personal information.
- At the same time, law enforcement struggles with unreliable or manipulated data, making it harder to act on genuine threats.
- Seeing these problems pushed us to design a system that protects identities, prevents tampering, verifies information using AI, and securely stores evidence.
- The goal was simple: build a platform where people feel safe to speak up, and authorities receive accurate, dependable reports that can actually help prevent crime.

Challenges

- **Keeping Users Anonymous:**
  We didn’t want to store any personal information that could reveal who sent the tip.

- **Tip Submission Was Slow:**
  It took time for the blockchain to confirm that the tip was submitted, which confused users.

- **High Blockchain Costs:**
  Saving too much data on the blockchain was expensive (in terms of gas fees).

- **Keeping the Authority Dashboard Secure:**
  We didn’t want unauthorized people to access sensitive tip information.

Applications

- **Anonymous Crime Reporting:**
  Citizens can safely report suspicious activities without revealing their identity, thanks to AES encryption and secure data transmission.

- **Tamper-Proof Evidence Storage:**
  Tips stored on the blockchain cannot be edited or deleted, making them reliable sources of evidence for law enforcement agencies.

- **Automated Verification of Reports:**
  A TensorFlow CNN model can analyze submitted information (text, images, or patterns) to filter out false or misleading reports before authorities act on them.

- **Enhanced Public Safety Platforms:**
  The system can be integrated into apps, websites, or police portals to build a more trustworthy and transparent public safety ecosystem.

Hardware & Software Requirements

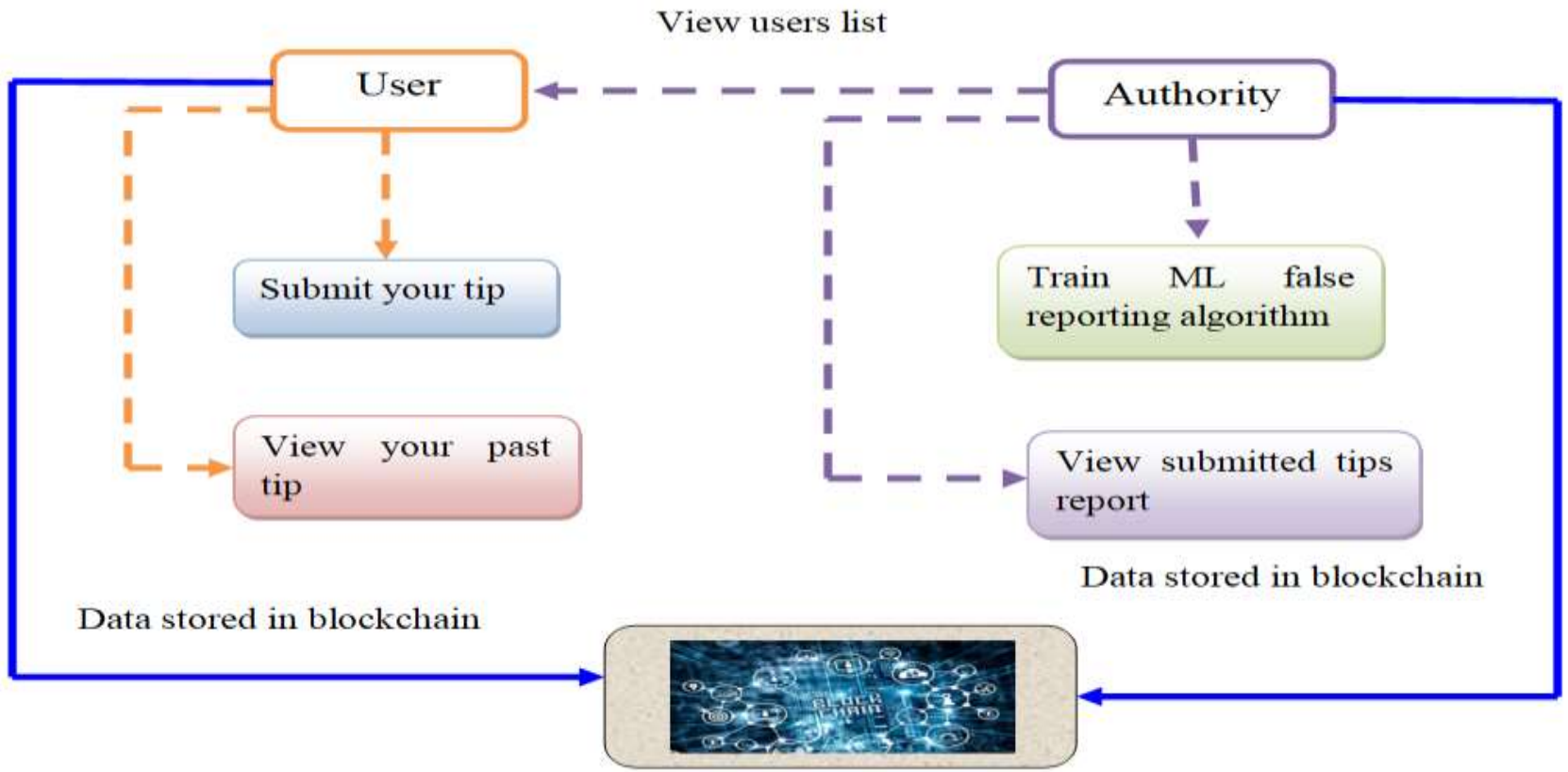
Hardware Requirements:

- Windows with i5 and above.
- Min 8GB RAM and 25 GB in local drive.

Software Requirements:

- Python Idle.
- Ganache.
- Metamask Chrome extension.
- Back-end:- Python, Java Script, Solidity.
- Front-end:- HTML, CSS.

Architecture



Algorithm Used

- **Input Collection:**
  The user submits a suspicious activity tip along with optional images or videos.

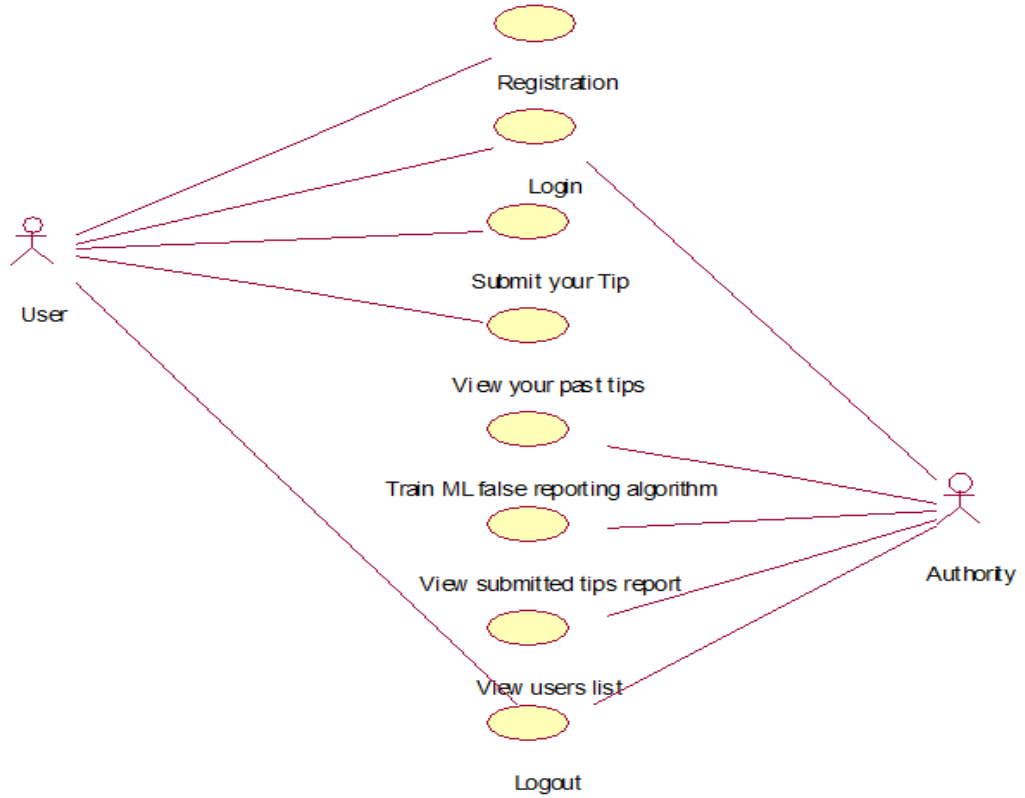
- **AES Encryption Process:**
  The user's personal details are encrypted using the AES algorithm where a secret key is generated to convert the identity information into unreadable ciphertext, ensuring anonymity.

- **Decentralized File Storage (IPFS):**
  IPFS generates a unique content hash which is used as a permanent reference to the files.

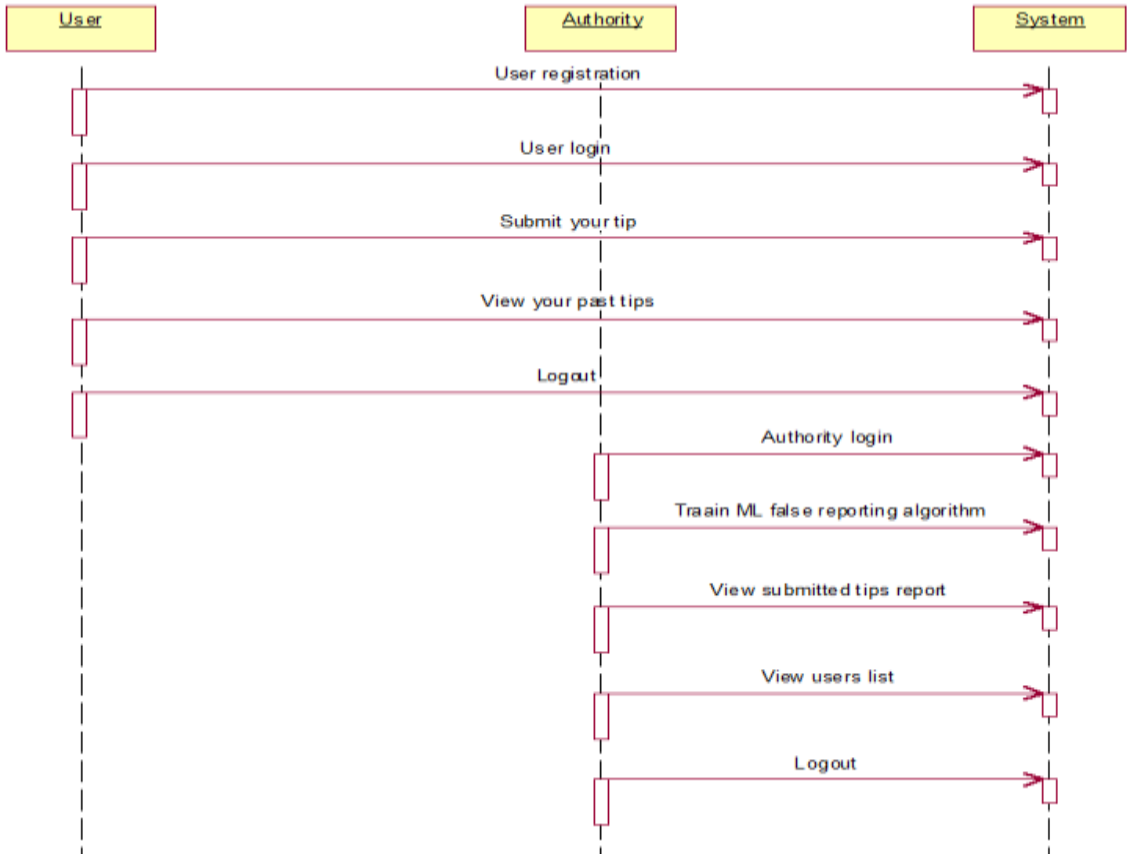
- **Blockchain Recording:**
  The encrypted tip and the IPFS hash are stored on a blockchain, each entry becomes immutable, meaning no one can alter or delete the report.

- **Result Generation:**
  Authorities receive secure access to the blockchain entry and IPFS media.

Use Case Diagram



Sequence Diagram



Implementation

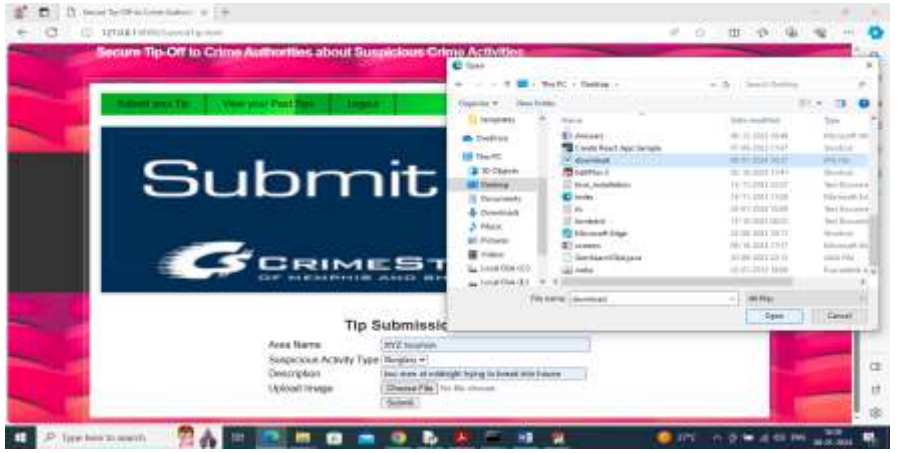
- First go inside ‘hello-eth/node-modules/bin’ folder and then find and double click on ‘runBlockchain.bat’ file to start Ethereum tool and then the cmd prompt will open with the default private keys.
- Now type command as ‘migrate’ and press enter key to deploy contract.
- A new page will appear with white colour text that displays ‘Smart Contract’ deployed and gives the contract address where this address should be specified in the python code to save and get details from Thorium.

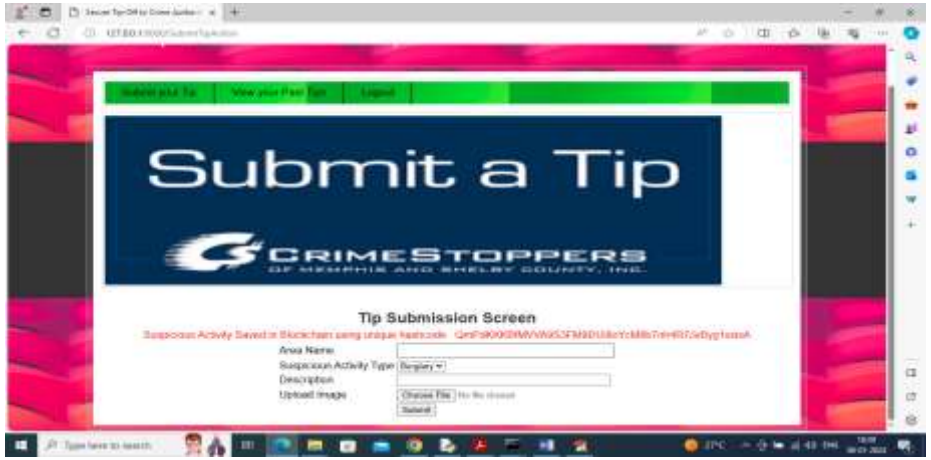
To implement this we have designed following modules

- **New User Sign up:** Using this module user can sign up with the application.
- **User Login:** Using this module user can login to application and all user details will be managed with server in AES encrypted format.
- **Submit your Tip:** After login using this module user can submit tip about any suspicious activities.
- **View your Past Tips:** Using this module user can view all submitted tip reports.
- **Authority Login:** Authority can login to system using username and password as ‘admin’. After login authority can perform following options.
- **Train ML:** Using this module authority can train ML to predict weather submitted tip is false or true.
- **View Submitted Tips Report:** Using this module authority can view all submitted tips and ML predicted top status as true or false.
- **View User Lists:** Using this module authority can view all registered user details but all username will be anonymised for security reason.

Results


Secure Tip-Off to Crime Authorities about Suspicious Crime Activities
Submit a Tip
CRIMESTOPPERS
User Login Screen

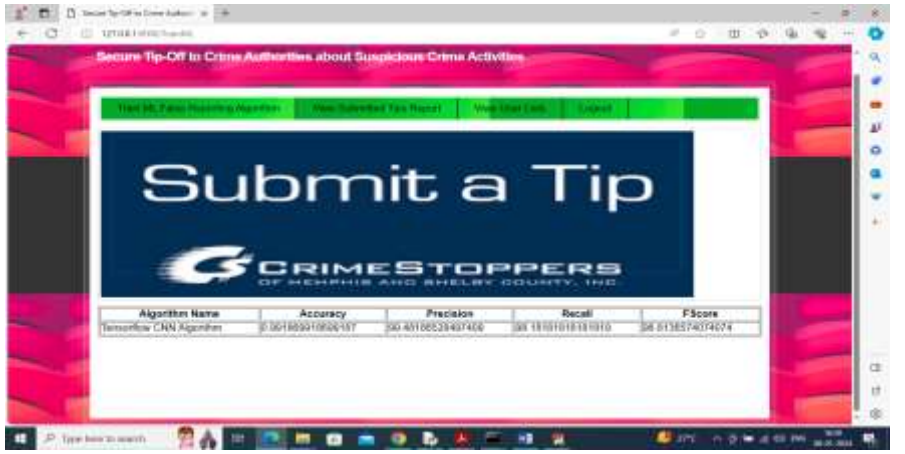

Secure Tip-Off to Crime Authorities about Suspicious Crime Activities
Submit


Submit a Tip
CRIMESTOPPERS
Tip Submission Screen


Submit a Tip
CRIMESTOPPERS
Username
Suspicious Activity Address
Type of Activity
Tip Description
Hashcode
Tip Date
Predicted Report Status
Tip Image

Results


Secure Tip-Off to Crime Authorities about Suspicious Crime Activities
Submit a Tip
CRIMESTOPPERS
Authority Login Screen


Secure Tip-Off to Crime Authorities about Suspicious Crime Activities
Submit a Tip
CRIMESTOPPERS
Algorithm Name
Accuracy
Precision
Recall
FScore


Submit a Tip
CRIMESTOPPERS
Username
Suspicious Activity Address
Type of Activity
Tip Description
Hashcode
Tip Date
Predicted Report Status
Tip Image


Secure Tip-Off to Crime Authorities about Suspicious Crime Activities
Submit a Tip
CRIMESTOPPERS
Username
Password
Contact No
Gender
Email ID
Address

Result Analysis

- The developed system successfully demonstrates a secure and reliable platform for reporting suspicious activities. AES encryption effectively protected user identity during data submission, ensuring that no personal information could be intercepted or exposed.
- Storing reports on the blockchain proved highly effective—data remained immutable, and every tip carried a verifiable timestamp, improving trust and transparency.
- IPFS storage showed strong performance for handling images and videos, with fast retrieval and no dependency on a central server.
- The TensorFlow CNN model achieved consistent accuracy in validating the credibility of submitted information, reducing false alerts.
- Overall, the integrated system performed smoothly, providing a secure, tamper-proof, and efficient reporting framework suitable for real-world implementation.

Conclusion

- The project provides a robust platform that allows witnesses to report suspicious activities anonymously, ensuring their safety while enhancing collaboration with law enforcement.
- By leveraging Ethereum blockchain, the system ensures that crime reports remain immutable and tamper-proof, fostering trust between users and authorities.
- The TensorFlow CNN model improves the credibility of reported tips by analyzing and predicting their authenticity, helping authorities prioritize genuine cases efficiently.
- With IPFS for decentralized multimedia storage, the system securely handles evidence, preserving crucial information for investigations.
- By integrating encryption, blockchain, machine learning, Ganache, and MetaMask, the system enhances the security, efficiency, and accuracy of crime reporting, contributing to faster responses from authorities and ultimately safer communities.

References

- Burke Mark-John and Kayem Anne V.D.M., (2014) “K-Anonymity for Privacy Preserving Crime Data Publishing in Resource Constrained Environments”, May 13-16, 2014.
- Jensen, K. L., Iipito, H. N., Onwordi, M. U. and Mukumbira, S. “Toward an mPolicing solution for Namibia: leveraging emerging mobile platforms and crime mapping”, 2012.
- Lasley, J.R. and Palombo, B.J. “When crime reporting goes high-tech: An experimental test of computerized citizen response to crime”, 1996.
- P. Mahalakshmi, S. Thenmalar, "Feature Based Training for Crime Detection using Deep Learning Techniques“, 2023.
- Uma N, "Deep Convolutional Generative Adversarial Networks for Crime Scene Object Detection", 2023.

Thank you!