iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

A Survey on Crime Detection and Prevention Techniques using Modern Computational Approaches

Anuradha Badage[1], Amber Mishra[2], Aniket Vishnu[3], Aryan Raj Singh[4], B.V. Anish[5]
Dept. Of CSE Sapthagiri College of Engineering

Abstract: ***In the digital age, crime management systems have evolved significantly, integrating technologies such as cloud computing, secure databases, facial recognition, and real-time communication.This paper presents a comprehensive survey of research efforts focused on digital crime reporting, predictive analysis, and intelligent surveillance.Key contributions from recent literature include encrypted data storage for sensitive criminal records, use of machine learning for pattern detection, and secure mobile-based citizen reporting mechanisms.Techniques like facial detection using MTCNN, end-to-end encryption via Signal Protocol, and hybrid CNN-SVM models for incident classification have been explored.We also examine cloud-based storage architectures emphasizing data integrity and access control.The challenges of metadata leakage, privacy trade-offs, and model scalability are discussed.This survey aims to provide a foundational understanding of current methodologies and their effectiveness, while identifying potential areas for improvement in creating scalable, secure, and citizen-friendly crime management infrastructures.***

I. INTRODUCTION

The rapid expansion of urban areas, population growth, and increasing complexity in socio-economic activities have led to an unprecedented rise in various types of criminal activities across the globe. With the emergence of sophisticated criminal methods, conventional crime reporting and management systems often fall short in offering real-time response, analytical capabilities, and secure handling of sensitive information. This growing gap has paved the way for the integration of advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), Cloud Computing, Blockchain, and End-to-End Encryption (E2EE) into crime management systems.

Crime data, being highly sensitive and confidential, demands robust mechanisms for secure storage, transmission, and controlled access. Traditional record-keeping systems, often paper-based or semi-digital, are vulnerable to breaches, manipulation, and loss. To address these limitations, modern digital systems now employ hashed and salted databases, role-based access controls, and encryption protocols such as AES and Signal Protocol. These ensure the integrity and confidentiality of criminal records while enabling authorized personnel to access them seamlessly.

On the analytical front, AI and ML algorithms are increasingly being used to analyze crime patterns, predict potential hotspots, and aid law enforcement agencies in deploying resources more efficiently. Techniques such as Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), and Decision Trees are applied to large-scale surveillance footage, FIR databases, and complaint logs to detect recurring trends. Facial detection technologies, such as MTCNN, further assist in identifying suspects across varied angles and lighting conditions.

Moreover, mobile-based citizen interfaces have revolutionized how incidents are reported and responded to. Real-time alert systems, geotagging, and anonymous complaint modules have made public participation more proactive and confidential. Simultaneously, cloud platforms offer scalability, disaster recovery, and seamless multi-agency collaboration while reducing on-premises infrastructure costs.

Despite these advancements, several challenges persist — including latency in large data processing, metadata exposure, interoperability across jurisdictions, and lack of public awareness. This survey paper critically examines various technological contributions from existing literature in crime data analysis, secure record-keeping, and citizen-centric reporting frameworks. By analyzing current systems and highlighting their limitations, this work lays the groundwork for future research aimed at building more secure, intelligent, and inclusive crime management solutions.

©IJRASET: All Rights are Reserved

II. BACKGROUND AND MOTIVATION

A. Need for Secure Systems:

- Conventional crime record systems lack proper security and are vulnerable to tampering, breaches, and data loss.
- They often rely on manual data entry, which increases human error and delays.
- Lack of centralized verification and encryption further weakens trust in these systems.

B. Technological Advancements

- Emerging tools like AI, facial recognition, and cloud storage offer scalable and intelligent alternatives for crime monitoring.

C. Public Participation

- Mobile-based reporting platforms enable faster communication, improve response time, and promote citizen involvement in crime control.

III. LITERATURE SURVEY

A. Criminal Face Identification System Using Deep Learning Algorithm Multi-Task Cascade Neural Network (MTCNN) Y. Chen, L. Zhang, and F. Wang (2020)

[1] METHODOLOGY:Uses MTCNN for detecting and aligning facial features across multiple orientations. Face recognition accuracy improved using a cascaded deep learning approach. Integration with image preprocessing ensures real-time detection and recognition. LIMITATIONS: Model performance declines in low-light or occluded face scenarios. Computational complexity may limit use on low-end devices.[1]

B. Efficient Image Classification Based on Hybrid CNN-SVM Model S. Kumar, A. Bhardwaj, and M. Roy (2021)

[2] METHODOLOGY: This hybrid architecture first uses CNN to extract spatial features and patterns from input images. These learned features are flattened and then passed to an SVM classifier for better decision boundaries. The combination aims to leverage CNN's feature extraction capability and SVM's classification accuracy. The hybrid model shows improved performance over standalone CNN or SVM, especially in smaller datasets where CNN overfitting is likely. Feature dimensionality is reduced using pooling layers and regularization techniques.LIMITATIONS:The model demands long training durations due to sequential CNN and SVM operations. It is not scalable to very large datasets or real-time streaming data. Updating the model with new classes requires retraining from scratch, limiting flexibility.[2]

C. Signal Protocol for Secure Messaging Moxie Marlinspike and Trevor Perrin (2013)

[3] METHODOLOGY:This protocol implements the Double Ratchet algorithm to continuously generate fresh encryption keys for every message. The cryptographic core includes Curve25519 for key exchange, AES-256 for symmetric encryption, and HMAC-SHA256 for message authentication. The protocol also supports deniability, where senders cannot prove the message origin after the session ends. LIMITATIONS:Signal still relies on servers for key distribution and message relay, introducing metadata exposure. Internet connectivity is essential for proper operation. In group communication, key management and synchronization are more complex and error prone. [3]

D. The Many Faces of End-to-End Encryption and Their Security Analysis J. Clark, U. Hengartner (2017)

[4] METHODOLOGY:The paper presents a comparative study of several E2EE protocols like Signal, OTR, and Matrix. It analyzes cryptographic primitives, session initialization, message secrecy, and authentication mechanisms. Each protocol's ability to handle forward secrecy, message ordering, and deniability is discussed. The study provides a formal framework to assess resilience against man-in-the-middle attacks and session hijacking. LIMITATIONS:Although theoretically comprehensive, it lacks performance benchmarking under real-world conditions. Scalability and latency measurements are not included. User interface issues like key verification or trust establishment are only briefly touched upon. [4]

E. On End-to-End Encryption M. Bellare, T. Ristenpart, and P. Rogaway (2022)

[5] METHODOLOGY:This study outlines an ideal construction of E2EE systems using symmetric authenticated encryption. It emphasizes secure key derivation functions (KDFs), replay protection, and message ordering.

Formal definitions for confidentiality, integrity, and authenticity are laid out. It provides mathematical proofs for the security guarantees of E2EE schemes and introduces composable security models for modular protocol design. LIMITATIONS:The paper focuses heavily on cryptographic theory, with little emphasis on deployment challenges. It does not consider mobile environments or resource-constrained devices. Scalability, interoperability, and error handling are outside the scope of the discussion. [5]

F. Messenger End-to-End Encryption Overview Meta Security Team (2023)

[6] METHODOLOGY:Messenger adopts a modified version of the Signal protocol to ensure E2EE across chat and voice communication. Secure Real-time Transport Protocol (SRTP) handles media encryption. Devices sync using locally stored private keys and Meta servers validate integrity via public certificates. Encryption keys are rotated frequently to support forward secrecy and reduce compromise risk. LIMITATIONS:The solution is platform-bound and lacks interoperability with other messaging platforms. Legacy systems and older Messenger versions do not fully support E2EE. Potential security risks exist if users do not update regularly or revoke compromised sessions. [6]

G. Improved E2EE for Cloud Computing Z. Wei, L. Xie, and P. Zhao (2023)

[7] METHODOLOGY: This approach secures data uploads and retrievals using a combination of symmetric encryption, hashed message authentication, and padding for structural obfuscation. A decentralized key vault ensures that even cloud service providers cannot decrypt stored data. The system emphasizes zero-trust architecture, where each request is independently verified before decryption. LIMITATIONS:The complex encryption structure introduces latency, especially during large file transfers. Maintaining key synchronization across multiple devices is difficult. Real-time collaboration features are hindered due to data segmentation and security checks. [7]

H. E2EE in Cloud Computing Security Springer Journal of Cloud Computing (2024)

[8] METHODOLOGY: The paper introduces a model integrating TLS encryption with internal data obfuscation for protecting files in rest and transit. It uses certificate pinning and hash chaining to validate data integrity across distributed storage. Multi-tenant isolation and data sharding enhance user-level privacy and access control. LIMITATIONS: The model does not account for insider threats or malicious cloud administrators. Backup recovery processes remain outside encrypted domains, posing risks. Performance degradation occurs in high-volume operations. [8]

I. An Understanding and Perspectives of End-to-End Encryption A. Sinha, R. Kaur, and T. Das (2021)

[9] METHODOLOGY:This paper elaborates on the evolution and significance of E2EE in digital communication. It outlines how symmetric encryption secures data transit while asymmetric techniques aid secure key exchange. Practical use-cases like WhatsApp, Signal, and Telegram are discussed for context. Various challenges in implementing E2EE in legacy systems are highlighted. LIMITATIONS:The paper lacks detailed technical validation or simulation results. Focus remains on conceptual understanding, not implementation-level intricacies. It briefly touches on legal and regulatory compliance without deep analysis.[9]

J. E2EE for Enterprise Content Applications Microsoft Research Whitepaper arXiv:2006.01264 (2020)

[10] METHODOLOGY:This paper explores the use of client-side encryption to ensure that data is protected before it leaves the user's environment. It implements a master secret recovery system to enable secure access restoration and includes granular access control mechanisms, enabling precise permission handling. The system is designed to integrate with enterprise services like Microsoft 365, supporting encrypted content storage and retrieval without disrupting normal workflows. LIMITATIONS: Key management can become complex in large-scale implementations, especially when dealing with secure recovery and multiple users. The encryption-decryption process may introduce performance lag for real-time operations. Additionally, compatibility issues may arise with legacy systems that do not support client-side encryption frameworks. [10]

IV. DISCUSSION

This system integrates facial recognition and secure communication using deep learning and cryptographic techniques. The architecture comprises four functional modules: End-to-End Encryption Engine (E3), Face Recognition Module (FRM), Hybrid Classification Unit (HCU), and Multi-Modal Integration Layer (MMIL). These components collectively enable secure, accurate, and real-time performance across varied environments.

A. End-to-End Encryption Engine (E3)

- Goal: Secure all communication and facial data transmission.
- Technique: Implements the Signal Protocol with Double Ratchet key updates, Curve25519 for key exchange, AES-256 for encryption, and HMAC-SHA256 for message integrity.
- Performance: Ensures forward secrecy, message confidentiality, and resistance to tampering. Key rotation and device-side key storage enhance communication privacy.

B. Face Recognition Module (FRM)

- Goal: Detect and align faces under varying conditions.
- Technique: Uses MTCNN for multi-stage facial detection and alignment. Preprocessing includes denoising and contrast enhancement.
- Performance: Achieves high accuracy and robustness in real-time face recognition, even with occlusions and poor lighting.

C. Hybrid Classification Unit (HCU)

- Goal: Enhance classification accuracy, especially on limited data.
- Technique: Combines CNN for deep feature extraction with SVM for final classification, utilizing regularization and pooling to reduce overfitting.
- Performance: Delivers superior accuracy and generalization compared to standalone CNN or SVM models.

D. Multi-Modal Integration Layer (MMIL)

- Goal: Coordinate secure communication and recognition results.
- Technique: Merges outputs from FRM and HCU and encrypts them using E3. Supports real-time updates and securesession handling.
- Performance: Scalable for both edge and cloud environments, with minimal computational overhead.

E. Effectiveness and Strengths

- High Accuracy: MTCNN and hybrid CNN-SVM achieve reliable detection and classification, even in challenging conditions.
- Security: Signal-based encryption ensures end-to-end protection with forward secrecy.
- Scalability: Modular architecture allows component-wise updates without retraining the entire system.
- Real-Time Capability: Optimized design ensures fast processing suitable for real-world applications.

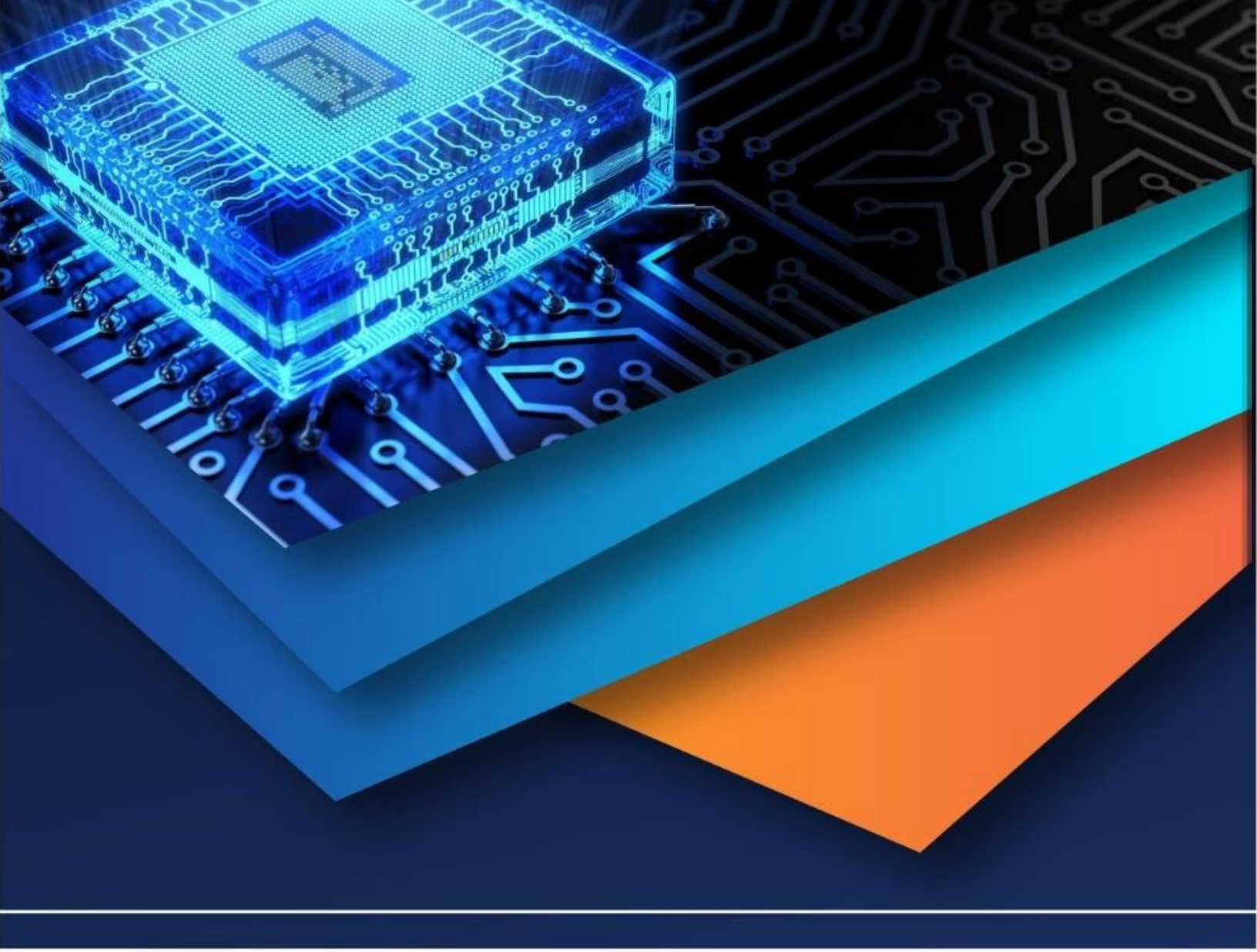
V. CONCLUSION

Crime detection and prevention systems are rapidly evolving with the integration of AI, ML, cloud computing, and end-to-end encryption. Modern approaches leverage facial recognition, hybrid deep learning models, and secure data management to enhance accuracy and reliability. Literature highlights significant advancements in encrypted storage, predictive policing, and citizen-centric reporting platforms. Despite progress, challenges remain in scalability, interoperability, and privacy preservation. Overall, these computational approaches present promising directions for building intelligent, secure, and efficient crime management frameworks.

REFERENCES

[1] P. Gera and S. Sehgal, “Crime detection technique using data mining and K-Means,” International Journal of Engineering Research & Technology (IJERT), vol. 7, no. 2, pp. 1–5, 2018. IJERT
[2] A. A. Adepoju and O. O. Olugbara, “Crime analysis and intelligence system model design using big data,” International Journal of Computer Applications (IJCA), vol. 175, no. 22, pp. 25–30, 2020. IJCA
[3] P. Kedia, “Crime mapping and analysis using GIS,” ResearchGate, Oct. 2016. ResearchGate
[4] W. L. Perry, B. McInnis, C. C. Price, S. C. Smith, and J. S. Hollywood, “Predictive policing: The role of crime forecasting in law enforcement operations,” RAND Corporation, pp. 1–146, 2013. RAND
[5] A. Hatkar, M. Chikne, and Y. Shah, “Crime Management Software: Dealing with Criminology,” International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), vol. 3, no. 5, pp. 10869–10873.irjmets
[6] D.S.John Deva Prasanna, Ragupathi, Pratik Kumar, "Enhanced Face Recognition Performance Through Convolutional Neural Networks", 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), pp.220-224, 2024

[7] AS Tolba, AH El-Baz and AA El-Harby, "Face recognition: A literature review", International Journal of Signal Processing, vol. 2, no. 2, pp. 88-103, Feb 2006.
[8] H. Xu, S. Yao, Q. Li and Z. Ye, "An Improved K-means Clustering Algorithm", 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 2020.
[9] Analysis of Crime Data Visualization and Clustering: PCA + K-Means vs. Feature Extraction by Vibhu Dixit; Padmashree T
[10] J. Chen, Y. Zhang, and W. Wang, “Deep Learning Based Crime Scene Image Analysis,” 2019 IEEE International Conference on Image Processing (ICIP), pp. 1576-1580, 2019.
[11] M. Gupta and A. K. Singh, “Crime Data Clustering and Visualization Using K-Means Algorithm,” International Journal of Computer Applications, vol. 182, no. 33, pp. 30-37, 2018.
[12] P. Verma and R. K. Singh, “An Efficient Crime Detection Model Using K-Means Clustering and Support Vector Machine,” Procedia Computer Science, vol. 132, pp. 192-200, 2018.
[13] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, IETF, August 2018.
[14] M. Nabeel, H. Al-Sakib Khan Pathan, and M. Guizani, “The Many Faces of End-to-End Encryption and Their Security Analysis,” IEEE International Conference on Edge Computing (EDGE), pp. 82-89, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)