International Journal of Engineering Research & Science (IJOER) ISSN: [2395-6992] [Vol-12, Issue-3, March 2026]

CrimeNet Intelligence Tool

Krish Mahalunge[1*]; Shreekant Belvalkar[2]; Yash Wade[3]; Prof. Saniket Kudoo[4]

[1-3]Department of Computer Engineering, VIVA Institute of Technology, India
[4]Assistant Professor, Department of Computer Engineering, VIVA Institute of Technology, India
Mathematics Teacher, Kota
*Corresponding Author

Abstract— *CrimeNet Intelligence Tool is an AI-assisted data visualization and analysis platform designed to convert raw telecommunication records (CDR/IPDR) into intuitive graphical insights tailored for law enforcement and investigative agencies. It ingests multiple input formats — such as CSV, XLSX, and TXT — and processes them via a pipeline combining data parsing, relationship extraction, geospatial clustering, and graph network construction. The system maps communication flows, device associations, and call/SMS/IP channels into visually interpretable networks, overlaying spatiotemporal heatmaps and interactive dashboards. Users can filter by time, location, and identity attributes; probe nodes and edges with metadata; annotate relationships; and generate PDF reports summarizing insights. Unlike static charting tools, CrimeNet's architecture ensures that visualizations are semi-automated, responsive, and production-ready, facilitating rapid exploratory analysis, pattern detection, and investigative intelligence workflows. By automating much of the heavy lifting in transforming raw records to relational visuals, CrimeNet accelerates the analysis cycle, lowers the barrier for non-technical users in intelligence and policing domains, and supports scalable deployment in both academic and operational settings.*

Keywords— CrimeNet Intelligence Tool, CDR Analysis, IPDR Analysis, Cybercrime Investigation, Digital Forensics, Graph Analytics, Relationship Mapping, Interactive Data Visualization, Law Enforcement.

I. INTRODUCTION

The CrimeNet Intelligence Tool project is designed to transform raw telecommunication datasets such as Call Detail Records (CDR) and Internet Protocol Detail Records (IPDR) into meaningful, interactive visual insights, enabling faster and more accurate investigative analysis. It offers applications in cybercrime investigation, law enforcement intelligence, forensic auditing, and academic research where large volumes of communication data need to be quickly processed, interpreted, and visualized.

Leveraging data parsing, relationship mapping, and advanced visualization techniques, CrimeNet extracts call logs, IP connections, device IDs, and location metadata, and then organizes them into structured graphs and heatmaps that highlight associations between individuals, networks, and geospatial patterns. These processed insights are delivered through an interactive web platform built with React, Node.js, and modern visualization libraries, providing users with features such as timeline filters, node-link analysis, geolocation clustering, and downloadable reports.

By combining data science, graph analytics, and intuitive dashboards, CrimeNet reduces manual investigation effort, accelerates decision-making, and bridges the gap between raw digital evidence and actionable intelligence.

II. MATERIAL AND METHODS

The CrimeNet Intelligence Tool utilizes a structured, multi-stage pipeline to transform raw CDR/IPDR data into actionable cyber-forensic intelligence. The process begins with data ingestion and validation, followed by telecom-specific parsing, transformation, and analytical modeling. The system outputs interactive network graphs and geographical maps that enable investigators to examine communication relationships and mobility patterns. The modular pipeline ensures extensibility across components, allowing additional features such as anomaly detection, device profiling, or OSINT integration.

The methodology adopted in CrimeNet follows a cyber-forensic analytical pipeline that transforms heterogeneous telecommunication datasets into structured intelligence representations suitable for investigative reasoning. The pipeline consists of five integrated stages: (i) data acquisition, (ii) preprocessing and normalization, (iii) forensic feature extraction,

(iv) analytical modeling, and (v) visualization and reporting. Each stage introduces abstractions that progressively convert raw CDR/IPDR logs into interpretable communication networks and mobility traces.

2.1 Proposed Detailed Architecture

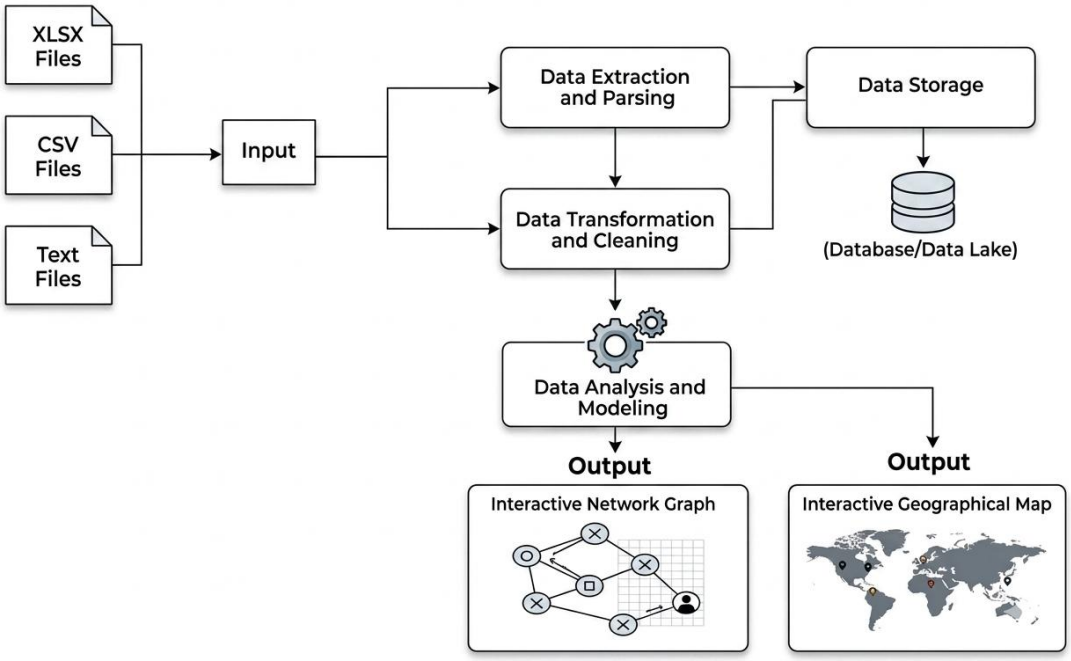

FIGURE 1: Block Diagram / Working of CrimeNet Intelligence Tool

CrimeNet is a comprehensive forensic analytics platform designed to process, standardize, and analyze large-scale telecom datasets such as Call Detail Records (CDR) and Internet Protocol Detail Records (IPDR), which play a crucial role in modern digital investigations.

Stage 1: Data Ingestion — The system supports multiple input formats including CSV, XLSX, and plain text files, ensuring compatibility with datasets provided by different telecom operators. During the ingestion phase, CrimeNet extracts essential attributes such as subscriber identifiers (MSISDN), device identifiers (IMEI), temporal details (start time, end time, duration), spatial information (Cell ID, LAC), and protocol-specific attributes like source and destination IP addresses and ports. It also performs encoding validation and schema inference to identify inconsistencies or missing values.

Stage 2: Preprocessing and Normalization — Following ingestion, the system performs preprocessing and normalization to bring uniformity across heterogeneous datasets. This includes converting all timestamps into a standardized format (YYYY-MM-DD) to enable accurate chronological analysis, removing duplicate records, and handling null or incomplete entries based on their forensic importance. Schema normalization maps diverse field names into a unified canonical structure, ensuring consistency in downstream analysis. Entity resolution techniques are applied to associate multiple MSISDNs with a single IMEI, effectively identifying device-level identities and uncovering patterns such as SIM swapping or shared device usage.

Stage 3: Forensic Feature Extraction — Once the data is cleaned and structured, CrimeNet performs forensic feature extraction to convert raw logs into meaningful analytical representations:

- **Entity-level features:** Communication frequency, call duration, device usage trends, mobility range
- **Relational features:** Number of connections, strength of relationships (edge weights), communication patterns
- **Spatiotemporal features:** Movement trajectories, activity hotspots
- **Endpoint features (for IPDR):** IP source/destination, ports, protocols

Stage 4: Analytical Modeling — CrimeNet applies analytical modeling techniques to derive actionable intelligence. Communication data is represented as a network where nodes correspond to subscribers or devices and edges represent interactions. Edge weights are calculated using a combination of communication frequency and duration, allowing the system to quantify relationship strength. Centrality measures such as degree and betweenness help identify key individuals within the network, including potential coordinators or high-risk suspects.

Stage 5: Visualization and Reporting — The system outputs interactive network graphs and geographical maps that enable investigators to examine communication relationships and mobility patterns. Users can filter by time, location, and identity attributes; probe nodes and edges with metadata; annotate relationships; and generate PDF reports summarizing insights.

III. RESULTS AND DISCUSSION

The following results demonstrate the outputs of the implemented CrimeNet Intelligence Tool, showing the system's ability to process telecom datasets and generate analytical visualizations. The results include network graphs, geographical maps, communication analysis dashboards, and the user interface.

3.1 Main Dashboard

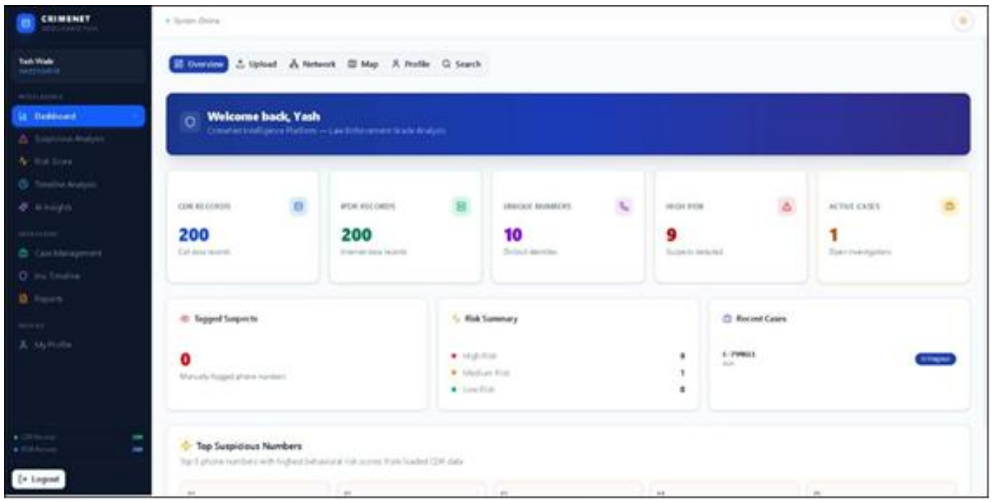

FIGURE 2: CrimeNet Intelligence Interface

The main dashboard of the CrimeNet Intelligence Tool displays summarized investigation data such as CDR records, IPDR records, unique numbers, risk levels, and active cases. It provides investigators with a quick overview of telecom data analysis and suspicious activity insights through an interactive user interface.

3.2 Network Graph Visualization

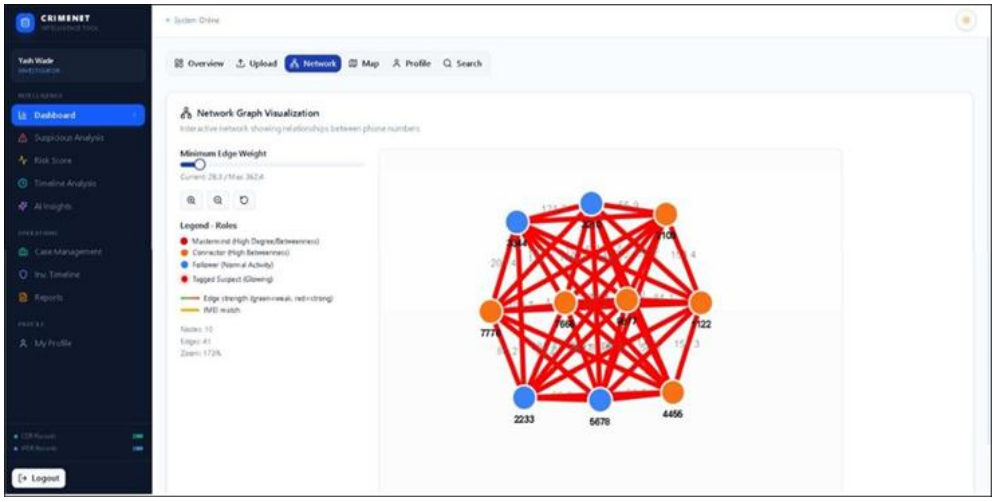

FIGURE 3: Network Graph Visualization of Communication Relationships

The network graph visualization module shows phone numbers represented as nodes and communication links as edges. This visualization helps investigators identify relationships, key connectors, and potential suspects within the communication network.

3.3 Suspicious Pattern Detection

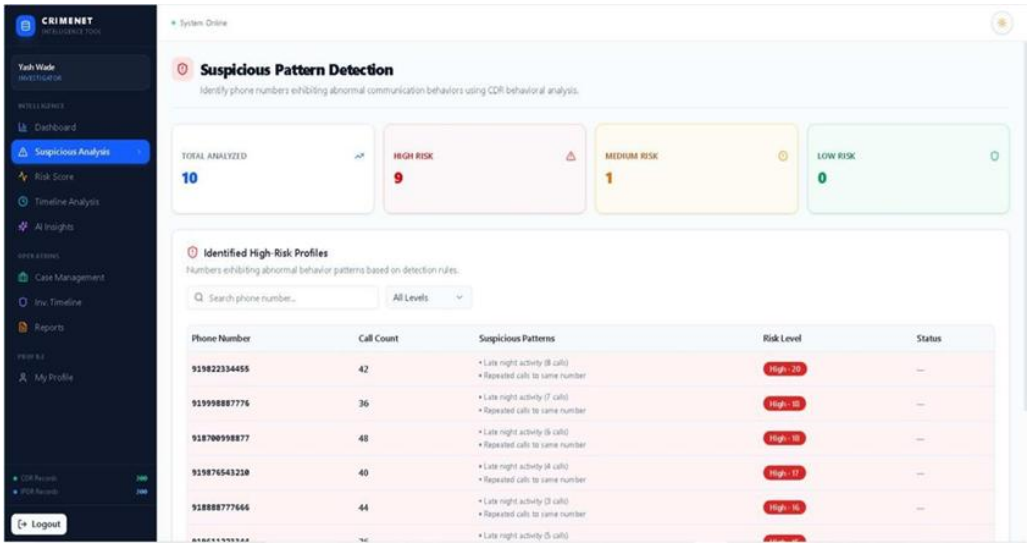

FIGURE 4: Suspicious Pattern Detection and Risk Analysis

The suspicious pattern detection module analyzes communication behavior to identify high-risk phone numbers. It highlights abnormal patterns such as repeated calls and late-night activity, helping investigators detect potentially suspicious profiles.

3.4 Timeline Communication Analysis

FIGURE 5: Timeline Communication Analysis

The timeline communication analysis module visualizes call activities over time using an interactive timeline graph. It helps investigators identify communication spikes, call patterns, and long-duration calls that may indicate suspicious behavior.

3.5 Discussion

The experimental results confirm that the CrimeNet platform accelerates investigative workflows by reducing analysis time and increasing clarity in identifying suspicious entities and behavioral patterns. Key observations include:

Feature	Investigative Value
Network Graph Visualization	Identifies key connectors and hidden relationships
Suspicious Pattern Detection	Flags abnormal communication behavior (late-night calls, high frequency)
Timeline Analysis	Reveals temporal patterns and communication spikes
Geospatial Mapping	Tracks mobility patterns and location-based associations

IV. CONCLUSION

The CrimeNet Intelligence Tool demonstrates that visual analytics significantly enhances the cyber-forensic investigation of telecommunication datasets such as CDR and IPDR. The system provides a structured workflow for transforming heterogeneous telecom records into graph-based relational intelligence and geospatial mobility insights.

By integrating parsing, normalization, analytical modeling, and visualization under a unified architecture, CrimeNet reduces the need for manual cross-referencing and improves the interpretability of large communication datasets. The experimental results confirm that the platform accelerates investigative workflows by reducing analysis time and increasing clarity in identifying suspicious entities and behavioral patterns.

Future work will focus on:

- Integration of real-time data streams
- Advanced anomaly detection using machine learning
- OSINT integration for enriched entity profiling
- Mobile application development for field investigators

ACKNOWLEDGMENT

We express sincere gratitude to our guide, **Prof. Saniket Kudoo**, Department of Computer Engineering, for his invaluable guidance and constant support throughout this research. We are also grateful to the teaching and non-teaching staff of the Computer Engineering Department for their continuous support.

CONFLICT OF INTEREST

The authors declare no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Ahmed, M., Pal, S., and Islam, M. T. “Real-Time Visual Analytics for Cybercrime Investigation Using Streaming CDR Data.” IEEE Transactions on Information Forensics and Security, vol. 17, no. 4, 2022.
[2] Kumar , M., Hanuman thappa, M., and Kumar, T. V. S. “ Crime Investigation and Criminal Network Analysis Using Archive Call Detail
[3] Records.” Proceedings of the IEEE International Conference on Advanced Computing (ICoAC), 2017.
[4] Kao, Da-Yu, et al. “Extracting Suspicious IP Addresses from WhatsApp Network Traffic in Cybercrime Investigations.” Proceedings of
[5] the IEEE International Conference on Advanced Communication Technology (ICACT), 2019.
[6] Cai, Z., Cui, J., and Chen, J. “High Performance Computing for Cyber Physical Social Systems Using Evolutionary Multi-Objective Optimization Algorithm.” IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 8, 2020.
[7] Yu Q., et al. “Clustering Analysis for the Silent Telecom Customers Based K-means++ .” Proceedings of the IEEE 4th International
[8] Conference on Information Technology, Networking, Electronic and Automation Control (ITNEC), 2020.
[9] Jones, B., and Smith, C. “Cybercrime Detection Using the Call Detail Records and the Graph Analytics.” IEEE Symposium on Digital
[10] Forensics and Security, 2016, pp. 87–99.
[11] Jiang, s, Ferreira, J, and González, M. C. “Activity-Based Human Mobility Patterns Inferred from Mobile Phone Data: A Case Study of
[12] Singapore.” IEEE Transactions on Big Data, vol. 3, no. 2, 2016, pp. 208–219.

[13] JR AS et al., "A Deep Learning Approach for Generating Markup Code from Sketch Images", International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2022, Vol. 10, No. IV, pp. 235–238.
[14] Shastry, C., and Thangavel, A. “Telco Big Data Analytics Using Open-Source Data Pipeline: Use Cases and Implementation Results.”
[15] International Journal of Innovative Science and Research Technology, vol. 7, no. 11, 2023, pp. 2128–2136.
[16] Chetry, A, and Sharma, U. “Investigating VoIP Calls: Law Enforcement Perspective” INFOCOMP Journal of Computer Science, vol.
[17] 23, no. 2, 2024.
[18] Mitra, D. “Proliferation of Cyber Crime via Social Media.” International Journal of Novel Research and Development (IJNRD), 2024.
[19] Jyoti, D. “A Study of Influence of Cyber Crime and Prevention Procedures.” Journal of the Emerging Technologies and Innovative
[20] Research (JETIR), vol. 6, no. 1, 2019.
[21] Malathi, A., and Baboo, S. S. “An Enhanced the Algorithm to Predict Future Crime Using Data Mining.” International Journal of
[22] Computer Applications, vol. 21, no. 1, 2011.
[23] Bharati, A., and Chaudhary, A. “Cyber Crime Detection and Prevention Using Data Mining Techniques.” International Journal of
[24] Computer Science and Information Technologies, vol. 6, no. 3, 2015, pp. 2341–2344.
[25] Soni, R., and Kumar, P. “Cybercrime Investigation Using Data Analytics and Visualization Techniques.” International Journal of Computer Applications, vol. 174, no. 15, 2021.