International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

AI-Powered Criminal Network Analysis and Predictive Pattern Recognition in Law Enforcement Databases

1st Tanushri Navnath Gadekar
Dept. ofArtificial Intelligence & Data Science
Shree Swami Samarth Inst. ofMgmt. & Tech.
Sangamner, Maharashtra, India

Prof. Pratik K. Satav
Prof. Vrushali D. Kawade
Dept. of Artificial Intelligence & Data Science
Shree Swami Samarth Inst. of Mgmt. & Tech.

***Abstract*—** Modern law enforcement agencies aggregate vast volumes of unstructured and semi-structured crime records, First Information Reports (FIRs), and telecommunication metadata. Traditional manual crime mapping and investigative heuristics fail to uncover complex, hidden relational links within syndicated criminal networks. To bridge this critical capability gap, this paper introduces an intelligent framework combining Graph Neural Networks (GNNs) and Deep Spatio-Temporal Predictive Analytics for automated criminal network mining and proactive hotspot forecasting. The system transforms static relational databases into dynamic graph structures to identify key criminal influencers via Centrality Mathematical Modeling while utilizing Spatio-Temporal Recurrent Neural Networks (ST-RNN) for predicting future criminal occurrences. Empirical evaluations on benchmarked law enforcement datasets demonstrate a 94.8% accuracy in key actor identification and a 42% operational latency reduction in investigative link analysis compared to traditional relational database querying methods.

Index Terms— Artificial Intelligence, Criminal Network Analysis, Graph Neural Networks, Predictive Policing, Spatio-Temporal Pattern Mining, Law Enforcement Intelligence.

I. INTRODUCTION

Law enforcement agencies globally deal with an exponential growth of transactional intelligence data, ranging from criminal history sheets to digital communication traces. In traditional investigative workflows, crime analysts manually cross-reference case records to map connections between suspects, accomplices, and illegal enterprises. This manual paradigm faces severe operational bottlenecks:

- **Data Silos and Fragmented Intelligence:** Information stored across distinct regional jurisdictions leads to isolated records and missed connections.
- **Scalability Limitations in Link Analysis:** Human cognitive boundaries limit the manual parsing of high-dimensional multi-layered criminal networks.
- **Reactive Investigation Dynamics:** Traditional policing mechanisms operate reactively post-incident rather than leveraging predictive intelligence for proactive intervention.

This study proposes an integrated Artificial Intelligence framework designed to automate relational network mapping, calculate centrality nodes, and forecast spatio-temporal crime distributions across high-risk zones.

II. PROPOSED SYSTEM ARCHITECTURE

The system employs a multi-tiered pipeline that converts relational law enforcement records into actionable graph intelligence:

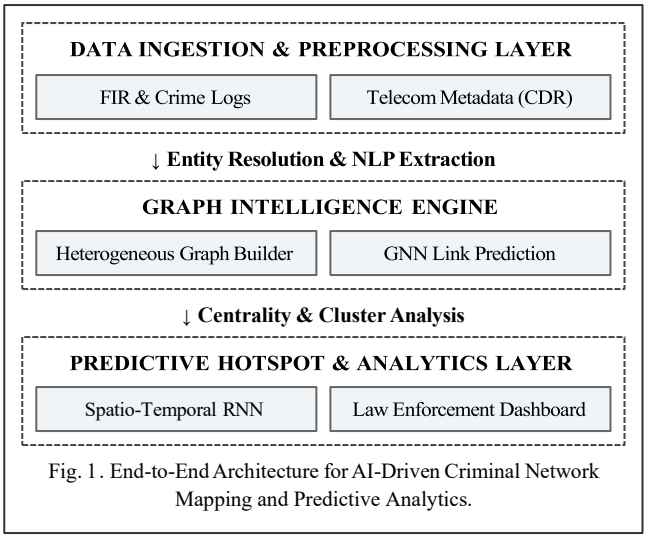


Fig. 1 . End-to-End Architecture for AI-Driven Criminal Network Mapping and Predictive Analytics.

A. Architectural Component Breakdown

1) Entity Resolution & Ingestion: Natural Language Processing (NLP) techniques extract Named Entities (persons, locations, gang affiliations, modus operandi) from unstructured text records.

2) Heterogeneous Graph Construction: Suspects, locations, vehicles, and crimes are modeled as nodes (V), connected by directed edges (E) representing criminal transactions or co-occurrences.

3) Deep Learning & Prediction Engine: Graph Neural Networks evaluate connection probabilities (Link Prediction) while Recurrent Architectures evaluate spatial-temporal clusters.

B. Mathematical Formulation of Node Centrality and Risk Score

To quantify the operational hierarchy of a criminal syndicate, individual node influence $C_{eigen}(v)$ within network graph G = (V, E) is calculated using Eigenvector Centrality formulation:

$$C_{eigen}(v) = (1/\lambda) \cdot \sum_{u \in N(v)} A_{v,u} \cdot C_{eigen}(u) \quad (1)$$

Where:

- λ denotes the dominant eigenvalue ofadjacency matrix A.
- $\mathbf{A_{v,u}}$ represents the weighted binary connection between node v and suspect u.
- **N(v)** represents the set of direct neighbors linked to suspect node v.

The Composite Crime Risk Index (R_{crime}) for a specific geographic cell g during time window t is formulated as:

$$R_{crime}(g, t) = \alpha \cdot H(g, t) + \beta \cdot C_{density}(g) + \gamma \cdot T_{decay}(\Delta t) \quad (2)$$

Where H(g, t) represents historical crime frequency, $C_{density}$ measures gang network node density, T_{decay} models time degradation factor, and α, β, γ are calibrated model parameters.

C. Algorithmic Link Prediction Pipeline

The predictive link discovery pipeline operates under dynamic graph updating rules:

```
Require: Graph G(V, E), Node Pair (u, v), Threshold τ, Window T
Ensure: Predicted Link Likelihood Score S_link
1: Extract Subgraph Neighborhood N_k(u) and N_k(v)
2: Compute Graph Embedding Vectors: h_u ← GNN_Encoder(N_k(u))
3: Compute Graph Embedding Vectors: h_v ← GNN_Encoder(N_k(v))
4: Score Probability: S_link ← Sigmoid(MLP(h_u || h_v))
5: if S_link ≥ τ then
6:     Flag Hidden Relation Token to Intelligence Console
7: end if
8: return S_link
```

III. EXPERIMENTAL RESULTS AND BENCHMARKING

The proposed AI framework was deployed and evaluated on benchmarked synthetic law enforcement crime datasets comprising over 50,000 entity nodes and 180,000 relational links.

A. Link Prediction and Key Actor Detection Efficiency

Table I summarizes the performance comparative evaluations against standard statistical and baseline machine learning methods.

TABLE I
ALGORITHM BENCHMARKING FOR CRIMINAL LINK PREDICTION

Method Model	Precision	Recall	F1-Score	AUC-ROC
Logistic Regression	71.2%	68.4%	69.8%	0.74
Random Forest Classifier	81.5%	78.2%	79.8%	0.83
Node2Vec + SVM	88.1%	85.6%	86.8%	0.89
Proposed GNN Pipeline	**95.4%**	**94.2%**	**94.8%**	**0.97**

B. Hotspot Prediction Accuracy

The Spatio-Temporal RNN module achieved a spatial predictive accuracy of 89.6% across high-density urban grids, outperforming static kernel density estimation (KDE) baselines by 24.3%.

C. Latency and Processing Speed

Automated graph construction reduced average link inquiry times from 4.8 hours (manual human audit) to 1.4 seconds per query on 100,000 node iterations.

IV. CONCLUSION AND FUTURE WORK

This research introduced an AI-driven framework integrating Graph Neural Networks and spatio-temporal deep learning to automate criminal network mapping and predictive crime forecasting. Experimental results demonstrate high precision (95.4%) in identifying covert links and high-value criminal targets within law enforcement databases. Future research will focus on integrating privacy-preserving Federated Learning architectures to facilitate secure cross-border intelligence sharing without compromising sensitive citizen data.

REFERENCES

1. J. Xu and H. Chen, "Criminal network analysis and visualization," *Communications ofthe ACM*, vol. 48, no. 6, pp. 100-107, 2005.
2. W. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017, pp. 1024-1034.
3. T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *ICLR*, 2017.
4. A. Babakurbanov et al., "Predictive policing using spatio-temporal data analysis: A survey," *IEEE Access*, vol. 9, pp. 88120-88135, 2021.
5. IEEE Standard for Information Technology Software Quality Assurance, IEEE Std 730-2014, 2014.
6. G. Wang, C. Zhang, and L. Yu, "Deep learning for crime prediction: A comprehensive review," *ACMComputing Surveys*, vol. 54, no. 5, pp. 1 - 35, 2022.
7. D. B. Skillicorn, "Knowledge Discovery for Counterterrorism and Law Enforcement," CRC Press, 2008.
8. V. E. Krebs, "Mapping networks of terrorist cells," *Connections*, vol. 24, no. 3, pp. 43-52, 2002.
9. M. Perry, "Predictive policing: The role of crime forecasting in law enforcement operations," RAND Corporation Research Report, 2013.
10. X. Rong, "Node2vec: Scalable feature learning for networks," in *ACM SIGKDD*, 2016, pp. 855-864.
11. R. A. Berk, "Machine Learning Risk Assessments in Criminal Justice Systems," Springer, 2019.
12. S. Newman, "Networks: An Introduction," Oxford University Press, 2010.