iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80479

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 14 Issue IV Apr 2026- Available at www.ijraset.com

CrimeNet Intelligence Tool

Yash Wade[1], Krish Mahalunge[2], Shreekant Belvalkar[3], Prof. Saniket Kudoo[4]
[1, 2, 3]*Department of Computer Engineering, VIVA Institute of Technology, India*
[4]*Assistant Professor, Department of Computer Engineering, VIVA Institute of Technology*

Abstract: ***This 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, Winterfell'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, Winterfell 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, Winterfell 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, Winterfell reduces manual investigation effort, accelerates decision-making, and bridges the gap between raw digital evidence and actionable intelligence workflows.

II. MATERIAL AND METHODS

For the purpose of this research, a systematic and implementation-oriented methodology was adopted to design and develop the proposed CrimeNet Intelligence Tool, which aims to assist cybercrime investigators in analyzing telecommunication datasets such as Call Detail Records (CDR), Internet Protocol Detail Records (IPDR), CSV logs, XLSX reports, and text-based evidence files. The methodology focuses on integrating data extraction, preprocessing, graph analytics, geospatial intelligence, and interactive visualization to enable efficient investigation of suspicious communication networks and digital crime patterns [1], [2], [8].

The complete system was developed using modern web technologies including React.js for the front-end interface, Node.js for backend processing, JavaScript libraries for graph and map visualization, and database/data lake mechanisms for scalable storage. Analytical modules were incorporated for relationship mapping, location tracing, communication frequency analysis, and pattern detection to support real-time cybercrime investigations [6], [9].

©IJRASET: All Rights are Reserved

A. Proposed detailed Architecture

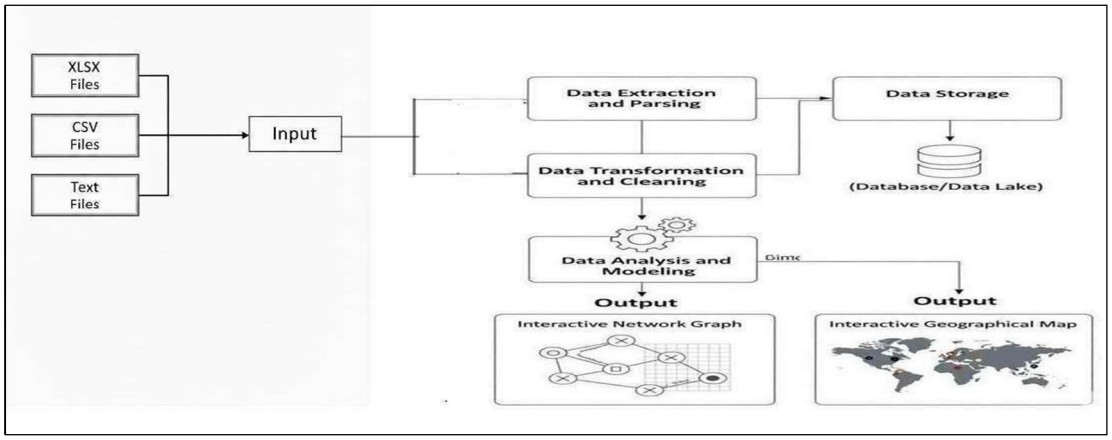


FIGURE 1: Block Diagram / Working of CrimeNet Intelligence Tool

The methodology is divided into multiple sequential stages to ensure systematic collection, transformation, analysis, and visualization of telecom investigation data.

In the first stage, heterogeneous data sources such as XLSX files, CSV files, and Text files are accepted as input into the system. These files may contain call logs, subscriber details, IP session records, tower locations, timestamps, or suspect communication history. The input module validates file formats and prepares them for further processing [2], [8].

In the second stage, data extraction and parsing are performed. Structured and semi-structured records are read from uploaded files and converted into machine-processable formats. Key attributes such as mobile numbers, IMEI, IMSI, timestamps, duration, source-destination pairs, IP addresses, and geographical coordinates are extracted. Parsing methods ensure that inconsistent formats from different telecom providers can be handled efficiently [3], [9].

The third stage involves data transformation and cleaning. Missing values, duplicate records, null entries, invalid timestamps, and corrupted fields are detected and corrected. Data normalization techniques are applied to unify date formats, phone number structures, and location fields. This improves analytical accuracy and reduces noise during investigation [5], [7].

In the fourth stage, cleaned data is transferred to data storage systems such as a relational database or data lake. Centralized storage enables fast retrieval, historical analysis, indexing, and secure management of large telecom datasets generated during cybercrime investigations [1], [4].

The fifth stage focuses on data analysis and modeling, which forms the intelligence core of the proposed system. Graph analytics techniques are used to detect hidden communication networks, identify central suspects, and uncover frequent contact chains. Temporal analysis helps trace activity timelines, while clustering and anomaly detection methods reveal unusual calling or internet usage behavior. Predictive models may also support prioritization of suspicious entities [6], [10].

In the sixth stage, the processed results are visualized through an Interactive Network Graph. This module represents suspects, victims, and linked entities as nodes, while communication records are shown as edges. Investigators can dynamically explore connections, detect hubs, and understand criminal network structures visually [2], [6].

In the final stage, the system generates an Interactive Geographical Map using extracted location or tower data. Communication events are plotted geographically to trace movement patterns, identify operational zones, and correlate multiple suspects across locations. This provides actionable geospatial intelligence for field investigations [7], [8].

Thus, the proposed methodology establishes a complete pipeline that transforms raw telecom records into meaningful investigative intelligence through automated parsing, cleaning, modeling, and interactive visualization. Each stage contributes to reducing manual workload, accelerating cybercrime investigations, and improving evidence-driven decision making [1], [12].

III. RESULT 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 outputs such as network graphs, geographical maps, and communication analysis dashboards along with the user interface.

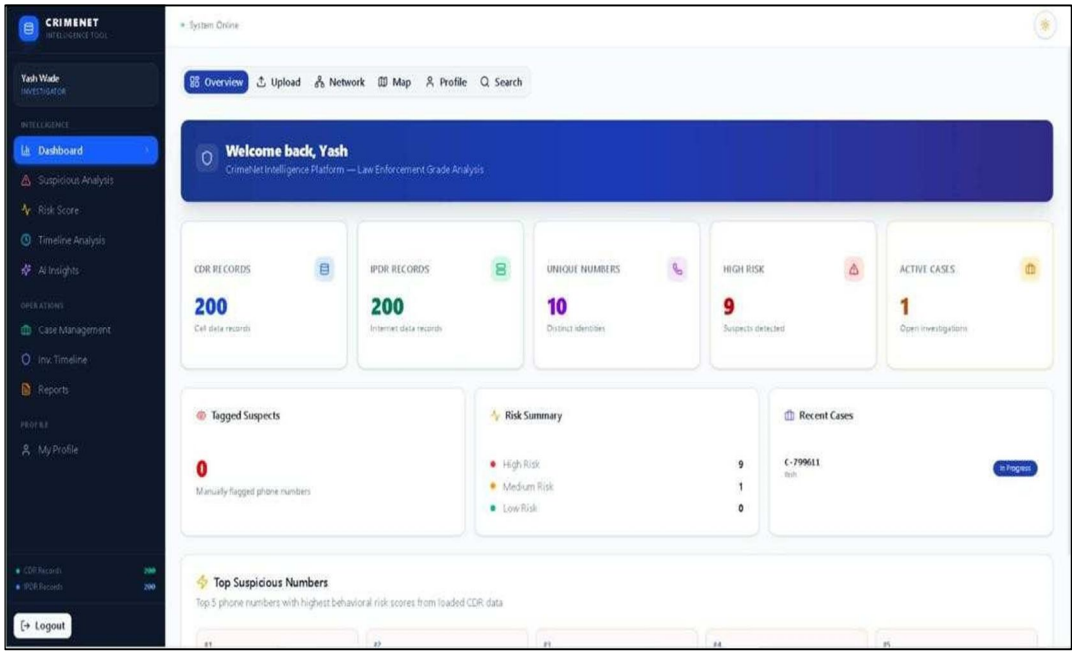


FIGURE 2: CrimeNet Intelligence Interface

The main dashboard of the CrimeNet Intelligence Tool, displaying 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.

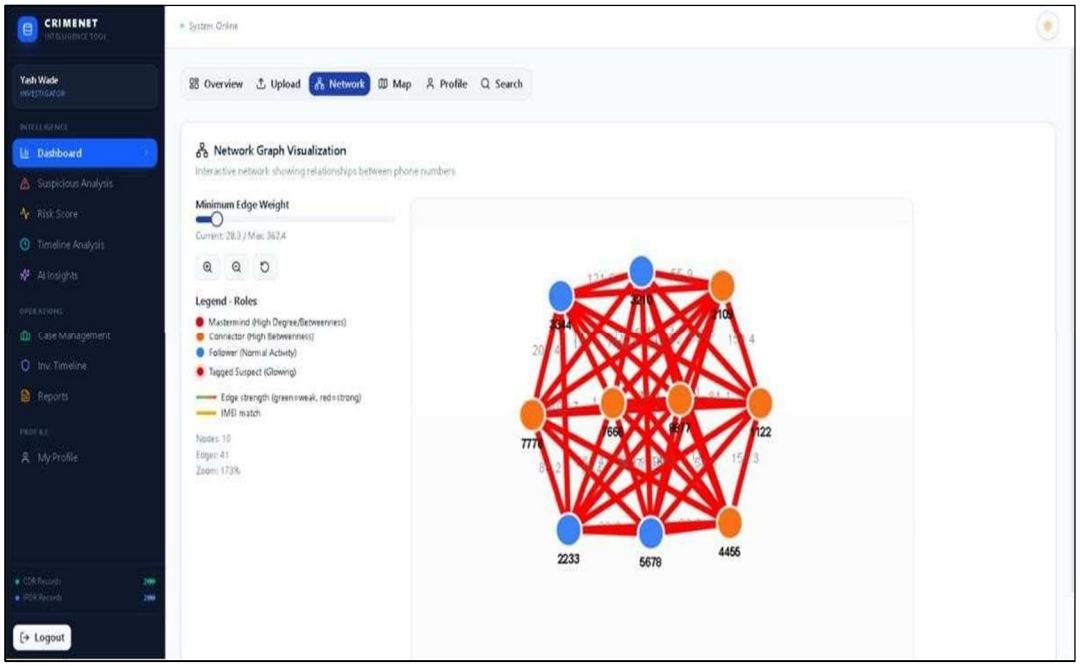


FIGURE 3: Network Graph Visualization of communication Relationship

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

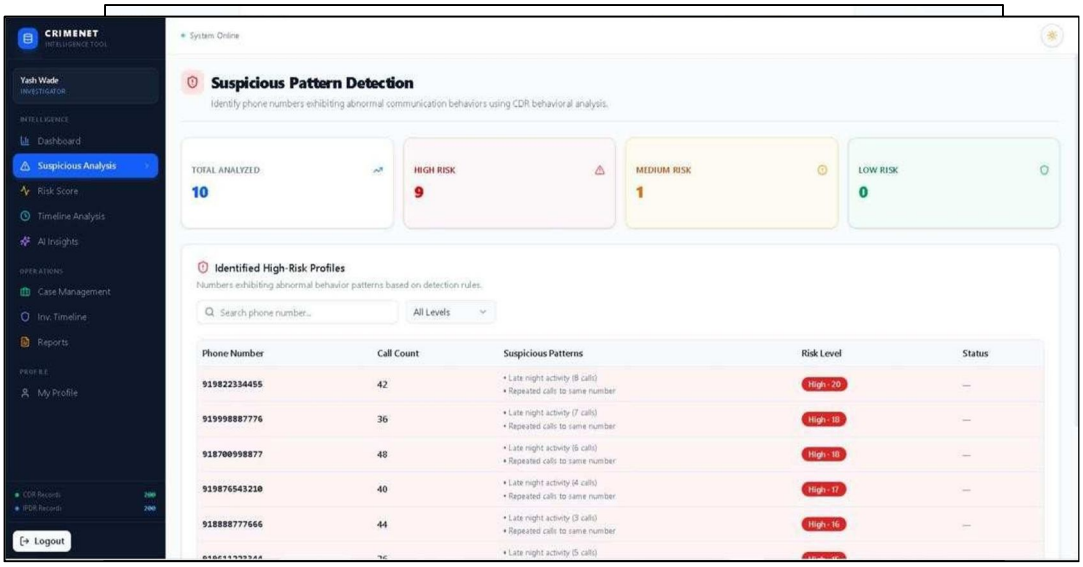


FIGURE 4: Suspicious Pattern Detection and Risk Analysis

Further, the suspicious pattern detection module, where the system 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.

FIGURE 5: Timeline Communication Analysis

The timeline communication analysis module, which 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

IV. CONCLUSION

This 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.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Ahmed, M., Pal, S., & Islam, M. T. (2022). Real-Time Visual Analytics for Cybercrime Investigation Using Streaming CDR Data. IEEE Transactions on Information Forensics and Security, 17(4).

[2] Kumar, M., Hanumanthappa, M., & Kumar, T. V. S. (2017). Crime Investigation and Criminal NetworkAnalysis Using Archive Call Detail Records. Proceedings of the IEEE International Conference on Advanced Computing (ICoAC).

[3] Kao, D.-Y., et al. (2019). Extracting Suspicious IP Addresses from WhatsApp Network Traffic in Cybercrime Investigations. Proceedings of the IEEE International Conference on Advanced Communication Technology (ICACT).

[4] Cai, Z., Cui, J., & Chen, J. (2020). High Performance Computing for Cyber Physical Social Systems Using Evolutionary Multi-Objective Optimization Algorithm. IEEE Transactions on Emerging Topics in Computing, 8(8).

[5] Yu, Q., et al. (2020). Clustering Analysis for Silent Telecom Customers Based on K-means++. Proceedings of the IEEE 4th International Conference on Information Technology, Networking, Electronic and Automation Control (ITNEC).

[6] Jones, B., & Smith, C. (2016). Cybercrime Detection Using Call Detail Records and Graph Analytics. IEEE Symposium on Digital Forensics and Security, pp. 87–99.

[7] Jiang, S., Ferreira, J., & González, M. C. (2016). Activity-Based Human Mobility Patterns Inferred fromMobile Phone Data: A Case Study of Singapore. IEEE Transactions on Big Data, 3(2), 208–219.

[8] Kapri, P., Thanvi, N., Patane, S., & Thakur, R. (2022). CDR/IPDR Analyser and Visualizer: Enhancing Investigative Capabilities Through Communication Data Analysis. ShodhKosh: Journal of Visual and Performing Arts, 3(1), 1149–1154.

[9] Shastry, C., & Thangavel, A. (2023). Telco Big Data Analytics Using Open-Source Data Pipeline: Use Cases and Implementation Results. International Journal of Innovative Science and Research Technology, 7(11), 2128–2136.

[10] Chetry, A., & Sharma, U. (2024). Investigating VoIP Calls: Law Enforcement Perspective. INFOCOMP Journal of Computer Science, 23(2).

[11] Mitra, D. (2024). Proliferation of Cyber Crime via Social Media. International Journal of Novel Research and Development (IJNRD).

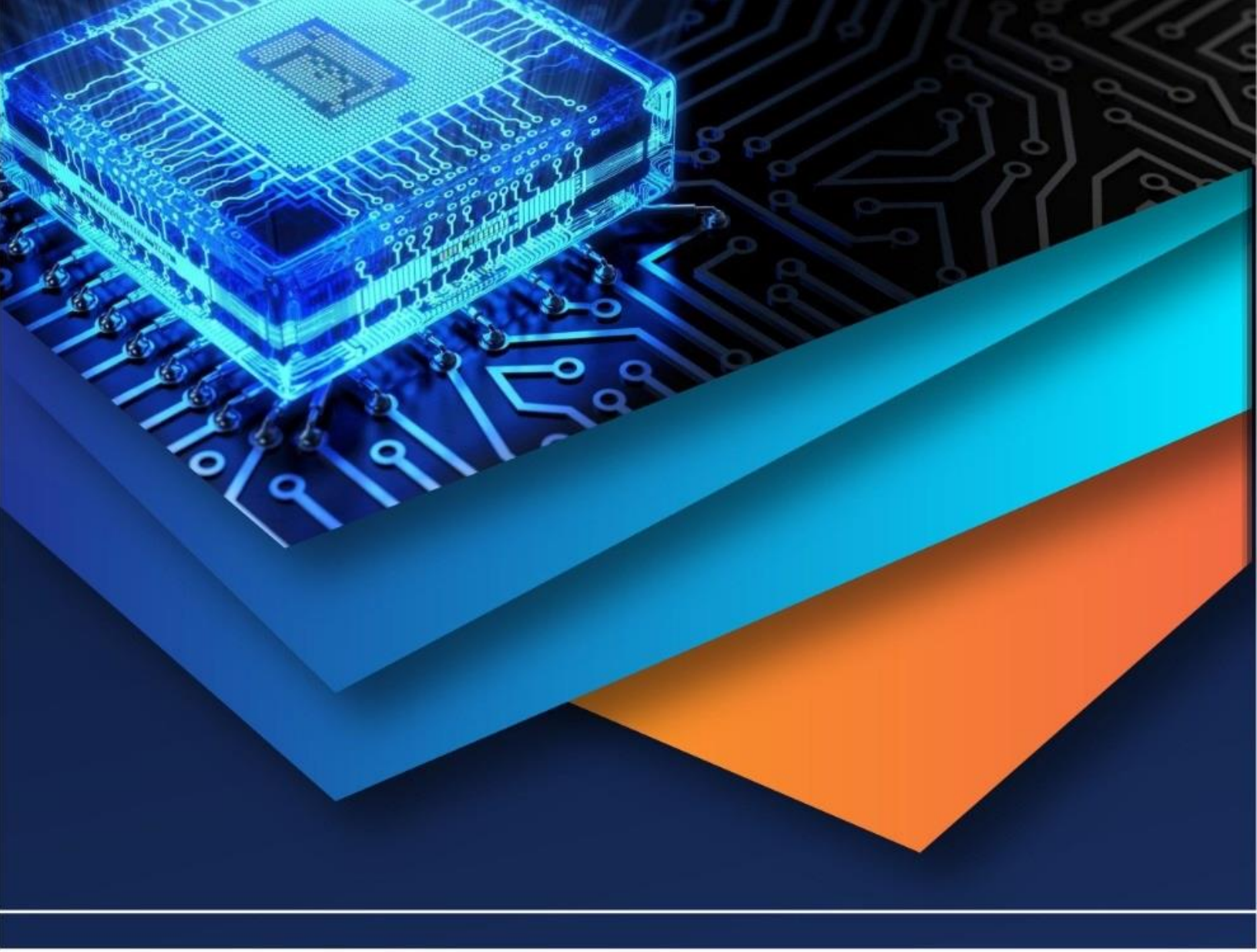
[12] Huamanñahui Chipa, I., Gamboa-Cruzado, J., & Ramirez Villacorta, J. (2022). Mobile Applications for Cybercrime Prevention: A Comprehensive Systematic Review. International Journal of Advanced Computer Science and Applications (IJACSA), 13(10).

[13] Jyoti, D. (2019). A Study of Influence of Cyber Crime and Prevention Procedures. Journal of Emerging Technologies and Innovative Research (JETIR), 6(1).

[14] Nayagam, G. K., & Prakash, A. (2024). An Analytical Study in the Prevention of Cybercrime in India. TIJER – International Research Journal, 11(6).

[15] Sangwan, S. (2022). A Review on Cyber Crime Prevention Using Steganography. International Journal for Research Publication & Seminar, 13(1).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



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)