WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Crime Analysis Mapping with Intrusion Detection System

***T. Tamilarasi [1], Sangeetha Varadhan[2]***

[1] PG Department of Computer Applications, DR. M.G.R. Educational & Research Institute, Chennai-95, India tamilarasibca18@gmail.com

[2]Assistant Professor, Department of Computer Applications, DR. M.G.R. Educational & Research Institute, Chennai-95, India sangeetha.mca@drmgrdu.ac.in

**ABSTRACT**

This study explores the integration of crime analysis mapping with an intrusion detection system (IDS) to enhance security measures and understand crime patterns. By visualizing crime data on maps and monitoring network traffic for malicious activities, this integrated approach offers a comprehensive view of security threats and vulnerabilities. The study demonstrates how correlation analysis, resource allocation, incident response, and predictive analysis can be leveraged to proactively identify and address security threats, optimize resource utilization, and foster collaboration between law enforcement agencies and security teams.

**Keywords:** Crime Analysis Mapping, Intrusion Detection System (IDS), Geospatial Analysis, Anomaly Detection, Correlation Analysis, Resource Allocation, Incident Response, Predictive Analysis.

## I. INTRODUCTION

The article also explored the contribution of dark web measurement by analyzing data from it, including cyber threats and incidents and identified technologies related to the dark web. In addition to a system consisting of a crawler, analyzer and proposed. a classifier to find sites where security nano analysts can gather information, and a game theoretic framework that simulates the attacker and defender CTI mining process and analysis as a security game, which includes previous attacks and security experts [1]

In addition, classify existing types of threat intelligence into strategic threat intelligence, operational intelligence, and tactical threat intelligence. Because focusing mainly on TTI (Tactical Threat Intelligence),which was mainly created by Indicators of Compromise(IOC), the work provided a comprehensive overview of TTI issues, emerging research directions and standards. With the development of artificial intelligence (AI), Ibrahim et al. provided a brief discussion of the application of AI and machine learning approaches to reinforcement [2]

Natural language processing for automatic extraction from text descriptions.Since usage is one of the most important steps to maximize its effectiveness, the study talked about the latest approach to sharing and the related challenges to automate the sharing process, both technical and non-technical challenges [3]

Summarized the current landscape of available formats and languages for sharing CTI.They also analyzed a sample of Data mining feeds, including the data they contain and the challenges associated with aggregating and sharing that data.Beyond the research works on CTI, the use and implementation of Data Mining is a common practice in government organizations and enterprises, reflecting the growing recognition of the critical importance of cyber security. These two parties have dedicated teams responsible for collecting, analyzing, and disseminating threat intelligence information, often through specialized Data Mining platforms and tools. For example, the Information Sharing and Analysis Center (ISACs) are centralized nonprofit organizations that are established to facilitate the sharing of CTI and other security-related information among their members [4]

They bring together organizations from a particular field or sector to share threat intelligence and best practices and collaborate on incident prevention and mitigation. ISACs are often supported by government agencies and other organizations and generally follow strict security and privacy policies to ensure that sensitive information is protected and shared only with authorized persons.However, according to a 2018 Crowdstrike Threat Intelligence report, CTI is more often seen as valuable with 72 percent planning to spend more the next three months on data mining [5]

## II. LITERATURE SURVEY

According to **Michele Russo**. et al., 2021 llegal cryptocurrency mining has become one of the most common methods of monetizing computer security breaches. In this attack, the computer resources of victims are misused to mine cryptocurrency for the benefit of the attackers. The most popular illegally mined digital currency is Monero because it offers strong anonymity and is efficiently mined by processors. Illegal mining is essentially based on data traffic between compromised systems and remote mining pools using the de facto standard Stratum protocol [6]

According to **Rodrigo Diaz**. et al., 2021 Security information and event management (SIEM) systems have been widely used as an effective tool to prevent, detect and respond to cyber attacks. SIEM solutions have evolved into comprehensive systems that provide comprehensive visibility to identify high-risk areas and proactively focus on mitigation strategies to reduce costs and incident response time. Nowadays, SIEM systems and related solutions are slowly converging towards big data tools. We examine the most commonly used SIEMs for their critical functionality and analyze external factors [7]

According to **Rasheed Ahmad**. et al., 2022 Data analytics projects span all types of domains and applications. Researchers publish results using specific data and classification models. They present the results and a summary of the performance indicators of the classifiers they evaluated. However, readers and reviewers may not compare the results of different publications for several reasons. One reason is the differences in classification models and the specific settings they use; Another reason is the difference in computing resources and environments used to obtain these results [8]

According to **Yonghang Tai**. et al., 2023 Today's cyberattacks have become more difficult and more widespread, and new defenses are needed to defend against them. The dynamic nature of new-generation threats, which are evasive, flexible and sophisticated, challenge traditional heuristic and signature-based security systems. Organizations strive to collect and share real-time cyber threat intelligence and then turn it into threat intelligence to prevent attacks, or at least respond proactively quickly. Mining Cyber Threat Intelligence (CTI) [9]

According to **Zhenhui Han**.et al., 2023 With the development of new technologies such as big data, cloud computing and the Internet of Things, cyber attack technology is constantly evolving and updating, and cyber attack detection technology must undergo a corresponding iterative development. There are three main problems with these technologies: the automatic representation of heterogeneous and complex network traffic data, the inconsistent patterns of network attacks, and the conflict between the accuracy of the anomaly detection model and the constant evolution of attacks [10].

## III. PROPOSED SYSTEM

We propose a comprehensive security system that synergizes crime analysis mapping with an advanced intrusion detection system (IDS). This integrated approach aims to proactively identify, analyze, and respond to security threats and criminal activities more effectively. The crime analysis mapping component will visualize and analyze crime data on geographical maps, enabling law enforcement agencies to identify crime hotspots, trends, and patterns. Meanwhile, the IDS will monitor network traffic and system activities in real-time, detecting malicious behaviors, anomalies, or policy violations. By correlating the insights from crime analysis mapping with the alerts and notifications generated by the IDS, the system will provide a holistic view of security vulnerabilities and incidents. This integrated system will facilitate data-driven decision-making, optimize resource allocation, and enable proactive measures to enhance security, reduce risks, and foster collaboration among law enforcement agencies, security teams, and other stakeholders.

**ARCHITECTURE DIAGRAM**

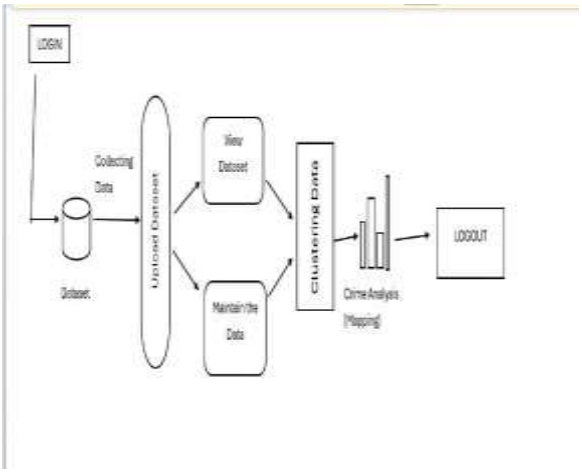


**FIGURE.1 Architecture**

**Data Collection:** Crime data is collected from the crime database, and network traffic system activity logs are collected from IDS sensors network monitors.

**Data Processing and Analysis:** Crime data is processed and analyzed to identify patterns, trends, and hotspots, while network traffic data and system activity logs are processed using anomaly detection and signature-based detection methods.

**Correlation and Integration:** Crime data is correlated with IDS alerts to identify potential patterns or correlations, and integrated with data from various sources and modules for comprehensive analysis.

**Alerts and Notifications:** Alerts and notifications are generated for detected security threats and criminal activities, and interactive dashboards and visualization tools are provided for monitoring and analysis.

**Response and Action:** Coordinated response actions are facilitated based on the analysis and insights generated by the system, and resource allocation is optimized to high-risk areas.

## IV.RESULT AND DISCUSSION


**FIGURE.2 Admin Login**

The admin login functionality serves as the gateway for authorized users to access the system's administrative features.

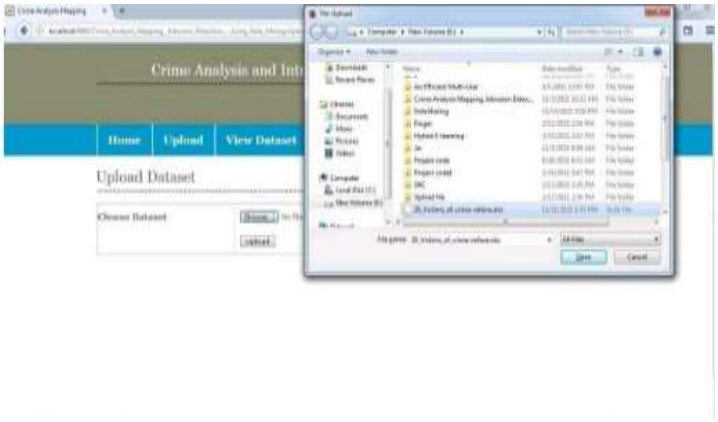


**FIGURE.3 Choose Dataset**

**The "Choose Dataset" feature allows** users to select and upload datasets for analysis. This functionality facilitates the integration of various data sources, such as crime data, demographic data, and sensor logs, to provide comprehensive insights and facilitate data-driven decision-making. Ensuring compatibility with different file formats and providing validation checks can help streamline the dataset selection and upload process, ensuring data integrity and accuracy.


**FIGURE.4 Upload Dataset**

It should support various file formats and sizes while adhering to data privacy and security standards. Implementing data validation, error handling, and encryption techniques can help safeguard sensitive information and ensure the reliability of the uploaded data for subsequent analysis.


**FIGURE.5 View Dataset**

The "View Dataset" feature allows users to visualize and explore the uploaded datasets. This functionality should provide interactive tools and visualizations, such as charts, graphs, and maps, to facilitate data exploration, analysis, and interpretation.


**FIGURE.6 Detector Login**

The detector login functionality provides authorized users, such as security personnel or system administrators, with access to the intrusion detection system (IDS). It ensures secure authentication and authorization to monitor network traffic or system activities for potential security threats and policy violations. I


**FIGURE.7 Clustering Page**

The clustering page allows users to perform cluster analysis on the uploaded datasets to identify similar patterns or groups within the data. This functionality can help uncover hidden relationships, trends, or anomalies in the data, facilitating deeper insights and understanding of complex datasets.

**FIGURE.8 Sholingar Area Analyze Report**

The Sholingar area analyze report provides a detailed analysis of crime data and security incidents within the Sholingar area. It includes key findings, trends, hotspots, and recommendations based on the integrated datasets and analytical tools. This report can help stakeholders, such as law enforcement agencies, local authorities, and community organizations, to understand and address security challenges effectively, allocate resources efficiently, and develop targeted crime prevention strategies tailored to the specific needs and characteristics of the Sholingar area.


**FIGURE.9 Crime Analysis Page**

The crime analysis page offers comprehensive crime analysis tools and features to explore, visualize, and interpret crime data across different locations, time periods, and crime types. It facilitates geospatial analysis, temporal analysis, and crime type analysis to identify patterns, trends, and hotspots, enabling stakeholders to make informed decisions and develop proactive crime prevention and intervention strategies.


**FIGURE.10 Sholingar Area View Graph**

The Sholingar area view graph functionality allows users to visualize crime data, security incidents, or analytical results specific to the Sholingar area through graphs, charts, and other visual representations. It provides a snapshot of key metrics, trends, and patterns, enabling stakeholders to quickly assess the current situation, monitor changes over time, and identify areas that require attention or intervention.

## V. CONCLUSION

The integration of crime analysis mapping with an intrusion detection system presents a promising approach to enhancing security and combating criminal activities effectively. By combining geospatial analysis, temporal analysis, and crime type analysis with anomaly detection, signature-based detection, and real-time monitoring, organizations can proactively identify security threats, optimize resource allocation, and foster collaboration among stakeholders. This data-driven approach enables informed decision-making, efficient resource utilization, and timely response to security incidents, thereby creating a more robust and proactive security framework. Future research and implementation of predictive models based on historical crime data and IDS logs can further enhance the effectiveness of this integrated approach in addressing evolving security challenges and safeguarding communities.

**REFERENCES**

[1].Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai, Jun Zhang 2023, Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives, IEEE Communications Surveys & Tutorials, 2023.

[2].Tao Yi, Xingshu Chen, Yi Zhu, Weijing Ge, Zhenhui Han 2023, Review on the application of deep learning in network attack detection,Journal of Network and Computer Applications 212, 103580, 2023.

[3].Rasheed Ahmad, Izzat Alsmadi, Wasim Alhamdani, Lo'ai Tawalbeh 2022, Towards building data analytics benchmarks for IoT intrusion detection, Cluster Computing 25 (3), 2125-2141, 2022.

[4]M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "What are the attackers doing now Automating data mining threat intelligence extraction from text on pace with the changing threat landscape: A survey," 2021,arXiv:2109.06808.

[5].Michele Russo, Nedim Šrndić, Pavel Laskov 2021, Detection of illicit cryptomining using network metadata,EURASIP Journal on Information Security 2021 (1), 11, 2021

[6].Gustavo González-Granadillo, Susana González-Zarzosa, Rodrigo Diaz 2021, Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures, Sensors 21 (14), 4759, 2021.

[7].A.Ramsdale, S.Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," Electronics, vol. 9, no. 5, p. 824, 2020.

[8] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," Computer Security, vol. 87, Nov. 2019, Art. no. 101589.

[9] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," Comput. Security, vol. 72,pp. 212–233, Jan. 2018.

[10] J. Robertson et al., Darkweb Cyber Threat Intelligence Mining.Cambridge, U.K.Cambridge Univ. Press, 2017.