International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 31 Issue 04 – AUGUST 2025.

Cognitive Threat Forensics for Preventive Cybernetic Shielding

S Senthil Murugan[#1], Ganavi N R[*2]

[#]*Assistant professor, T John Institute of Technology, Bengaluru, Karnataka, India*
[*]*Student, Dept. of MCA, T John Institute of Technology, Bengaluru, Karnataka, India*

***Abstract*— In recent times, security threats targeting the mining sector have become increasingly severe and frequent, necessitating a new generation of defense mechanisms. These evolving threats are often evasive, adaptive, and highly sophisticated, posing significant challenges to traditional security systems that rely on heuristic and signature-based detection methods. To counter these advanced threats, organizations are focusing on the collection and sharing of real-time threat intelligence, which enables proactive prevention and rapid response to cyberattacks . Artificia intelligence (AI) is playing a pivotal role in mining and analyzing valuable insights from cybersecurity data. Despite the growing potential of AI in threat intelligence, many organizations still rely on basic implementations—such as integrating threat data feeds into existing systems like firewalls, intrusion prevention systems, and Security Information and Event Management (SIEM) platforms—without fully leveraging the deeper analytical capabilities AI can offer.To address this gap and enhance cybersecurity resilience, this article presents a comprehensive review of recent research on AI-driven mining of security threats in the mining sector. We propose a detailed taxonomy to categorize existing studies based on their objectives, including analysis of cybersecurity entities and events, threat tactics and techniques, hacker profiling, indicators of compromise, exploitation of vulnerabilities and malware behavior, and proactive threat hunting. Furthermore, we explore the current state-of-the-art technologies, identify key research challenges, and outline potential future directions for advancing AI-based threat intelligence in mining security.**

***Index Terms*— Mining security threats, cybersecurity, artificial intelligence, threat intelligence, real-time threat detection, evasive cyberattacks, security information and event management (SIEM), intrusion prevention systems, hacker profiling, indicators of compromise (IoCs), malware analysis, vulnerability exploitation, threat hunting, AI-driven cybersecurity, taxonomy of threat mining, future research directions.**

I. INTRODUCTION

The increasing frequency and sophistication of cyberattacks in the mining sector demand advanced and intelligent security measures to protect critical digital infrastructure. Traditional cybersecurity systems, which largely depend on signature-based and heuristic detection mechanisms, are becoming inadequate in the face of modern threats that are evasive, adaptive, and complex in nature. These new-generation threats require proactive strategies that not only detect and respond to attacks but also predict and prevent them.

Artificial Intelligence (AI) has emerged as a powerful tool in the cybersecurity landscape, offering capabilities to mine, analyze, and interpret large volumes of threat-related data in real time. This approach known as Mining Security Threats Artificial Intelligence (MST-AI) facilitates the transformation of raw threat data into actionable intelligence. While current practices in many organizations involve the basic integration of threat data with firewalls, intrusion detection systems, and SIEMs, they often overlook the deeper analytical insights that AI can deliver for preemptive security actions.

The existing research and implementations in MST-AI have predominantly focused on data sharing mechanisms and automation of basic threat information processing. However, they lack a comprehensive framework to utilize AI for preventive digital safety and strategic threat mitigation. Furthermore, limitations such as the absence of Tactical Threat Intelligence (TTI) and a lack of deeper profiling of hacker behavior and attack patterns reduce the effectiveness of current systems. To address these gaps, the proposed system introduces a comprehensive six-step methodology that applies MST-AI to enhance proactive cyber defense. It emphasizes the transformation of cybersecurity data into knowledge through perception, comprehension, and projection similar to situational awareness models. The system also proposes taxonomies based on attacker behaviors, indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), and hacker profiles, enabling a more informed and predictive defense posture. By expanding the application of AI in mining security threat analysis and sharing, this work aims to empower organizations to foresee, detect, and neutralize threats more effectively, thereby significantly strengthening the overall digital security landscape.

II. LITERATURE SURVEY

C. Fachkha and M. Debbabi present a comprehensive

survey positioning the darknet as a valuable source of cyber intelligence, proposing a taxonomy that distinguishes services, infrastructures, and behaviors observable across hidden networks, and characterizing how botnets, malware distribution, command-and-control traffic, and illicit marketplaces manifest in darknet data; their work highlights collection/measurement methodologies (e.g., honeypots, darknet telescopes), analytical challenges such as attribution and noise filtering, and practical use cases for threat detection and situational awareness, while underscoring ethical and legal considerations in leveraging covert ecosystems for intelligence.

W. Tounsi and H. Rais survey technical threat intelligence (TTI) amid increasingly sophisticated cyberattacks, mapping the lifecycle from collection and normalization of indicators of compromise to analysis, scoring, sharing, and operationalization within security controls; they compare data formats and standards (e.g., STIX/TAXII), assess automation/orchestration benefits and limits, and identify challenges including data quality, context scarcity, timeliness, adversary deception, and integration gaps, ultimately arguing for richer contextualization, trust models, and metrics to measure the defensive value of TTI.

T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah review cyber threat intelligence sharing practices and platforms, analyzing socio-technical barriers such as trust, liability, competitive concerns, and privacy, alongside technical hurdles like interoperability, standard mismatches, and indicator fidelity; they categorize sharing communities (governmental, sectoral ISACs, open-source, and commercial feeds), evaluate sharing models and incentives, and outline research directions including privacy-preserving sharing, quality assessment frameworks, automated relevance scoring, and mechanisms to counter free-riding while improving actionable uptake in SOC workflows.

M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof examine key issues and challenges in cyber threat intelligence, emphasizing the fragmentation of sources, inconsistency of schemas, and the difficulty of transforming raw indicators into actionable, context-rich insights; they discuss limitations in validation and timeliness, the scarcity of skilled analysts, integration friction with existing SIEM/SOAR stacks, and adversarial manipulation of feeds, recommending standardized evaluation metrics, enhanced automation with human-in-the-loop analysis, and governance frameworks to improve trust, sharing efficacy, and operational impact.

III. Existing System

Mining Security threats Artificial intelligence sharing has become a novel weapon in the arsenal of cyber defenders to proactively mitigate increasing Mining Security threats. Automating the process of Mining Security threats Artificial intelligence sharing, and even the basic consumption, has raised new challenges for researchers and practitioners.
This extensive literature survey explores the current state-of-the-art and approaches different problem areas of interest pertaining to the larger field of sharing Mining Security threats Artificial intelligence. The motivation for this research stems from the recent emergence of sharing Mining Security threats Artificial intelligence and the involved challenges of automating its processes.
This work comprises a considerable amount of articles from academic and gray literature, and focuses on technical and non-technical challenges. Moreover, the findings reveal which topics were widely discussed, and hence considered relevant by the authors and Mining Security threats Artificial intelligence sharing communities.
Disadvantage of existing system
In the existing work, the system did not implement Mining Security threats Artificial intelligence for Preventive Digital safety Security.
This system is less performance due to lack of Tactical Threat Intelligence (TTI).

IV. Proposed System

Our review summarizes a six-step methodology that transforms Cyber security-related information into evidence based knowledge through perception, comprehension, and projection for proactive cyber security defense using Mining Security threats Artificial intelligence. We collect and review the state-of-the-art solutions and provide an in-depth analysis of collected work with the proposed taxonomies based on Mining Security threats Artificial intelligence consumption, particularly seeing through the eyes of attackers for proactively defending against cyber threats.As part of our efforts to expand the perspectives of other researchers and Mining Security threats Artificial intelligence communities, we discuss challenges and open research issues as well as identify new trends and future directions.

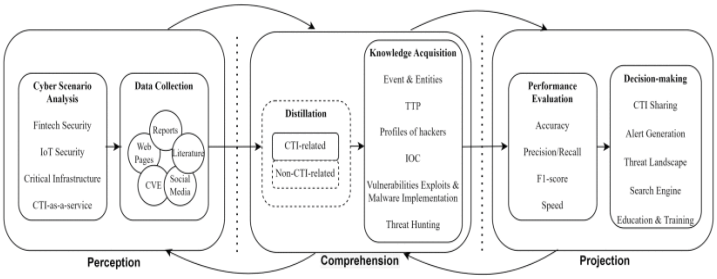

Fig: Architecture Digram

Advantages

Cybersecurity related entities and events: The identification of cybersecurity-related entities and events in Mining Security threats Artificial intelligence is like a diagnosis step that identifies the nature of a particular illness or disease.Mining Security threats tactics, techniques, and procedures: In this task category, the goal is to determine how Mining Security threats actors and hackers prepare and execute Mining Security threats by analyzing their Tactics, Techniques, and Procedures (TTPs). The profiles of hackers: The third category in our taxonomy of Mining Security

threats Artificial intelligence is called profiles of hackers which trace the origin of Mining Security threats.Indicators of compromise: The extraction of IoCs aims to find pieces of forensic data that provide evidence of potentially malicious activity on an organization's system, for example, the names, signatures, and hashes of malware.

V. IMPLEMENTATION

Remote Users: Remote users interact with the digital safety security system to benefit from its protective capabilities. They are the individuals or entities whose digital safety is being monitored and secured. Remote users may indirectly interact with the system through its automated threat detection and prevention mechanisms. They might receive alerts or notifications about potential security risks or vulnerabilities affecting their digital environment. The system uses data related to their digital activity to identify and mitigate threats, ensuring a safer online experience.

Service Provider: The service provider manages the core functionality of the AI-driven digital safety security system, ensuring its threat detection capabilities are accurate and effective through the use of machine learning algorithms. They leverage Artificial Neural Networks (ANNs) to model complex relationships in security data, identifying subtle patterns indicative of emerging threats and continuously learning to improve threat recognition. Support Vector Machines (SVMs) are employed for robust classification, distinguishing between malicious and benign activities to build accurate threat detection models. Gradient Boost Classifiers are utilized to create highly accurate, ensemble-based models that combine multiple weak learners, effectively handling complex datasets and enhancing overall threat detection accuracy. The service provider uploads and processes training data, monitors algorithm performance, and manages user access to maintain the system's reliability in predicting and preventing digital safety threats.

VI. RESULT

The performance evaluation of the threat detection algorithms reveals the following accuracy rates: Artificial Neural Networks (ANN) achieved an accuracy of 50.92%, demonstrating its ability to model complex relationships within the security data. Support Vector Machines (SVM) attained an accuracy of 48.17%, indicating its effectiveness in classifying malicious and benign activities. The Gradient Boost Classifier reached an accuracy of 49.54%, showcasing its capability to combine multiple weak learners for robust threat prediction. These results, visually represented in a pie chart, provide a clear comparison of each algorithm's performance in accurately identifying and classifying digital safety threats, highlighting the strengths and limitations of each approach.

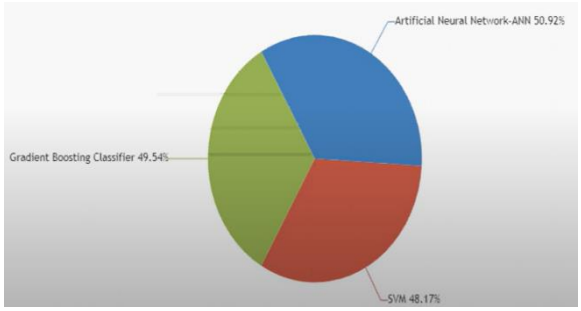

Fig: Resultant graph

VII. CONCLUSION

In response to the increasing severity and frequency of cyberattacks in the mining sector, this research proposes a novel approach leveraging Mining Security Threats Artificial Intelligence (MST-AI) for proactive digital safety and security. Addressing the limitations of traditional signature-based systems and the basic integration of threat data in existing practices, the proposed system introduces a six-step methodology to transform cybersecurity data into actionable knowledge, enabling organizations to foresee, detect, and neutralize threats more effectively. By focusing on attacker behaviors, indicators of compromise, and hacker profiles, this system aims to empower a more informed and predictive defense posture, significantly strengthening the overall digital security landscape through enhanced AI-driven threat analysis and sharing.

VIII. REFERENCES

[1] [1] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1197–1227, 2nd Quart., 2015.

[2] 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.

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

[4] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence—Issue and challenges," Ind. J. Elect. Eng. Comput. Sci., vol. 10, no. 1, pp. 371–379, 2018.

[5] A. Ibrahim, D. Thiruvady, J.-G. Schneider, and M. Abdelrazek, "The challenges of leveraging threat intelligence to stop data breaches," Front. Comput. Sci., vol. 2, p. 36, Aug. 2020.

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

[7] M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "A literature review on mining cyberthreat intelligence from unstructured texts," in Proc. Int. Conf. Data Min. Workshops (ICDMW), 2020, pp. 516–525.

[8] R. Brown and P. Stirparo, SANS 2022 Cyber Threat Intelligence Survey, SANS Inst., North Bethesda, MD, USA, 2022.

[9] 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.

[10] "What is cyber threat intelligence? 2022 threat intelligence report." 2022. Accessed: Feb. 13, 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence.