International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database

[1]T. Niranjan Babu, [2]S.K.Mohammed Waseef, [3]K.Siva Sai Reddy

[1]Assistant Professor, Department of Computer Science and Engineering and Cyber Security (UG), Madanapalle Institute of Technology & Science (Autonomous), Madanapalle, India
[2,3]UG Scholar, Department of Computer Science and Engineering and Cyber Security (UG), Madanapalle Institute of Technology & Science (Autonomous), Madanapalle, India
E-mails: [1]niranjanbabut@mits.ac.in, [2]shaikwaseef143@gmail.com, [3]Ksivasai34@gmail.com

***Abstract* - MITRE ATT&CK is a detailed knowledge base of adversary TTPs, based on real-world cyber-attack scenarios. It's widely used throughout government, academia, and industry. It has become a cornerstone for threat modeling, risk assessment, and developing defense strategies. Since the topics of the framework have been highly applied to these fields, comprehensive statistical analysis of this dataset holds the need to be able to uncover actionable insights. This work therefore fills this gap by systematically extracting, analyzing, and characterizing insights from the knowledge base of statistical insights in the MITRE ATT&CK threat database. A hierarchical analysis is executed, starting at the level of threat profiles then down to very specific techniques captured in the cataloged database; the findings recommend improvements in strengthening the cybersecurity posture in enterprises, in ICS as well as the mobile infrastructures. It is intended to give a better view of the data and provide guidance for further investigations in support of the development of robust, data-driven security strategies.**

Keywords: Threat Modeling, Cyber Threats, Statistical Analysis, Risk Assessment, Cybersecurity, Defensive Strategies.

I. INTRODUCTION

The MITRE ATT&CK framework has become a foundational resource for understanding and mitigating cyber threats. Developed by MITRE Corporation, it provides a structured repository of adversarial tactics, techniques, and procedures (TTPs) observed in real-world cyber incidents. Since its inception, it has been widely adopted by cybersecurity professionals, government agencies, and academic researchers [1] for threat modeling, red teaming, and security analytics. The ability to catalog adversary behaviors across various operational stages makes it possible for organizations to proactively defend against sophisticated cyber threats through MITRE ATT&CK. Though its practical applications have been explored in great detail, its dataset has remained an underdeveloped area of study in systematic statistical analysis. This research attempts to bridge this gap by conducting a structured and quantitative investigation into the knowledge base of MITRE ATT&CK, thus revealing patterns that can inform cybersecurity strategies.

An important strength of the MITRE ATT&CK framework is that it uses a hierarchical structuring that categorizes adversary behaviors under tactics, which represent different phases during the execution of an attack. Techniques and sub-techniques further elucidate how these tactics can be executed [2] in various scenarios. This type of granularity allows security teams to design targeted defenses, correlating detected behaviors with known attack patterns. Despite its wide application, the dataset of the framework has not been fully explored from a statistical perspective. The frequency, distribution, and interconnections between different attack techniques could reveal underlying trends in adversarial behavior, which would help cybersecurity teams prioritize defenses and resource allocation.

Cyber threats have grown in complexity over the past few years, targeting a broad spectrum of environments, including enterprise networks [3], cloud infrastructures, Industrial Control Systems (ICS), and mobile platforms. The adaptability of MITRE ATT&CK makes it a valuable tool for defending these diverse domains. However, security teams often struggle with information overload due to the extensive catalog of techniques available in the database. A data-driven approach can help in identifying the most critical attack vectors, allowing organizations to focus on high-impact threats. Our study aims to provide actionable insights that can enhance cybersecurity readiness by analyzing correlations between tactics and techniques.

Following a hierarchical methodology, our study analyzes the MITRE ATT&CK dataset. First, we categorize threat profiles and study trends in attack tactics over time. By applying statistical methods, we quantify the prevalence of specific techniques [4], their relationship with different

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

adversary groups, and their evolution as new techniques emerge. In addition, we analyze the differences within the enterprise, ICS, and mobile domains to quantify sectoral weaknesses. This will allow us to draw attention to attack patterns relevant to certain sectors that cybersecurity professionals use to shape their defense accordingly.

Translation of raw statistical output into recommendations is one of the primary goals of this paper. Organizations cannot keep up with defenses against all possibilities, so some prioritization [5] regarding mitigation is quite essential. Providing security teams with insights into techniques most frequently used, as well as the techniques that have significant impacts, guides security policies and threat intelligence frameworks and incident response strategies. For example, if particular techniques are inordinately related to APTs, organizations may dedicate more surveillance and defensive controls to mitigate these attacks. Our results also inform cybersecurity education and training. Specifically, red teams and blue teams can update their methodologies using actual operational experience.

The research also contributes to the continuous advancement of the MITRE ATT&CK framework. Updates in the dataset must be made continually to keep abreast of changes in adversarial [6] techniques. Detection of trends and anomalies in methodologies related to attacks can serve as feedback for the cybersecurity community to improve on the framework. Our work here also lays down a foundation for future research by opening avenues to machine learning-driven threat detection, automated attack modeling, and predictive cybersecurity analytics.

This framework is a crucial tool for understanding adversarial tactics, yet its dataset has not been fully leveraged for statistical analysis. This study [7] bridges that gap by extracting and interpreting key insights from the framework, offering a structured approach to understanding cyber threats. Through a hierarchical analysis of tactics and techniques, we aim to provide security practitioners with valuable intelligence to strengthen their defenses. The results will support enterprises, ICS operators, and mobile security professionals in the decision-making process, contributing in turn to an increasingly resilient cybersecurity ecosystem.

This work is organized as Section II presenting a review of the literature survey. Section III describes the methodology, highlighting its key features and functionality. Section IV discusses the results, analysing the system's effectiveness. Lastly, Section V concludes with the main findings and explores future implications.

II. LITERATURE REVIEW

Cyber threat intelligence serves as an indispensable component in today's security operations because it enables organizations to predict, discover, and react to attacks. The frameworks for adversary tactics are standardized structures, which can categorize the actual attack behaviors through real-world incident observations. However, though a lot of these frameworks are employed in the process of security operations, the dataset is relatively less explored in quantitative terms. Statistics can analyze and show patterns on attack methodologies and threat actor behavior. Such insights are better for risk assessment and proper strategic planning. A data-driven approach enhances cybersecurity resilience by merely prioritizing high-risk techniques and aligning security controls with changing attack trends.

It is possible to understand adversarial behavior and design cybersecurity defenses more effectively through threat modeling. It involves mapping attack strategies into structured categories, by means of which organizations can assess vulnerabilities and prepare appropriate countermeasures. Effective threat [8] modeling requires analyzing how attack techniques interrelate across different operational phases. A quantitative analysis of adversarial tactics may reveal the most exploited vulnerabilities. It helps organizations to prioritize security resources in the right areas. Statistical analysis can be used by security teams to predict attack trends, improve detection mechanisms, and enhance overall cyber resilience in enterprise, cloud, and industrial environments.

Industrial control environments are highly challenged in terms of cybersecurity because they heavily rely on legacy systems and infrequently [9] update. Many of the security frameworks designed for enterprise networks fail to address the specifics of critical infrastructure, however. Structured analysis of attack techniques against an industrial environment can define the most frequent types of threats. The frequency and impact of specific attack methods may therefore be understood better through improved risk mitigation strategies. A data-driven approach to cybersecurity for these systems improves resilience, ensuring that security investments focus on high-risk attack vectors that pose significant operational threats.

Mobile devices have become the primary attack surface because of their prevalence and increased storage of sensitive information. Security mechanisms designed for traditional networks do not fully [10] address the evolving mobile threat landscape. Cyber adversaries exploit these vulnerabilities by exploiting platform vulnerabilities, application weaknesses, and misconfigurations to gain access into mobile systems. Looking at statistical studies on mobile-focused attack

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

strategies reveals emerging trends and helps organizations improve defenses. Enhancing protections against evolving threats involves prioritizing security measures according to attack frequency and severity. These trends in understanding aid in developing better mobile security policies and incident response strategies.

Advanced persistent threats often use highly complex attack methods. They usually remain undetected for prolonged periods. Thereby, knowing the patterns involved in their operational tactics helps [11] organizations become more effective with their defense. A statistical review of historical APT activity can disclose frequently used attack vectors and emerging methodologies. Hence, by considering trends over time, security teams can predict possible future attack strategies and implement proactive defenses. Quantitative insights into APT operations support attribution efforts because the intelligence teams are able to link specific techniques with known adversary groups and apply corresponding mitigation efforts.

Developing intrusion detection and prevention systems falls under the ambit of cybersecurity frameworks. Systems developed under this category rely on predetermined attack models that help to identify malicious behavior in real time. Statistical examination of attack patterns will improve detection accuracy by identifying the common vulnerabilities being exploited. The organizations can optimize their security monitoring capabilities and reduce false positives by focusing on high-frequency attack techniques. This data-driven approach enhances overall threat detection effectiveness [12], allowing security teams to allocate resources efficiently and prioritize responses to the most critical threats.

Machine learning has been widely adopted for cybersecurity applications, especially in anomaly detection and automated threat response. Labeled datasets that contain attack behavior patterns [13] are used for training AI-driven security models. The efficiency of these models is highly dependent on the selection of high-quality features and accurate classification of attack methods. A statistical analysis of the attack data will help in identifying the most relevant attributes for machine learning models. Understanding attack trends enables AI systems to focus on high-impact threats, which ensure the accuracy and efficiency of automated security mechanisms in different network environments.

Incident response teams must have a structured methodology to analyze cyber threats and mitigate potential damage. Mass-scale handling of cyber incidents requires strategies that often focus on the most impactful threats. A statistical analysis of common [14] attack techniques can help response teams identify frequently exploited vulnerabilities and attack paths. Leverage data-driven insights to improve their playbooks, speed up response times, and minimize the disruption in operation. Quantitative findings enhance decision-making, ensuring that mitigation efforts are targeted at the most severe security threats.

Cyber deception techniques are gaining traction as an effective way to mislead attackers and gather intelligence on their tactics. The design of effective deception strategies is based on the understanding of which attack techniques are most commonly used. A statistical [15] evaluation of adversarial behaviors allows organizations to deploy decoys in high-risk areas. Aligning deception-based defenses with real-world attack patterns increases attacker dwell time while providing security teams with valuable intelligence. This proactive security approach strengthens overall cyber resilience by reducing an attacker's ability to operate undetected.

The sharing of threat intelligence increases collaborative cybersecurity defense as it enables organizations to share information about emerging threats. Standardized classification systems enable security teams and industry stakeholders to communicate [16] consistently. However, quantitative analysis is necessary for meaningful insights to be extracted from shared intelligence. Statistical evaluation of attack data enables organizations to identify industry-specific threat patterns and emerging attack methodologies. Understanding how attack techniques evolve over time improves proactive defense strategies, allowing organizations to implement measures that address the most significant security risks.

Cybersecurity training and awareness programs are essential for equipping security professionals with the knowledge required to counter evolving threats. However, training effectiveness depends on focusing on the most relevant attack methods. Statistical analysis [17] of attack techniques commonly encountered can be helpful in tailoring the training content according to real-life threats. Data-driven approach is a boon for security professionals as it brings out the most critical cyber risks. Thus, aligning the training programs with actual trends of threats enhances workforce readiness and overall security posture.

III. METHODOLOGY

The continuously evolving landscape in cybersecurity necessitates successive developments in threat intelligence as well as defenses. This is exactly where the MITRE ATT&CK framework is useful-it systematically documents the adversary tactics, techniques, and procedures found in real-world cyber incidents. However, despite widespread use within the

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

development of threat models as well as security assessments, this framework has not been subjected to extensive statistical analysis in order to derive deeper insights. This study bridges that gap by applying a structured, data-driven approach to analyze the MITRE ATT&CK knowledge base. The research looks at the relationships between threat groups, techniques, and targeted infrastructures to identify attack patterns, emerging trends, and platform-specific vulnerabilities. The findings provide actionable intelligence to strengthen cybersecurity postures across enterprises, Industrial Control Systems (ICS), and mobile platforms. This study enhances situational awareness but also informs proactive security strategies for organizations and researchers in the cybersecurity domain by using a hierarchical and statistical approach.

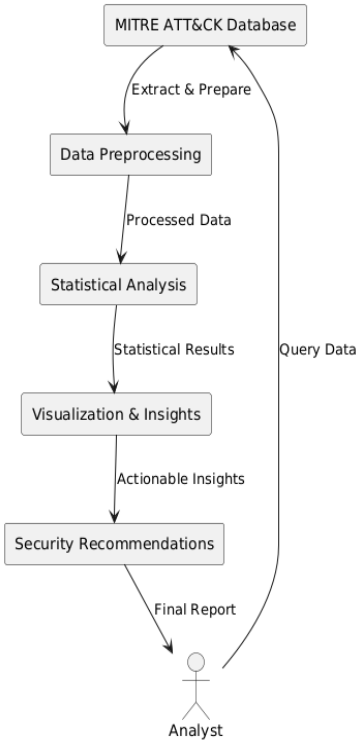

Figure 1: Architecture Diagram

Depicting a data flow and processing for security analysis

A. Data Extraction and Preprocessing

The MITRE ATT&CK dataset is retrieved from its official repository to ensure a comprehensive and up-to-date collection of threat intelligence. This dataset consists of structured information on adversary groups, tactics, techniques, procedures, and their mappings to targeted infrastructures. The raw data are preprocessed with a pipeline that enhances consistency and usability. The first step involves the identification and resolution of redundant entries and inconsistencies through normalization. Then, missing values are addressed using statistical imputation techniques if any exist. The dataset is structured into hierarchical categories to allow for efficient querying and analysis. Data transformation methods, including encoding and feature engineering are applied to prepare the information for further statistical examination. Thus, this preprocessing phase ensures that the dataset is robust, standardized, and ready for some advanced analytical techniques. A cleaned and structured dataset would then be used in the subsequent stages of hierarchical analysis to extract meaningful insights related to adversarial behaviors and attack patterns.

B. Hierarchical Analysis of Threat Profiles

Adopting a hierarchical approach, the analysis of adversary threat profiles is systematically done from broad threat actor categorizations to specific attack techniques. First, the classification into threat groups is based on documented tactics, so a general assessment of often-used attack strategies may be done and thereafter statistical methods, such as frequency analysis and correlation metrics, in order to identify common patterns among them. This method points out the most used techniques and how often they appear with other techniques, as used by other adversaries. It utilizes network graph visualization and heatmaps to express interrelations among groups of people and their applied techniques. With these relations of the threat actors with their respective attack methods, the structured approach offers an outlook into how cyber adversaries operate. The results help predict the future trend of attacks, thus helping organizations build a counter based on empirical evidence rather than theoretical assumptions. This hierarchical structure allows insights to be granular, comprehensive, and practically applicable.

C. Technique-Level Statistical Characterization

Attack methodologies are better understood by quantitative analysis of the individual techniques of the MITRE ATT&CK framework. Each technique's prevalence is assessed by calculating occurrence frequencies over multiple adversary profiles. Temporal trend analysis will help establish shifts in the behavior of attackers over time, indicating emerging and declining techniques. Correlation analysis will be applied to understand how different techniques fit together to understand attack chain patterns, and an entropy-based metric is introduced to measure diversification by threat actors. This shall be a quantitative measure of how widely adopted a particular method is or how specialized a particular method might be. These insights allow security teams to focus on defensive capabilities against the most commonly used and potentially evolving techniques of attack. This knowledge of technique-level trends will enable cybersecurity practitioners to craft targeted defense strategies that make them better at

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

detecting and mitigating threats in more varied attack scenarios.

D. Platform-Specific Analysis

Cyber threats are quite varied in different operational environments, which require a platform-specific assessment of attack techniques. MITRE ATT&CK categorizes the techniques based on application in the respective domains of enterprise, Industrial Control Systems, and mobile security. Through statistical analysis on the dataset, the frequency of each technique applied across the mentioned environments can be derived, showing attack vectors with greater criticality in those sectors. Such a step further discusses cross-domain attack patterns that focus on the attacks that have broad risks but depend on a single infrastructure. Comparative analysis aids in prioritizing security efforts by highlighting domain-specific vulnerabilities, allowing organizations to make effective resource allocation. For example, ICS environments are likely to be more susceptible to lateral movement attacks, while mobile platforms are more vulnerable to credential theft techniques.

IV. RESULT AND DISCUSSION

The statistical analysis of the MITRE ATT&CK dataset indicates that there are some significant patterns in adversary behavior, technique prevalence, and platform-specific attack strategies. The frequency distribution of threat groups shows that a small subset of well-known adversaries is responsible for a disproportionate number of attack techniques. High-profile groups show a broad attack surface, leveraging diverse methods across multiple domains. Conversely, less known attackers specialize in fewer techniques, which implies targeted and strategic attacks, rather than the wide exploitation of tools.

A closer look at the attack techniques reveals that some methods are commonly used by all threat profiles. Credential dumping, privilege escalation, and C2 techniques show the highest frequency, indicating that these are critical to adversarial operations. Data exfiltration methods also correlate well with persistence tactics, which suggests that attackers often target long-term infiltration before stealing data. This insight suggests that early detection of persistence mechanisms can significantly mitigate data breaches.

Temporal analysis of attack trends indicates a steady increase in the adoption of sophisticated evasion techniques. Adversaries are increasingly employing defense evasion methods such as process injection and obfuscated scripting to bypass security measures. The rise in living-off-the-land (LotL) techniques, where attackers exploit legitimate system tools, further complicates detection efforts. This trend underscores the need for enhanced anomaly detection systems capable of distinguishing malicious use from legitimate administrative activities.

The analysis of the attack tactics suggests that spear-phishing and exploiting public-facing applications remain the major initial access methods, but mobile and ICS environments involve different attack vectors than traditional enterprise systems. While in ICS environments, adversaries widely use external remote services and valid accounts to acquire initial access, this indicates strong authentication controls to be implemented at the earliest level. In terms of mobile threats, quite naturally, their main exploitation focuses on application-based vulnerability: developing secure apps, permission controls must be really strict.

Platform-specific analysis came out with different risk profiles between the enterprise, ICS, and mobile infrastructures. Enterprise environments have a higher predominance of privilege escalation and lateral movement attacks given the sophistication of networked corporate systems. As for ICS attacks, system impairment and sabotage come into play; attackers focus more on disruption than data theft. In contrast, mobile threats rely much on social engineering and unauthorized application modifications to take control of the devices. The differences indicate that there is a need for custom defense strategies for each platform.

The diversity of technique adoption among APT groups that is, some actors are very narrow in their few effective techniques that they use, and others are constantly changing their ways to avoid getting caught. All this indicates the need for looking beyond traditional signature-based security systems and supplementing them with more behavioral analysis as well as with machine learning driven anomaly detection.

V. CONCLUSION

The current study gives an in-depth statistical analysis of the MITRE ATT&CK framework, providing insight into the critical nature of adversary tactics, techniques, and attack patterns for enterprises, ICS environments, and mobile. This way, systematic analysis of the dataset revealed high-frequency attack techniques, correlations between tactics, and platform-specific vulnerabilities that present a data-driven understanding of modern cyber threats. The results show that the small percentage of clever adversaries is responsible for most attacks, thus underlining the importance of intelligence-led defence strategy. One of the key takeaways is the prevalence of credential access, privilege escalation, and

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

command-and-control techniques across multiple attack scenarios.

Common attack chains and technique dependencies are other critical areas of examination. Understanding the pattern of adversary movement through different stages of an attack can help security teams predict and interrupt attack sequences before their final objective is achieved. Such proactive attitudes to cyber resilience enhance that resilience and minimize the impact of security incidents. Additionally, the entropy-based analysis of technique distribution shows how advanced threat actors are flexible. The former uses a few effective but limited techniques, whereas the latter changes their techniques every now and then in order to stay ahead of the detection mechanisms. The results thus developed will establish the bedrock for strengthening cybersecurity strategies and refining risk assessments and defensive mechanisms. Future studies may be carried out on top of this work by incorporating real-time attack data to establish advanced predictive models for furthering resilience in cybersecurity.

REFERENCES

[1] A.A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," in IEEE Access, vol. 11, pp. 125138-125158, 2023, doi: 10.1109/ACCESS.2023.3327016.

[2] J. Jang, K. Kim, S. Yoon, S. Lee, M. Ahn and D. Shin, "Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage," in IEEE Access, vol. 11, pp. 45113-45128, 2023, doi: 10.1109/ACCESS.2023.3273612.

[3] S. Ghosh, A. Zaboli, J. Hong and J. Kwon, "An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System," in IEEE Access, vol. 11, pp. 14752-14777, 2023, doi: 10.1109/ACCESS.2023.3243906.

[4] Z. -S. Chen et al., "Clustering APT Groups Through Cyber Threat Intelligence by Weighted Similarity Measurement," in IEEE Access, vol. 12, pp. 141851-141865, 2024, doi: 10.1109/ACCESS.2024.3469552.

[5] F. Aldauiji, O. Batarfi and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," in IEEE Access, vol. 10, pp. 61695-61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

[6] S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi and M. Surridge, "Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems," in IEEE Access, vol. 12, pp. 82482-82505, 2024, doi: 10.1109/ACCESS.2024.3404264.

[7] S. H. Javed et al., "APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System," in IEEE Access, vol. 11, pp. 74000-74020, 2023, doi: 10.1109/ACCESS.2023.3291599.

[8] M. Alajmi, H. A. Mengash, H. Alqahtani, S. S. Aljameel, M. A. Hamza and A. S. Salama, "Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment," in IEEE Access, vol. 11, pp. 127669-127678, 2023, doi: 10.1109/ACCESS.2023.3332213.

[9] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto and H. Inoue, "A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS," in IEEE Access, vol. 11, pp. 18148-18156, 2023, doi: 10.1109/ACCESS.2023.3246497.

[10] F. De Rosa, N. Maunero, P. Prinetto, F. Talentino and M. Trussoni, "ThreMA: Ontology-Based Automated Threat Modeling for ICT Infrastructures," in IEEE Access, vol. 10, pp. 116514-116526, 2022, doi: 10.1109/ACCESS.2022.3219063.

[11] A.Presekal et al., "Cyber Security of HVDC Systems: A Review of Cyber Threats, Defense, and Testbeds," in IEEE Access, vol. 12, pp. 165756-165773, 2024, doi: 10.1109/ACCESS.2024.3490605.

[12] D. Mishchenko, I. Oleinikova, L. Erdődi and B. R. Pokhrel, "Multidomain Cyber-Physical Testbed for Power System Vulnerability Assessment," in IEEE Access, vol. 12, pp. 38135-38149, 2024, doi: 10.1109/ACCESS.2024.3375401.

[13] F. Whitelaw, J. Riley and N. Elmrabit, "A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services," in IEEE Access, vol. 12, pp. 34752-34768, 2024, doi: 10.1109/ACCESS.2024.3373265.

[14] L. Novais, N. Naia, J. Azevedo and J. Cabral, "Let’s Get Cyber-Physical: Validation of Safety-Critical Cyber-Physical Systems," in IEEE Access, vol. 12, pp. 142569-142581, 2024, doi: 10.1109/ACCESS.2024.3470216.

[15] F.-Z. Hannou et al., "Semantic-Based Approach for Cyber-Physical Cascading Effects Within Healthcare Infrastructures," in IEEE Access, vol. 10, pp. 53398-53417, 2022, doi: 10.1109/ACCESS.2022.3171252.

[16] A.Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz and A. Goulart, "Design of Next-Generation Cyber-Physical Energy Management Systems: Monitoring to Mitigation," in IEEE Open Access Journal of Power and Energy, vol. 10, pp. 151-163, 2023, doi: 10.1109/OAJPE.2023.3239186.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 33-39, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202505
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

[17] M. Battaglioni, G. Rafaiani, F. Chiaraluce and M. Baldi, "MAGIC: A Method for Assessing Cyber Incidents Occurrence," in IEEE Access, vol. 10, pp. 73458-73473, 2022, doi: 10.1109/ACCESS.2022.3189777.

[18] G. B. Gaggero, A. Armellin, G. Portomauro and M. Marchese, "Industrial Control System-Anomaly Detection Dataset (ICS-ADD) for Cyber-Physical Security Monitoring in Smart Industry Environments," in IEEE Access, vol. 12, pp. 64140-64149, 2024, doi: 10.1109/ACCESS.2024.3395991.

[19] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya and S. Khan, "Offensive Security: Cyber Threat Intelligence Enrichment with Counterintelligence and Counterattack," in IEEE Access, vol. 10, pp. 108760-108774, 2022, doi: 10.1109/ACCESS.2022.3213644.

[20] A.Presekal, A. Ştefanov, V. S. Rajkumar, I. Semertzis and P. Palensky, "Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems," in IEEE Access, vol. 12, pp. 177746-177771, 2024, doi: 10.1109/ACCESS.2024.3507386.

Citation of this Article:

T. Niranjan Babu, S.K.Mohammed Waseef, & K.Siva Sai Reddy. (2025). Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. In proceeding of Second International Conference on Computing and Intelligent Systems (ICCIS-2025), published in *IRJIET*, Volume 9, Special Issue ICCIS-2025, pp 33-39. Article DOI https://doi.org/10.47001/IRJIET/2025.ICCIS-202505

****

