Sparking Light Publisher

Sparklinglight Transactions on Artificial Intelligence and Quantum Computing

journal homepage: https://sparklinglightpublisher.com/

A Systematic Evaluation of Artificial Intelligence's Impact on the Landscape of Threat Modeling

Santosh Pai[a], Srinivasa. R. Kunte[b], Nadeem Najeeb[c]

[a]*Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India*
[b]*Research Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India*
[c]*Cyber Security Architect, Abu Dhabi, U.A.E*

Abstract

This article systematically evaluates the influence of Artificial Intelligence (AI) on the landscape of Threat modeling in cybersecurity. The study involves an extensive review of relevant journal articles, books, and conference papers to comprehensively assess the current state of the field. By synthesizing existing literature, we identify and analyze the ways in which AI technologies are applied in Threat modeling methodologies. The evaluation explores the strengths and limitations of these applications, shedding light on the advancements that have significantly enhanced Threat modeling. Furthermore, the research includes a meticulous gap analysis within the existing literature, revealing areas where further investigation is warranted. Identified gaps in the current research landscape serve as a foundation for proposing future research directions in AI-enhanced Threat modeling. The current literature related to the current landscape of Artificial Intelligence research in cybersecurity predominantly focuses on articles and active studies pertaining to the detection and prevention of cyber-attacks. However, there is a noticeable gap in the existing literature when it comes to leveraging Artificial Intelligence to enhance Threat modeling. While numerous innovative methods have been proposed in recent articles, these predominantly concentrate on Threat modeling within specific domains, such as unmanned vehicles, Cyber-Physical Systems, and Healthcare. There is a lack of generalization in applying these findings to improve Threat modeling practices more broadly. A promising avenue for further research lies in the automation of Threat modeling. Existing literature predominantly emphasizes the study of Threat generation areas, leaving other crucial aspects, such as Architecture representation and Model validation, in need of more comprehensive exploration and analysis.

Keywords: Threat modeling; Artificial Intelligence; Machine learning; Cybersecurity

1. Introduction

Threat modeling is a systematic approach employed in cybersecurity to proactively identify and manage potential threats and vulnerabilities within information systems. It involves a structured analysis of a system's components, data flows, and potential attack vectors to evaluate the likelihood and impact of different security risks. By understanding potential threats early in the development process, organizations can implement robust security measures to safeguard their assets and sensitive information [1].

Threat modeling serves as a critical component in the arsenal of cybersecurity practices, aiding in the identification and prioritization of security concerns. Threat modeling methodologies allows organizations to properly evaluate threats and vulnerabilities [2] [3]. For instance, in the healthcare sector, where the protection of patient data is paramount, Threat modeling becomes indispensable.

Email address of Authors: g.santoshpai@gmail.com, kuntesrk@gmail.com, mail.nadeemn@gmail.com

Please cite this article as: Santosh Pai, Srinivasa. R. Kunte, and Nadeem Najeeb (2023). A Systematic Evaluation of Artificial Intelligence's Impact on the Landscape of Threat Modeling. *Sparklinglight Transactions on Artificial Intelligence and Quantum Computing*, 3(2), 1-8. **ISSN (Online):2583-0732.** Received Date: 2023/12/01, Reviewed Date: 2023/12/07, Published Date: 2023/12/10.

The United States regulatory body, Food and Drug Administration (FDA) is increasingly emphasizing the incorporation of Threat modeling practices as part of software development lifecycle of medical devices [4] [5] [6]. By doing so, they aim to ensure that these devices are resilient to potential cyber threats, thereby protecting patient safety and preserving the integrity of vital healthcare systems.

One of the key advantages of Threat modeling lies in its proactive nature, enabling organizations to identify and protect against the potential security risks before they are exploited by malicious actors [7]. Additionally, Threat modeling facilitates informed decision-making for management and technical teams. It aids in resource optimization by directing efforts towards addressing the most critical and high-impact vulnerabilities [8] [9]. Moreover, Threat modeling fosters a security-aware culture within organizations, encouraging a mindset that considers security implications throughout the entire development process. The growing emphasis on Threat modeling by regulatory bodies like the FDA reflects a broader recognition of its efficacy in enhancing the resilience of vital systems in the face of growing cyber threats.

Artificial Intelligence (AI) concentrates on devising intelligent machines to accomplish repetitive tasks done by humans [10]. The general AI aims to maintain the ability to comprehend, understand, and use knowledge across various domains. The field of AI has witnessed remarkable advancements in recent years, driven by researches in the underlying technologies, revolutionizing industries and domains across the globe [11].

In this paper, we conducted a systematic evaluation of the applications of the area of Artificial Intelligence on the landscape of Threat modeling. Our research involved an exhaustive review of pertinent journal articles, books, and conference papers, aiming to comprehensively analyze the current state of the field. Through this extensive literature review, we identified and examined the multifaceted applications of AI. Additionally, we performed a thorough gap analysis within the existing literature, pinpointing areas where further exploration is needed. This paper not only contributes to a nuanced understanding of AI's role in cybersecurity but also proposes research directions to address identified gaps, providing a valuable roadmap for future investigations in this critical intersection of artificial intelligence and threat modeling.

2. Methodology

The literature review involved searching various scholarly articles from recognized journals, academic conferences, and books. The search was conducted on the areas of Threat modeling and Artificial Intelligence. Majority of the papers used in the study were obtained using Web of Science platform. We also used Google Scholar for to ensure better coverage of the scholarly articles. The search string used was a combination of ‘Threat modeling’, ‘threat analysis’, ‘security by design’, ‘Artificial Intelligence’, and ’machine learning’. Various combinations were used to ensure we gather all relevant articles.

3. Literature Survey

The details of our literature study have been reported here under two sub-sections; Articles on Threat modelling and Cyber security articles utilizing AI as they happen to be the two primary areas of our literature review.

3.1. Threat modeling articles

In the study of Valenza et. al. [14], the focus is to include human and physical elements in the Threat modeling process. Typical Threat Analysis activities include the cyber security aspects. The human aspects involved considers the attack triggered by human on the systems that involve significant human interactions. The devices installed in remote areas are susceptible to physical attacks leading to critical infrastructure impacts. The study includes some of the examples such as attacks on the wind farm, a safe box, and a web server. A new software called TAMELESS is also implemented as part of the study to perform Threat modeling. The software is tested in various attack scenarios.

The risk assessment framework study of Ekstedt et. Al [15] is focused on Threat modeling of the Enterprise Information Technology domain. The study has identified current gaps in the Threat modeling methodologies and risk calculation techniques. Outcome of the study involves a metamodel based approach named Yet Another Cybersecurity Risk Assessment Framework (Yacarf). It is focused on the Enterprise IT domain and not generalized to other domains. The study also provides examples on applying the suggest methodology.

Widel et. al. [16] studied the Meta Attack Language and provided the domain specific language's syntax in detail and also semantics to apply the language in different areas. The study aims to formalize the languages to be used in different domains. The study also captures various domains where MAL is formally introduced and used. Rencelj Ling and Eksetedt [17] studied Meta Attack Language for substation automation systems. The study included creating extensions to the language to include threats and assets relevant to the domain. The extension of threats used the review of the previous attacks in the substation automation domain. Engstrom et. al. [18] further extended the Meta Attack Language in the study for creating AWS domain specific language. The study also found that the use of domain specific languages requires less efforts and security expertise of the user performing the Threat modeling.

Microservice based application Threat modeling is studied by Wong et. al. [19]. The study indicates microservice Threat modeling as an area that needs deep research. Using the STRIDE methodology, the Threat modeling is performed for a microservice application based on containers. The identified threats are then listed with respective mitigations. Survey method is used to collect the mitigations for the identified threats.

Studies of Azam et. al. [20] provides a privacy perspective for the Threat modeling of autonomous systems. The study identifies gaps from twelve different Threat modeling methodologies with respect to privacy requirements specified in General Data Protection Regulations. A novel methodology is proposed to include GDPR requirements in the Threat modeling. Rodrigues et. al. [21] created a Threat modeling methodology for online social networks. The study also evaluates the effectiveness of the methodology on novice users performing Threat modeling. The methodology provides is found to be easy for novice users and also helps include privacy controls in the system design phase.

Masi et. al. [22] provides a methodology for digital twins for critical cyber-physical systems. The proposed method uses a security by design approach. The study also identified that using digital twins for security assessments, allowed testing the mitigations before they are applied to production systems.

The Threat modeling methodologies applicable for financial institutions is studied by Alevizos and Stavrou [23]. The research indicates a single methodology could help protect the institution's crown jewels up to certain level. A broader security coverage would need combination of methodologies.

Hacks et. al. [24] studied different ways to identify effectiveness of the tests to cover the different security areas identified in the Threat modeling. The work also includes a proof of concept of an automated method to calculate the test coverage.

The study done by Ansari et. al. [25] proposed a methodology to elicitate security requirements for a business requirement. The methodology proposed is compared with previous proposed methodologies using Enterprise Resource Planning domain as an example. The STORE methodology is found to be effective in the study compare to other methodologies.

Threat modeling of Cyber Physical Systems is detailed by Khalil et. al. [26]. It provides threat detection methods based on STRIDE, along with asset identification, and trust boundary identification. The study also includes modeling of a microgrid based system on which the novel idea is experimented.

Threats for Unmanned Aerial Vehicles are studied in articles by Almulhem [27]. Threat tree methodology is used to create different branches of attacks along with their mitigations. The research also indicates an area of improvement in deciding the completeness of the Threat trees.

Threat modeling for Agile software development is studied by Bernsmed et. al. [28]. The study included surveys, interviews, and observations methodologies. The outcomes of the study have provided recommendation to improving the effectiveness of Threat modeling in agile teams by creating detailed data flow diagrams, proper asset identification, and using right software tools for the modeling process.

Apart from the above, the details of the study of other papers have been summarized in Table 1.

Table 1 – Scholarly literature on Threat modeling

Focus area of research	Outcome of the Research	Reference
Threat modeling and simulation of attacks in Industrial Internet of Things	A novel Threat modeling language called Threat Response Modeling language is proposed. The method includes attacker profiles to make the Threat modeling process more realistic and relevant to the domain.	[29]
Associating Safety aspects with Threat modeling	Prioritizing the threats identified considering the safety aspects helps to address the critical threats first. The impact-based prioritization proposed is crucial for healthcare sector.	[30]
Automation of attack graph generation	The proposed method generated an attack graph based on the system topology and other vulnerability data provided.	[31]
Threat modeling for Industrial control systems	An Machine Learning and Artificial Intelligence enabled Intrusion Detection System is required to mitigate the threats significantly in Industrial Control Systems.	[32]
Threat modeling for hardware IC supply chain	The study proposed a game-based methodology for identifying threats in hardware supply chains. The proposed method is tested by university students and lacks the practitioners view of the effectiveness.	[33]
Using Markov Decision Process in Threat modeling using Attack Trees	Probabilistic method checking enhances the capability of Attack Trees in performing detailed security analysis. Input to the probabilistic system needs to be in a specific format. Converting architecture diagrams to such formats is not considered in this study.	[34]
Domain specific Threat modeling for Miniaturized Wireless Biomedical Devices.	The study provides a user centric Threat modeling methodology for wireless miniaturized devices. The proposed methodology is compared against other generic methodologies used today. The outcome of comparison indicated the proposed methodology to be sufficient to disclose threats and easy to apply.	[35]
Data driven threat analysis for cloud-based applications	A Threat modeling process names d-TM proposed in the study considers data as the primary asset. The research is applied to a cloud system to identify relevant threats. The threats identified targeted the business and management data.	[36]

3.2 Articles on adoption of Artificial Intelligence in Cybersecurity

A survey was conducted as part of the research by Wazid et. al [37] to identify the uses of machine learning by the cyber security industry and vice versa. The research has identified new areas such as securing the machine learning data using cyber security and improving the accuracy of the algorithms to make better use in the cyber security domain.

Automation of the risk management for threats in the insurance domain is studied by Althar et. al. [38]. The proposed model maps the customer requirements to Common Weakness Enumerations. The mapping is done using a Machine learning model to ease the mapping process. This approach requires updates to the model based on the change in the vulnerabilities data published by the industry and regulators.

Zhang et.al [ailit06] conducted a survey of previous academic literature on the amalgamation of AI and cyber security. Research concluded that a combination of human intelligence and AI works better in the cyber security domain, especially to protect against the real time attacks.

In their study of adversarial attacks based on explainable AI, Kuppa and Le-Khac [40] provided various attacks that are possible from the additional information provided by the explainable AI models. Identifying mitigations to such model extraction attacks is one of the major future research objectives found in the study.

Wang et. al [41] proposed a generative AI threat model to protect against software supply chain attacks. The proposed method uses ChatGPT and other attack matrix to build the threat model. Verification of the proposed model along with the expert review indicated that the method proposed can help identify software supply chain attacks and provide the defense strategies.

Various attributes of the ChatGPT application is studied by Godde et. al. [42] in the area of medical publishing. The study found that it was not accurately possible to distinguish between generated text and human created text in journal articles. The research indicated need for a strict and clear regulation for review of the published articles to be identified as created using ChatGPT or by a human intelligence.

Study by El Mendili et. al [43] combines the detection of fake social media profiles and also the spam messages being spread by those profiles. The method proposed has high accuracy and lesser loss compared to similar algorithms proposed in other studies. The method is limited to Twitter application and not generalized for other applications.

In addition, Table 2 summarize the details of the study of other papers.

Table 2 – Scholarly literature on Artificial Intelligence

Focus area of research	Outcome of the Research	Reference
Threat modeling for AI ML based systems	A new methodology STRIDE-AI is proposed that is extended version of STRIDE methodology. There are not many ML-AI specific threats or countermeasures available in the literature. The study indicates need for Threat modeling methodologies for AI-ML areas.	[44]
Addressing the cyber security attack issues in the home based IoT devices using machine learning approach.	Method considers both service providers for IoT home based system and the users of the system. The proposed methods require user cooperation to provide accurate survey data. Inaccuracy of the data can lead to non-optimal algorithm.	[45]
Detection of malicious DNS messages using machine learning models.	The article proposes an intrusion detection system. The method works with hybrid learning methodology and requires less data to learn. The accuracy is high close to hundred percent.	[46]
Natural Language Processing based Threat analysis for healthcare systems	Proposed method uses Natural Language Processing abilities to parse the widely available documents from the internet. The result of the processing is used as a Threat library for assessing the healthcare systems. Relying on the documents from the internet could be biased in some cases and not very reliable.	[47]
Applications of AI in cyber security	The study focuses on several sub-domains of cyber security such as intrusion detection, network security, fraud detection etc. Review of the included articles does not have any reference with respect to security by design or Threat modeling.	[48]
Study of attacks on machine learning models and proposal of a secure data analytics method	The study involved research of previous articles on the different attacks on the machine learning models. The proposal in the study includes different machine learning models that perform secure data analytics. The comparisons of these	[49]

	various methods using different parameters are provided.	
Identification of insider threats using machine learning	The research proposes a method to train a machine learning model to learn insider behavior based on the organization's user activity data. The end product then categorizes the actions performed by the users as malicious.	[50]
Improving efficiency of attack detection in software defined networks using deep learning	The proposed method includes use of deep learning to extract the hidden features of the intrusions on the software defined networks. The mitigation technique proposed can reduce the attack surface by protecting the network.	[51]

4. Current Status and New Related Issues

The research conducted so far in the areas of Threat modeling and AI has shown various novel ideas and enhancements. Various domains such as healthcare, cyber physical systems, autonomous vehicles, and critical systems were studied. Few research also concentrated on automation of Threat modeling. Most of the Threat modeling research are concentrated on creating models specific to the domain. We could find few papers that provide generalized ideas to improve the Threat modeling.

Based on the review we identified below issues present in the current research:

- Generalized Threat modeling methodologies are not always helpful in identifying domain specific threats. A metamodel based approach needs to be applied to every domain for Threat modeling.
- The research area on applications of AI in Threat modeling needs more contribution, as this currently lacks research.
- Threat rating methods consider the impact and likelihood. However, impacts such as safety are not considered in prioritization.
- Human aspects are important in any type of attacks on the cyber physical systems and the current methods do not always consider these in Threat modeling.
- There is a lack of formalization and awareness of the Meta Attack Language, and few efforts are made to detail the possibilities of using such tools to automate Threat modeling.
- Microservices Threat modeling area needs more research as this is the vehicle for delivering lightweight applications in cloud.
- Privacy aspects are not always integrated in the Threat modeling, and few have put effort to define ways to solve this issue.
- Mitigating the attacks on machine learning models that are built with explainable AI are an area that needs more research.

5. Research Gap

- Current research on Artificial Intelligence in the cyber security domain has many articles and active studies in the area of detection and prevention of cyber-attacks. There is limited literature available in enhancing Threat modeling using Artificial Intelligence.
- Several novel methods proposed in the articles concentrate on Threat modeling of solutions created in specific domains such as unmanned vehicles, Cyber physical systems, and Healthcare. Generalization of the such research to improve the Threat modeling is lacking.
- Automation of Threat modeling has scope for further research as current literature includes majority of study on the Threat generation areas. The other areas such as Architecture representation, and Model validation need more research.

6. Research Agendas

Based on the conducted literature review, we have identified below agendas:

- Investigate role of Artificial Intelligence in creating the system architecture representations in the Threat modeling process.
- Explore the area of threat identification using Artificial Intelligence to provide advanced threats as part of Threat modeling.
- Develop methods to reduce the generation of false positive Threats by using Artificial Intelligence.

- Propose automation possibilities in different stages of Threat modeling using Artificial Intelligence.
- Explore the possibility of integrating Generative Artificial Intelligence in the Threat modeling process.

7. Conclusion

This systematic evaluation has provided a comprehensive overview of the impact of AI on the landscape of Threat modeling in cybersecurity. Through an exhaustive review of pertinent journal articles, books, and conference papers, we have illuminated the diverse applications of AI in Threat modeling. Our analysis has revealed the strengths and limitations of current AI-driven Threat modeling methodologies, highlighting the gaps in the current literature. We critically evaluated the articles and have provided a detailed review of the same. Based on the review of the articles, we defined different research agendas that we plan to work further to contribute to the area of application of AI in Threat modeling.

References

[1] Køien, G. M. (2020). A Philosophy of Security Architecture Design. *Wireless Personal Communications*, 113(3), 1615–1639. https://doi.org/10.1007/s11277-020-07310-5
[2] Abuabed, Z., Alsadeh, A., & Taweel, A. (2023). STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles. *Computers & Security*, 133, 103391. https://doi.org/10.1016/j.cose.2023.103391
[3] Pai, S., & Kunte R., S. R. (2022). A Comprehensive Analysis of Automated Threat Modeling Solution Company: Threat Modeler Software, Inc. *International Journal of Case Studies in Business, IT, and Education*, 249–258. https://doi.org/10.47992/IJCSBE.2581.6942.0193
[4] Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. *IEEE Access*, 9, 40049–40075. https://doi.org/10.1109/ACCESS.2021.3064682
[5] Ahamad, S. S., Al-Shehri, M., & Keshta, I. (2022). A Secure and Resilient Scheme for Telecare Medical Information Systems With Threat Modeling and Formal Verification. *IEEE Access*, 10, 120227–120244. https://doi.org/10.1109/ACCESS.2022.3217230
[6] Wazid, M., Das, A. K., Mohd, N., & Park, Y. (2022). Healthcare 5.0 Security Framework: Applications, Issues and Future Research Directions. *IEEE Access*, 10, 129429–129442. https://doi.org/10.1109/ACCESS.2022.3228505
[7] Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation*, 45, 301540. https://doi.org/10.1016/j.fsidi.2023.301540
[8] Mihelič, A., Hovelja, T., & Vrhovec, S. (2023). Identifying Key Activities, Artifacts and Roles in Agile Engineering of Secure Software with Hierarchical Clustering. *Applied Sciences*, 13(7), 4563. https://doi.org/10.3390/app13074563
[9] Rao, S. P., Chen, H.-Y., & Aura, T. (2023). Threat modeling framework for mobile communication systems. *Computers & Security*, 125, 103047. https://doi.org/10.1016/j.cose.2022.103047
[10] Biswas, S. (2023). Role of ChatGPT in Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4403584
[11] Gill, S. S., & Kaur, R. (2023). ChatGPT: Vision and challenges. *Internet of Things and Cyber-Physical Systems*, 3, 262–271. https://doi.org/10.1016/j.iotcps.2023.05.004
[12] Crothers, E. N., Japkowicz, N., & Viktor, H. L. (2023). Machine-Generated Text: A Comprehensive Survey of Threat Models and Detection Methods. *IEEE Access*, 11, 70977–71002. https://doi.org/10.1109/ACCESS.2023.3294090
[13] Liu, X., Zhu, P., Zhang, Y., & Chen, K. (2015). A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. *IEEE Transactions on Smart Grid*, 6(5), 2435–2443. https://doi.org/10.1109/TSG.2015.2418280
[14] Valenza, F., Karafili, E., Steiner, R. V., & Lupu, E. C. (2023). A Hybrid Threat Model for Smart Systems. *IEEE Transactions on Dependable and Secure Computing*, 20(5), 4403–4417. https://doi.org/10.1109/TDSC.2022.3213577
[15] Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00713-y
[16] Wideł, W., Hacks, S., Ekstedt, M., Johnson, P., & Lagerström, R. (2023). The meta attack language—A formal description. *Computers & Security*, 130, 103284. https://doi.org/10.1016/j.cose.2023.103284
[17] Rencelj Ling, E., & Ekstedt, M. (2023). A threat modeling language for generating attack graphs of substation automation systems. *International Journal of Critical Infrastructure Protection*, 41, 100601. https://doi.org/10.1016/j.ijcip.2023.100601
[18] Engström, V., Johnson, P., Lagerström, R., Ringdahl, E., & Wällstedt, M. (2023). Automated Security Assessments of Amazon Web Services Environments. *ACM Transactions on Privacy and Security*, 26(2), 1–31. https://doi.org/10.1145/3570903
[19] Wong, A. Y., Chekole, E. G., Ochoa, M., & Zhou, J. (2023). On the Security of Containers: Threat Modeling, Attack Analysis, and Mitigation Strategies. *Computers & Security*, 128, 103140. https://doi.org/10.1016/j.cose.2023.103140
[20] Azam, N., Michala, L., Ansari, S., & Truong, N. B. (2023). Data Privacy Threat Modelling for Autonomous Systems: A Survey From the GDPR's Perspective. *IEEE Transactions on Big Data*, 9(2), 388–414. https://doi.org/10.1109/TBDATA.2022.3227336
[21] Rodrigues, A., Villela, M. L. B., & Feitosa, E. L. (2023). Privacy Threat MOdeling Language. *IEEE Access*, 11, 24448–24471. https://doi.org/10.1109/ACCESS.2023.3255548
[22] Masi, M., Sellitto, G. P., Aranha, H., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling*, 22(2), 689–707. https://doi.org/10.1007/s10270-022-01075-0
[23] Alevizos, L., & Stavrou, E. (2023). Cyber threat modeling for protecting the crown jewels in the Financial Services Sector (FSS). *Information Security Journal: A Global Perspective*, 32(2), 134–161. https://doi.org/10.1080/19393555.2022.2104766
[24] Hacks, S., Persson, L., & Hersén, N. (2023). Measuring and achieving test coverage of attack simulations extended version. *Software and*

Systems Modeling, 22(1), 31–46. https://doi.org/10.1007/s10270-022-01042-9
[25] Ansari, M. T. J., Pandey, D., & Alenezi, M. (2022). STORE: Security Threat Oriented Requirements Engineering Methodology. *Journal of King Saud University - Computer and Information Sciences*, 34(2), 191–203. https://doi.org/10.1016/j.jksuci.2018.12.005
[26] Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. *Computers & Security*, 124, 102950. https://doi.org/10.1016/j.cose.2022.102950
[27] Almulhem, A. (2020). Threat modeling of a multi-UAV system. *Transportation Research Part A: Policy and Practice*, 142, 290–295. https://doi.org/10.1016/j.tra.2020.11.004
[28] Bernsmed, K., Cruzes, D. S., Jaatun, M. G., & Iovan, M. (2022). Adopting threat modelling in agile software development projects. *Journal of Systems and Software*, 183, 111090. https://doi.org/10.1016/j.jss.2021.111090
[29] Zhang, S., Wang, S., Bai, G., Zhang, M., Chen, P., Zhao, C., Li, S., & Zhou, J. (2022). Design of Threat Response Modeling Language for Attacker Profile Based on Probability Distribution. *Wireless Communications and Mobile Computing*, 2022, 1–16. https://doi.org/10.1155/2022/2323228
[30] Castiglione, L. M., & Lupu, E. C. (2023). Which Attacks Lead to Hazards? Combining Safety and Security Analysis for Cyber-Physical Systems. *IEEE Transactions on Dependable and Secure Computing*, 1–16. https://doi.org/10.1109/TDSC.2023.3309778
[31] ..Zdemir S..nmez, F., Hankin, C., & Malacaria, P. (2022). Attack Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases. *Computers & Security*, 123, 102938. https://doi.org/10.1016/j.cose.2022.102938
[32] Kim, K. H., Kim, K., & Kim, H. K. (2022). STRIDE ‐ based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*, 44(6), 991 ‐ 1003. https://doi.org/10.4218/etrij.2021-0181
[33] Hart, S., Halak, B., & Sassone, V. (2022). CIST: A Serious Game for Hardware Supply Chain. *Computers & Security*, 122, 102912. https://doi.org/10.1016/j.cose.2022.102912
[34] Malik, S. U. R., Anjum, A., Moqurrab, S. A., & Srivastava, G. (2022). Towards enhanced threat modelling and analysis using a Markov Decision Process. *Computer Communications*, 194, 282–291. https://doi.org/10.1016/j.comcom.2022.07.038
[35] Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat Modeling and Risk Analysis for Miniaturized Wireless Biomedical Devices. *IEEE Internet of Things Journal*, 9(15), 13338–13352. https://doi.org/10.1109/JIOT.2022.3144130
[36] Alwaheidi, M. K. S., & Islam, S. (2022). Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems. *Sensors*, 22(15), 5726. https://doi.org/10.3390/s22155726
[37] Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 8(3), 313–321. https://doi.org/10.1016/j.icte.2022.04.007
[38] Althar, R. R., Samanta, D., Kaur, M., Singh, D., & Lee, H.-N. (2022). Automated Risk Management Based Software Security Vulnerabilities Management. *IEEE Access*, 10, 90597–90608. https://doi.org/10.1109/ACCESS.2022.3185069
[39] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0
[40] Kuppa, A., & Le-Khac, N.-A. (2021). Adversarial XAI Methods in Cybersecurity. *IEEE Transactions on Information Forensics and Security*, 16, 4924–4938. https://doi.org/10.1109/TIFS.2021.3117075
[41] Wang, M., Wu, P., & Luo, Q. (2023). Construction of Software Supply Chain Threat Portrait Based on Chain Perspective. *Mathematics*, 11(23), 4856. https://doi.org/10.3390/math11234856
[42] Gödde, D., Nöhl, S., Wolf, C., Rupert, Y., Rimkus, L., Ehlers, J., Breuckmann, F., & Sellmann, T. (2023). A SWOT (Strengths, Weaknesses, Opportunities, and Threats) Analysis of ChatGPT in the Medical Literature: Concise Review. *Journal of Medical Internet Research*, 25, e49368. https://doi.org/10.2196/49368
[43] El Mendili, F., Fattah, M., Berros, N., Filaly, Y., & El Bouzekri El Idrissi, Y. (2023). Enhancing detection of malicious profiles and spam tweets with an automated honeypot framework powered by deep learning. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00796-7
[44] Mauri, L., & Damiani, E. (2022). Modeling Threats to AI-ML Systems Using STRIDE. *Sensors*, 22(17), 6662. https://doi.org/10.3390/s22176662
[45] Zhang, Y., Malacaria, P., Loukas, G., & Panaousis, E. (2023). CROSS: A framework for cyber risk optimisation in smart homes. *Computers & Security*, 130, 103250. https://doi.org/10.1016/j.cose.2023.103250
[46] Abu Al-Haija, Q., Alohaly, M., & Odeh, A. (2023). A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach. *Sensors*, 23(7), 3489. https://doi.org/10.3390/s23073489
[47] Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023). A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. *Sensors*, 23(2), 651. https://doi.org/10.3390/s23020651
[48] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121(2), 1189–1211. https://doi.org/10.1007/s11192-019-03222-9
[49] Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Computer Communications*, 153, 406–440. https://doi.org/10.1016/j.comcom.2020.02.008
[50] Kumar, R. (2023). Thee Machine Learning Analysis of Data Granularity for Insider Threat Detection. *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*, 1–7. https://doi.org/10.1109/GCAT59970.2023.10353269
[51] Rao, D. S., & Emerson, A. J. (2023). Cyberattack defense mechanism using deep learning techniques in software-defined networks. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00785-w

******