International Journal of Advance Innovations, Thoughts and Ideas

Commentary Open Access

Cybersecurity: AI/ML, IoT, and Emerging Threats

Dr. Nora Evans*

Center for Cyber Studies, University of Toronto, Toronto, Canada

***Corresponding Author:** Dr. Nora Evans, Center for Cyber Studies, University of Toronto, Toronto, Canada, E-mail: nora.evans@utoronto.ca

Received: 02-Sep-2025, Manuscript No. IJAITI-25-173453; **Editor assigned:** 04-Sep-2025, PreQC No. IJAITI-25-173453(PQ); **Reviewed:** 18-Sep-2025, QC No. IJAITI-25-173453; **Revised:** 23-Sep-2025, Manuscript No. IJAITI-25-173453(R); **Published:** 30-Sep-2025, **DOI**: 10.4172/2277-1891.1000352

Citation: Evans DN (2025) Cybersecurity: AI/ML, IoT, and Emerging Threats. Int J Adv Innovat Thoughts Ideas 14: 352.

Abstract

This collection of studies examines diverse facets of modern cybersecurity, covering threats and defenses across various technological landscapes. *Focus areas include Artificial Intelligence* (AI) and Machine Learning (ML) techniques for detecting cyberattacks in Internet of Things (IoT) environments, alongside the application of Federated Learning (FL) to enhance privacy and security through collaborative model training. We also look at blockchain technology's role in securing healthcare systems and the crucial impact of human factors on cybersecurity vulnerabilities. Addressing specific challenges in smart homes and Cyber-Physical Systems (CPS), these works collectively identify research gaps and propose future directions for robust, privacy-preserving security solutions in an increasingly interconnected digital world.

Keywords

Cybersecurity; Internet of Things (IoT); Artificial Intelligence (AI); Machine Learning (ML); Federated Learning (FL); Blockchain; Smart Homes; Cyber-Physical Systems (CPS); Intrusion Detection; Privacy Preservation

Introduction

The digital era continually faces an evolving landscape of cybersecurity threats, encompassing sophisticated ransomware and Advanced Persistent Threats (APTs), with new vulnerabilities emerging from technologies like Internet of Things (IoT) and 5G [4].

Securing these interconnected systems requires adaptable defenses. Artificial Intelligence (AI) and Machine Learning (ML) have become indispensable tools across various facets of cybersecurity, including intrusion detection, malware analysis, and anomaly detection [8].

These methods offer significant benefits for automating security tasks, though challenges remain concerning data quality, model interpretability, and adversarial attacks. Specifically, in IoT environments, AI-driven methods are meticulously examined for detecting cyberattacks, classifying approaches based on ML paradigms. This delves into the complexities of applying AI to secure the vast and diverse landscape of IoT devices, pinpointing research gaps and future directions in areas like explainable AI, Federated Learning (FL), and adversarial attacks [1].

A thorough examination of Machine Learning and Deep Learning applications reveals their role in enhancing cybersecurity within IoT environments. Various techniques for intrusion detection, malware analysis, and secure data transmission are categorized and critically analyzed, highlighting performance, limitations, and the specific challenges posed by IoT's distributed and resource-constrained nature [2].

This further emphasizes the need for robust, scalable, and privacy-preserving security solutions. A systematic review of IoT

security and privacy requirements underscores critical areas such as authentication, access control, data confidentiality, and integrity across diverse IoT applications. It identifies these requirements based on architectural layers and common attack vectors [10].

Beyond traditional centralized approaches, Federated Learning (FL) presents a compelling paradigm for cybersecurity. An in-depth analysis of FL applications in this domain focuses on its ability to enable collaborative model training across decentralized devices without sharing raw data, thereby significantly enhancing privacy and security [3].

This approach reviews FL architectures for various security tasks, including intrusion detection and malware classification, while discussing challenges like communication overhead, non-Independent and Identically Distributed (non-IID) data distribution, and adversarial attacks on FL, alongside potential solutions and future research directions. The challenges extend to specialized sectors. For instance, smart home environments face a range of cybersecurity issues, from device vulnerabilities and network exploits to data privacy breaches, impacting user safety and system integrity. Securing heterogeneous smart home devices requires robust authentication, secure communication protocols, and user-centric security designs [7].

Similarly, the security of Cyber-Physical Systems (CPS) is a critical area, encompassing unique challenges from the convergence of physical and digital worlds. This includes industrial control systems, smart grids, and autonomous vehicles, identifying crucial research gaps in real-time threat detection and resilient control [9].

Adding another layer of complexity, human factors play a critical role in cybersecurity. A systematic literature review analyzes psychological, sociological, and organizational aspects that influence security behaviors and vulnerabilities, synthesizing findings on security awareness, phishing susceptibility, and insider threats. This proposes a framework for understanding and mitigating human-centric risks in cybersecurity strategies [6].

Furthermore, innovative technologies like blockchain are being explored to bolster security. A review on blockchain technology applications aims to enhance security and privacy in healthcare systems, directly addressing vulnerabilities associated with traditional centralized data management. This outlines blockchain-based solutions for secure electronic health records, patient data privacy, and supply chain integrity, alongside the unique challenges of integrating such technology into complex healthcare infrastructures [5].

Description

A significant body of work focuses on leveraging Artificial Intelligence (AI) and Machine Learning (ML) to bolster cybersecurity, particularly in the rapidly expanding Internet of Things (IoT) landscape. One survey meticulously examines AI-driven methods for detecting cyberattacks in IoT environments, classifying approaches based on various ML paradigms. It explores both the challenges and opportunities in applying AI to secure the vast and diverse array of IoT devices, pinpointing research gaps and future directions, notably in areas such as explainable AI, Federated Learning (FL), and adversarial attacks [1]. Complementing this, another review provides a thorough examination of ML and Deep Learning (DL) applications aimed at enhancing cybersecurity in IoT. This work categorizes and critically analyzes diverse techniques used for intrusion detection, malware analysis, and secure data transmission within IoT, highlighting their performance, inherent limitations, and the unique challenges presented by IoT's distributed and resource-constrained nature [2]. Furthermore, a comprehensive review extends this by exploring the extensive applications of machine learning across various facets of cybersecurity, including intrusion detection, malware analysis, spam filtering, and anomaly detection. It discusses different ML algorithms and their effectiveness in identifying and mitigating cyber threats, underscoring the benefits of ML for automated security tasks while also addressing challenges related to data quality, model interpretability, and adversarial attacks in the broader cybersecurity context [8].

Securing IoT ecosystems fundamentally requires addressing specific architectural and operational challenges. A systematic review comprehensively analyzes the security and privacy requirements for IoT environments. It categorizes these requirements based on IoT architectural layers and common attack vectors, identifying critical areas such as authentication, access control, data confidentiality, and integrity. This review particularly highlights the unique challenges involved in securing resource-constrained IoT devices and emphasizes the imperative for robust, scalable, and privacy-preserving security solutions across a wide spectrum of IoT applications [10]. These vulnerabilities and the sheer scale of IoT devices also contribute to the evolving landscape of cybersecurity threats in the digital era, alongside sophisticated ransomware, Advanced Persistent Threats (APTs), and vulnerabilities introduced by newer technologies like 5G [4]. This underscores the ongoing need for research and development to build more resilient and adaptive cybersecurity defenses.

To counter these pervasive threats, advanced paradigms are gaining traction. An in-depth analysis of Federated Learning (FL)

applications in cybersecurity focuses on how FL enables collaborative model training across decentralized devices without sharing raw data, thereby significantly enhancing privacy and security. This work reviews FL architectures for various security tasks like intrusion detection and malware classification, discussing challenges such as communication overhead, non-Independent and Identically Distributed (non-IID) data distribution, and adversarial attacks on FL, alongside potential solutions and future research directions [3]. Another innovative approach involves blockchain technology, which is being explored to enhance security and privacy, particularly in healthcare systems. This review addresses the vulnerabilities associated with traditional centralized data management and discusses various blockchain-based solutions for secure electronic health records, patient data privacy, and medical supply chain integrity. It outlines the benefits, architectural considerations, and the unique challenges of integrating blockchain into complex healthcare infrastructures [5].

Beyond general technological solutions, cybersecurity must also contend with human factors and domain-specific challenges. A systematic review investigates the critical role of human factors in cybersecurity, analyzing psychological, sociological, and organizational aspects that influence security behaviors and vulnerabilities. It synthesizes findings on topics such as security awareness, phishing susceptibility, insider threats, and user-friendly security interfaces, proposing a framework for understanding and mitigating human-centric risks in cybersecurity strategies [6]. Meanwhile, specific environments like smart homes present their own set of cybersecurity issues, challenges, and research gaps. This systematic review categorizes threats ranging from device vulnerabilities and network exploits to data privacy breaches, discussing implications for user safety and system integrity, and emphasizing the need for robust authentication and secure communication protocols [7]. Lastly, the security of Cyber-Physical Systems (CPS) receives focused attention, discussing unique security challenges from the convergence of physical and digital worlds, covering industrial control systems, smart grids, and autonomous vehicles. This paper highlights various attack vectors, existing defense mechanisms, and identifies crucial research gaps related to real-time threat detection, resilient control, and privacy preservation in interconnected CPS [9].

Conclusion

The provided research thoroughly explores the expansive domain of cybersecurity, highlighting advancements in AI and Machine Learning (ML) for threat detection, particularly within Internet of Things (IoT) ecosystems. One survey meticulously examines AI-driven methods for identifying cyberattacks in IoT, categorizing approaches by ML paradigms and pinpointing challenges in securing diverse IoT devices. This work also identifies future research in areas like explainable AI, Federated Learning (FL), and adversarial attacks. Another review complements this by thoroughly examining ML and Deep Learning techniques to boost IoT cybersecurity, analyzing methods for intrusion detection, malware analysis, and secure data transmission while noting limitations due to IoT's distributed and resource-constrained nature. Beyond IoT, the studies investigate FL applications in cybersecurity, demonstrating how FL enables private, collaborative model training across decentralized devices, crucial for tasks like intrusion detection and malware classification. Emerging threats in the digital era, such as ransomware and Advanced Persistent Threats (APTs), along with vulnerabilities in IoT and 5G, are also explored, alongside current mitigation strategies. The discussions extend to blockchain technology for enhancing security and privacy in healthcare systems, offering solutions for secure electronic health records and medical supply chains. Furthermore, the critical role of human factors in cybersecurity is analyzed, encompassing psychological and organizational aspects that influence security behaviors and insider threats. Specific environments like smart homes face cybersecurity issues, challenges, and research gaps, covering device vulnerabilities, network exploits, and data privacy. Moreover, the security of Cyber-Physical Systems (CPS) is examined, addressing unique challenges in industrial control systems and smart grids. A comprehensive review showcases the extensive uses of ML in cybersecurity, including intrusion detection, malware analysis, spam filtering, and anomaly detection. Finally, security and privacy requirements for IoT ecosystems are systematically reviewed, identifying critical areas like authentication, access control, and data confidentiality for resource-constrained devices.

References

1. Mohamed AF, Mohamed CM, Amine D, Henda BG, Leandros AM et al. (2023) A Comprehensive Survey of AI-based Cyberattack Detection Schemes for IoT. IEEE Comm. Surveys Tutorials 25:757-797.

2. Abdelghani K, Mohamed A, Mounir H, Said D, Mohammed-Amine O et al. (2023) A Review of Machine Learning and Deep Learning Techniques for Cybersecurity in IoT. J. Network Comput. Appl. 227:103704.

3. Xin Y, Yanjun L, Xiang L, Xiang C, Haibo H et al. (2023)

A Comprehensive Survey of Federated Learning for Cyber Security. IEEE Internet Things J. 10:13038-13063.

4. Muneer A, Sajjad NK, Muhammad N, Abdul W, Shahid A et al. (2023) Cybersecurity in the Digital Era: Emerging Threats and Challenges. Future Internet 15:182.

5. Junaid K, Abdul H, Zahid K, Muhammad N, Inayat K et al. (2022) A Review on Blockchain-Based Security and Privacy Preservation in Healthcare Systems. Sensors 22:5885.

6. Abdul M, Abdul H, Zahid K, Muhammad N, Inayat K et al. (2022) Human factors in cybersecurity: a systematic literature review. Human-centric Comput. Inf. Sci. 12:31.

7. Mohammad F, Ali AK, Aymen A, Hadeel AA, Omar Z et al. (2022) A Systematic Review on Cybersecurity Issues, Challenges, and Open Research Gaps in Smart Homes. Sensors 22:4192.

8. Asmaa AQ, Falah HAQ, Hassan MAQ, Zaid HAQ, Zahraa HAQ et al. (2020) Machine Learning for Cyber Security: A Comprehensive Review. J. Adv. Comput. Sci. Tech. 9:1-13.

9. Mohammad J, Abu-Khaled AJ, Mohammad JJ, Hamza AA, Ibrahim AJ et al. (2020) A Review on Current Research, Trends, and Future Directions in Cyber-Physical Systems Security. J. Adv. Comput. Sci. Tech. 9:14-25.

10. Mohammad AK, Teuku ATPA, Sayed HKA, Md AH, Md AH et al. (2019) A Systematic Review of IoT Security and Privacy Requirements. IEEE Access 7:120516-120542.