A Review of AI – Driven Security Frameworks for Autonomous IoT Networks

G.Athisha[1] Prof. (Dr.) S. K. Singh[2]
[1]Postdoctoral Researcher, Lincoln University College, Petaling Jaya, Selangor Darul Ehsan Malaysia
[2]Information Technology, Amity University Uttar Pradesh Lucknow Campus, Lucknow, Uttar Pradesh, India
Email ID: pdf.Athisha@lincoln.edu.my

Abstract

Today's cyber physical world witnesses the growth of Autonomous IoT Networks in most vital sectors such as healthcare, manufacturing, transportation and energy. Unlike traditional IoT networks which are used to predefined data communication flows and perimeter – based defenses, the A-IoT networks are highly adaptive, open – ended and adhoc in structure. These autonomous systems operate with minimal human intervention. The mechanisms which enable the autonomy of the A-IoT networks such as self-learning models, continuous interdevice communication and collaborative behavior make them vulnerable to sophisticated attacks and threats. Threats such as firmware tampering, data spoofing and insider compromise are further increased by the decentralized nature and heterogeneity of A-IoT systems. Further the autonomy of IoT networks make them highly vulnerable to adaptive cyber threats including DDoS attacks, routing manipulation and data poisoning. The traditional IoT security solutions are static and reactive, which focus on prevention rather than sustained operation under attack. The lack of centralized control and unified security policy in A- IoT networks makes real time threat detection and their mitigation strategies challenging. While the deep learning and machine learning models exist for intrusion detection, most of them lack integration with autonomous decision making and recovery, leading to the IoT networks becoming more vulnerable to cyber-attacks. Cyber resilience underlines the important ability of a system to detect, absorb, adapt, recover and learn from the cyberattacks. Thus it becomes imperative today to develop AI – based, context – aware, cyber resilient framework to safeguard autonomous IoT networks where machine learning and reinforcement learning techniques will help in real time threat detection, adaptive mitigation and recovery. The autonomous IoT networks currently lack the self - adaptive mechanisms which can respond to evolving cyber threats, integrated AI – based resilience decision engines, quantitative evaluation of resilience metrics such as recovery time and survivability. Thus this research focusses on the design and simulation of an AI – driven self - adaptive, cyber resilience framework for autonomous IoT networks. The proposed framework would be designed, implemented and evaluated using NetSim providing a realistic simulation environment. We implement multiple cyber-attack scenarios such as DDoS flooding attacks, sinkhole attacks targeting RPL routing, Sybil attacks using false identities and data injection attacks.

Keywords: Autonomous IoT, Cyber-attacks. Cyber resilient, DDoS Attack, Intrusion Detection, Flooding

Introduction

Autonomous Networks are next generation communication systems that use AI, machine learning, automation and self – management mechanisms to operate without human intervention. These autonomous networks are widely used in IoT ecosystems, autonomous vehicles, UAV networks, 5G/6G networks, cyber-physical systems and smart city applications. The complexity, scale and heterogeneity of autonomous environments lead to expanded attack surfaces, real – time data processing demands, sophisticated adversaries, threats and privacy risks.

Challenges in Autonomous IoT Environments

Autonomous IoT environments consist of a large number of devices with varying hardware architectures, communication protocols, software stacks and functions. This variability makes the authentication of devices, firmware integrity and secure data transit more complex.[1]Resource restrictions and real time processing present another obstacle of A-IoT system security[2].A-IoT is real – time, the decisions must be made autonomously within milliseconds, which requires light – weight and latency – aware security techniques [3]One of the research challenges of A-IoT cybersecurity is to develop a real – time, low – overhead, distributed AI – based security solution[4]The risk of data leakage and integrity breaches as these devices continually collect, process and communicate sensitive data such as personal health information, user behavior, geolocation and environmental measurements without the user's content[5].

Traditional network security measures are no longer sufficient to secure the IoT, since IoT applications cannot depend on mechanisms or reactions to the attacks after they have occurred [6]. Enterprises need to have a comprehensive security model which is adaptive in nature that can adapt to moving dynamics in a network. Adaptive network security is an implementation of a security system that analyses the patterns and user activities.[7]The security of autonomous systems require a dynamic, proactive approach to manage heterogeneity, resource constraints, privacy issues and ever-changing threats[8].The shortcomings of traditional cybersecurity procedures increases as the complexity and dynamism of cyber- threats in A-IoT had grown up/[9]Traditional defense mechanisms such as signature – based intrusion detection, rule based access control are outdated techniques which are based on pre-defined threat signatures or set rules. They are found to be ineffective against the zero-day threats in resource constrained IoT networks [10]. They lack situational awareness and on – the – fly flexibility to respond to challenges in cyber physical systems[11].

AI in Cybersecurity

Artificial Intelligence has revolutionized cybersecurity by allowing for data – driven, autonomous and adaptive threat identification and response. Machine learning learns from data patterns and generates predictions without using explicit programming [12]. Supervised Learning is used to perform tasks such as malware classification and intrusion detection, where labelled datasets of known threats exist[13].Unsupervised learning is used for anomaly detection which identifies the unexpected behavior or deviation from prior patterns which indicate an ongoing attack[14].Convolutional and recurrent deep neural networks are used for network traffic analysis, encrypted malware detection and behavioural profiling of IoT devices[15].

In Federated Learning, several A- IoT devices collaborate to train a global model, providing only local model updates than raw data. Deep Learning is used to preserve privacy [16].A swarm based intrusion detection system allows devices to communicate anomaly scores and co – ordinate responses in a decentralized manner[17].AI can enable real time and autonomous threat identification to track attack patterns without the continual participation of humans [18].AI models can identify multivector threats by combining the data from diverse sources by improving threat intelligence correlation[19]

The implementation of cybersecurity in autonomous system should be approached in a holistic manner by balancing automation with robustness, performance with interpretability and intelligence with privacy protection[20].AI enhanced Intrusion Detection and Prevention Systems(IDS/IPS) use ML and DL to examine large volumes of real time traffic and device behavior to detect known and attack patterns[21].

Lightweight IDS models ca be trained in the edge using federated learning to guarantee low latency and threat detection [22]. Unsupervised learning techniques like k – means clustering, auto encoders, one – class support vector machines(SVMs) are used to identify anomalous behaviors in A- IoT networks[23].

Advanced implementations on Graphical Neural Networks(GNNs) can be used to model device – to – device interactions in complex A-IoT infrastructures[24].Malware variants ca be classified with convolutional neural networks(CNNs) and recurrent neural networks(RNNs) by processing the opcode sequences, API call patterns and run – time behavior[25].The traditional authentication systems such as pre shared keys and static credentials are not suited for diverse, large scale deployments.[26]With AI, methods such as decision trees and reinforcement learning adjust privileges on a real time basis depending on the level of risk[27].

AI can also be used to develop lightweight cryptographic algorithms that can dynamically change key sizes, cipher strength and mode of operation based on the degree of threat and available resources [28]AI supports key management enabling automatic key rotation, breach detection and secure key distribution across mesh or adhoc networks [29].Explainable AI(XAI) embedded frameworks are employed to enable human stake holders to have an idea of the reasoning behind the automated decisions[30].

Identified Research Gaps

The current IoT/Autonomous security solutions are fragmented and emphasizes the need for standardized, inter- operable frameworks integrating AI and Block chain.

1.Lack of standardized architecture for autonomous networks

There is also a lack of standardized architecture and a need for cross – layer QoS – aware security frameworks [31].

2. Difficulty in securing AI Decision Models

AI – based systems in autonomous environments face privacy leaks, adversarial risks and data exposure issues [32].

AI models improve detection but also introduce new vulnerabilities such as model manipulation and high computational overhead [33].

3.Limited Lightweight Cryptographic Techniques for IoT Devices

Highlights that IoT devices are resource – constrained and unable to to support heavy security mechanisms [33].

Identifies the need for efficient, low – overhead cryptographic and AI – based techniques for scalable IoT security [34].

4.Poor Integration between cybersecurity and autonomous control systems

The current security systems separate detection and response and lack tight integration with control systems and real time mitigation loops. The need for co – designed AI and block chain systems that integrate decision making and security mechanisms [34].

5.Need for Real Time Distributed Intrusion Detection Systems

Limitation of a centralized IDS including latency, scalability and privacy issues are identified, thereby distributed and real – time IDS are motivated [35].

Federated IDS improves scalability, but still faces non – IDS data and communication overhead challenge [36].

An accuracy of 97% is demonstrated for distributed IDS and reduced resource usage in heterogeneous networks [37].The key challenges in distributed IDS such as Poisoning attacks and data heterogeneity are addressed [38].

Future Research Directions

1.AI – Driven Autonomous Security

An AI based adaptive security orchestration engine that dynamically adjusts security policies in IoT Networks is proposed [39].Deep Learning based Intrusion detection combined with decentralized trust to achieve real – time autonomous threat detection[40]

2.Self – Healing Networks

Autonomous self – healing is introduced through smart contracts, thereby enabling systems to detect and recover from attacks [41]. A true cyber resilient autonomous network model is represented.

3.Secure Federated Learning

RNN based intrusion detection with secure aggregation is used to achieve 98% detection accuracy in IoT environments [42]. Block chain and Post Quantum Cryptography are integrated to secure FL against future attacks[43].Byzantine Robust FL addresses modelling of Poisoning attacks, Byzantine adversaries and Quantum Safe Aggregation[44]

4.Quantum Safe Encryption

A combination of lattice based cryptography, block chain and AI is proposed for quantum resistant autonomous systems[40]The NIST standard ML- KEM 512 post – quantum encryption in IoT systems is implemented[41]

5.Trust Management in Decentralized Networks

Block chain based trust management and decentralized learning are combined to implement Federated learning for IoT [45]. Decentralized identity management and secure communication in IoT are implemented [46].

6.Cyber Resilience Frameworks for IoT

A first integrated framework combining Intrusion Detection, Federated Learning, Block chain Audit and Self-Healing is proposed [46]. Resilient architectures for distributed IoT systems, integrating ML, block chain and decentralized security is discussed.[47]Real – Time privacy preserving cyber resilience using Federated Learning is proposed[42].

Thus the objectives of this work are,

[i]To model an autonomous IoT network architecture and cyber-attack scenario.
[ii]To design an AI – based anomaly and intrusion detection mechanism.
[iii]To develop self – adaptive response and recovery strategies using reinforcement learning.

[iv] To integrate resilience metrics such as survivability, recovery time and service continuity.
[v]To validate the proposed framework using NetSim.

Discussions

Review and Analysis of Results

- Most studies show high accuracy (90–98%) using AI/ML models for intrusion detection.
- Deep Learning (CNN, LSTM) outperforms traditional security methods.
- Blockchain integration improves trust and data integrity in autonomous networks.
- Lightweight cryptography reduces energy consumption in IoT devices.
- Real-time detection is partially achieved, but still challenging in large-scale networks.

Strengths identified

- High detection accuracy using AI models.
- Ability to detect zero-day and unknown attacks.
- Automation reduces human intervention.
- Scalable solutions using cloud and edge computing.
- Integration with SDN/NFV enhances network flexibility.

Conclusion

Thus the scientific impact of this work is that it advances knowledge in autonomous cyber-resilient IoT systems, merging AI, networking, and security. This research work is applicable to smart cities, autonomous vehicles, industrial IoT, and critical infrastructure, where resilient operation is mission-critical. This work is of strategic importance since it addresses global priorities in cybersecurity for IoT.

References

[1] Vermesan, O., Bröring, A., Tragos, E., Serrano, M., Bacciu, D., Chessa, S., et al. (2022). "Internet of robotic things–converging sensing/actuating, hyperconnectivity, artificial intelligence and IoT platforms," in Cognitive hyperconnected digital transformation (Aalborg, Denmark: River Publishers), 97–155.

[2] Cardoso, P., Moura, J., and Marinheiro, R. N. (2023). Elastic provisioning of network and computing resources at the edge for IoT services. Sensors 23 (5), 2762. doi:10.3390/ s23052762

[3] Mondal, M. K., Mandal, R., and Biswas, U. (2024). Big IoT data analytics in fog computing. Fog Comput. Intelligent Cloud IoT Syst., 279–307. doi:10.1002/ 9781394175345.ch12

[4] Arulmurugan, L., Thakur, S., Dayana, R., Thenappan, S., Nagesh, B., and Sri, R.K. (2024). "Advancing security: exploring AI-driven data encryption solutions for wireless sensor networks," In 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). Piscataway, NJ, USA: IEEE. 1–6.

[5] Alam, T. (2024). Data privacy and security in autonomous connected vehicles in smart city environment. Big Data Cognitive Comput. 8 (9), 95. doi:10.3390/bdcc8090095.

[6] Tejaswini Goli, Yoohwan Kim, " A Survey on Securing IoT Ecosystems and Adaptive Network Vision," International Journal of Networked and Distributed Computing, Vol 9 (2-3),April – July 2021, pp 75 – 85.

[7]Marwa Salayma," Risk and Threat Mitigation Techniques in the Internet of Things(IoT) Environment a survey", Frontiers in the Internet of Things, 2024, doi:10.3389/friot.2023.

[8] Commey, D., Mai, B., Hounsinou, S. G., and Crosby, G. V. (2024). Securing blockchain-based IoT systems: a review. IEEE Access 12, 98856–98881. doi:10.1109/ access.2024.3428490

[9] Tariq, U., Ahmed, I., Bashir, A. K., and Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors 23 (8), 4117. doi:10.3390/s23084117

[10] Sadhu, P. K., Yanambaka, V. P., and Abdelgawad, A. (2022). Internet of things: security and solutions survey. Sensors 22 (19), 7433. doi:10.3390/s22197433

[11] Guesmi, A., Hanif, M. A., Ouni, B., and Shafique, M. (2023). Physical adversarial attacks for camera-based smart systems: current trends, categorization, applications, research challenges, and future outlook. IEEE Access 11, 109617–109668. doi:10.1109/ access.2023.3321118

[12] Taye, M. M. (2023). Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. Computers 12 (5), 91. doi:10.3390/computers12050091

[13] Allioui, H., and Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: a comprehensive survey. Sensors 23 (19), 8015. doi:10. 3390/s23198015

[14] Usmani, U. A., Happonen, A., and Watada, J. (2022). "A review of unsupervised machine learning frameworks for anomaly detection in industrial applications," in Science and information conference (Cham: Springer International Publishing), 158–189.

[15] Tayyab, M., Marjani, M., Jhanjhi, N. Z., Hashem, I. A. T., Usmani, R. S. A., and Qamar, F. (2023). A comprehensive review on deep learning algorithms: security and privacy issues. Comput. Secur. 131, 103297. doi:10.1016/j.cose.2023.103297

[16] Chang, Y., Zhang, K., Gong, J., and Qian, H. (2023). Privacy-preserving federated learning via functional encryption, revisited. IEEE Trans. Inf. Forensics Secur. 18, 1855–1869. doi:10.1109/tifs.2023.3255171

[17] Reddy, D. K. K., Nayak, J., Behera, H. S., Shanmuganathan, V., Viriyasitavat, W., and Dhiman, G. (2024). A systematic literature review on swarm intelligence based intrusion detection system: past, present and future. Archives Comput. Methods Eng. 31 (5), 2717–2784. doi:10.1007/s11831-023-10059-2

[18] Muppalaneni, R., Inaganti, A. C., and Ravichandran, N. (2024). AI-driven threat intelligence: enhancing cyber defense with machine learning. J. Comput. Innovations Appl. 2 (1), 1–11.

[19] Alhakami, W. (2024). Evaluating modern intrusion detection methods in the face of gen V multi-vector attacks with fuzzy AHP-TOPSIS. PLos One 19 (5), e0302559. doi:10. 1371/journal.pone.0302559

[20] Singh, T., Kumar, S., Singh, S. K., Gupta, B. B., Wu, J., and Castiglione, A. (2025). "Enhancing autonomous system security with AI and secure computation technologies," in AI developments for industrial robotics and intelligent drones (Hershey, PA, USA: IGI Global Scientific Publishing), 159–186

[21] Albulayhi, K. (2022). An adaptive deep-ensemble anomaly-based intrusion detection system-of-systems for the internet-of-things. (Doctoral dissertation, Moscow, ID, USA: University of Idaho).

[22] Kanzouai, C., Bouarourou, S., Zannou, A., Boulaalam, A., and Nfaoui, E. H. (2025). Enhancing IoT scalability and interoperability through ontology alignment and FedProx. Future Internet 17 (4), 140. doi:10.3390/fi17040140

[23] Kaliyaperumal, P., Periyasamy, S., Thirumalaisamy, M., Balusamy, B., and Benedetto,F. (2024). A novel hybrid unsupervised learning approach for enhanced cybersecurity in the IoT. Future Internet 16 (7), 253. doi:10.3390/fi16070253

[24] Sha, Z., Layton, A., Heydari, B., and Van Bossuyt, D. L. (2025). Special issue: networks and graphs for engineering systems and design. J. Comput. Inf. Sci. Eng. 25, 060301. doi:10.1115/1.4068457

[25] Almaleh, A., Almushabb, R., and Ogran, R. (2023). Malware API calls detection using hybrid logistic regression and RNN model. Appl. Sci. 13 (9), 5439. doi:10.3390/ app13095439

[26] Hossain, S., Senouci, S. M., Brik, B., and Boualouache, A. (2025). A privacy-preserving self-supervised Learning-based intrusion detection system for 5G-V2X networks. Ad Hoc Netw. 166, 103674. doi:10.1016/j.adhoc.2024.103674

[27] Van Hoang, N. (2023). Human expertise and machine learning in collaborative intelligence frameworks for robust cybersecurity solutions. J. Appl. Cybersecurity Anal. Intell. Decision-Making Syst. 13 (12), 1–12. Available online at: http://sciencespress. com/index.php/JACAIDMS/article/view/2023-12-04

[28] Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., et al. (2024). Enhancing security of internet of robotic things: a review of recent trends, practices, and recommendations with encryption and blockchain techniques. Internet Things 28, 101357. doi:10.1016/j.iot.2024.101357.

[29] Pothumarti, R., Jain, K., and Krishnan, P. (2021). A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. J. Ambient Intell. Humaniz. Comput., 1–19. doi:10.1007/s12652-020-02857-4

[30] Mahto, M. K. (2025). “Explainable artificial intelligence: fundamentals, approaches, challenges, XAI evaluation, and validation,” in Explainable artificial intelligence for autonomous vehicles Boca Raton, FL, United States: CRC Press (Taylor & Francis Group), 25–49.

[31] D. Kaushik et al., “Synergizing blockchain and AI to fortify IoT security: A comprehensive review,” Artif. Intell. Rev., 2026.

[32] S. S. Sefati et al., “A comprehensive survey of cybersecurity techniques based on QoS in IoT,” Cluster Comput., 2025.

[33] A. Heidari et al., “Artificial intelligence-driven privacy preservation in the internet of vehicles,” J. Big Data, 2026.

[34] A. Aparcana-Tasayco et al., “Anomaly detection in IoT security: Towards quantum machine learning,” EPJ Quantum Technol., 2025.

[35] S. A. Hakeem and H. Kim, “Advancing intrusion detection in V2X networks,” IEEE Trans. ITS, 2025.

[36] H. Zhang et al., “Survey of federated learning in intrusion detection,” Comput. Commun., 2024.

[37] V. T. Nguyen and R. Beuran, “FedMSE: Federated learning for IoT intrusion detection,” arXiv, 2024.

[38] S. Sun et al., “FedMADE: Robust federated learning for IDS in IoT,” arXiv, 2024.

[39] A. Alshamrani et al., “An AI-driven framework for integrated security and privacy in IoT,” Computers, 2025.

[40] R. Alluhaibi, “Quantum resistant blockchain and deep learning revolutionize secure communications for autonomous vehicles,” Scientific Reports, vol. 16, 2025.

[41] U. H. Khan et al., “TrustEdge: A quantum-safe, self-healing framework for federated TinyML in IoMT,” Internet of Things, 2025.

[42] M. Rahmati, “Federated learning-driven cybersecurity framework for IoT networks,” arXiv, 2025.

[43] D. Commey and G. Crosby, “PQS-BFL: A post-quantum secure blockchain-based federated learning framework,” arXiv, 2025.

[44] M. Rahmati and N. Rahmati, “Byzantine-robust federated learning with post-quantum secure aggregation,” arXiv, 2026.

[45] Settu, Munusamy & R, Jothi. (2025). Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management. Scientific Reports. 15. 10.1038/s41598-025-12225-x.

[46] Sathwik Narkedimilli, Pravisha P., Amballa Venkata Sriram, Satvik Raghav, and Parmitha Vangapandu. 2025. FL-DABE-BC: A Privacy-Enhanced Decentralized Authentication and Secure Communication Framework for FL in IoT-Enabled Smart Cities. In Proceedings of the 2nd International Workshop on Foundation Models for Cyber-Physical Systems & Internet of Things (FMSys). Association for Computing Machinery, New York, NY, USA, 37–42. https://doi.org/10.1145/3722565.3727194

[47] “Cybersecurity in smart microgrids using blockchain, federated learning and quantum-safe approaches,” Applied Energy, 2025.