

AI-Driven Cybersecurity in IoT-Based Systems

Wenbing Zhao ^{1,*}  and Pan Wang ² ¹ Department of Electrical and Computer Engineering, Cleveland State University, Cleveland, OH 44115, USA² School of Modern Posts, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; wangpan@njupt.edu.cn

* Correspondence: wenbing@ieee.org

1. Introduction

With the rapid development of the Internet of Things (IoT) [1,2], including Industrial IoT and Home IoT, sensors and IoT devices are starting to play an increasingly important role in various fields such as smart grids, power plants, manufacturing, and supply chains. Such sensors and IoT-based systems could be vulnerable to various cyberattacks [3,4]. As an innovative data-driven paradigm, artificial intelligence (AI) has revolutionized several classical areas such as image, video, speech, and text processing [5–7]. However, when applying to mitigating cyberattacks, the inherent limitations of AI, such as data dependence, weak generalization, and lack of explainability, have obstructed the development of AI-driven cybersecurity [8,9]. Furthermore, sensors and IoT devices have imposed additional obstacles, including low power, heterogeneity, and weak computing power, which makes applying AI for cybersecurity even more challenging [10]. The aim of this Special Issue is to attract studies that have applied AI and other cutting-edge technologies to enable and empower cybersecurity in sensors and IoT-based systems.

2. Contributions

This Special Issue accepted five research articles and one comprehensive review. These studies focused on various issues related to cybersecurity in IoT-based systems, ranging from enhancing the interpretability of feature selection and intrusion detection in IoT-based systems (1 contribution), detecting and mitigating attacks in the physical layer (2 contributions), and blockchain-facilitated cybersecurity in IoT-based systems (3 contributions).

2.1. Interpretable AI in Intrusion Detection

In contribution 1, Chen et al. performed feature selection based on the ranking of features using the SHAP method [11] with a deep learning model. SHAP is an explainability method based on Shapley values from cooperative game theory. SHAP treats prediction as a “payout” in a game where features are “players.” More specifically, SHAP calculates each feature’s contribution by averaging its marginal impact across all possible feature subsets. SHAP follows several key principles when calculating the value for each feature. First, it distributes the prediction difference fairly among features (i.e., fair attribution). Second, the sum of all feature contributions equals the model output, which ensures additive feature contributions. Third, if a model changes so a feature contributes more, its SHAP value will not decrease to ensure consistency.

In one dataset used for the study (CICIDS2017 [12]), the top 10, 15, and 20 features were selected from the 78 total features based on sorted SHAP values. For classification, the authors experimented with two different models, random forest (RF) and convolutional neural network (CNN). The results showed that the features selected by SHAP



Received: 16 November 2025

Accepted: 21 November 2025

Published: 28 November 2025

Citation: Zhao, W.; Wang, P. AI-Driven Cybersecurity in IoT-Based Systems. *Sensors* **2025**, *25*, 7254. <https://doi.org/10.3390/s25237254>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

outperformed traditional feature selection methods when using the top 20 and 15 features. Furthermore, the accuracy actually improved when using the top 20 features compared with using the full 78 features. On the other hand, the results were mixed when using another dataset (NSL-KDD [13]). While the top 20 and 15 features selected via SHAP tied or outperformed traditional feature selection methods for CNN and RF, the accuracy was reduced compared with when using the full 38 features for CNN. For RF, using top 20 features obtained via SHAP outperformed using the full 38 features. However, the RF performance was noticeably worse than that of CNN.

2.2. Physical Layer Cybersecurity

In contribution 2, Qi, Liu, and Ye introduced an attention-enhanced defensive distillation network (AEDDN) to improve robustness and accuracy in vehicle-to-everything (V2X) millimeter-wave communication in the presence of adversarial attacks. The AEDDN model combines the transformer algorithm with defensive distillation. The goal is to leverage the transformer's attention mechanism to focus on critical channel features and adapt to complex conditions. Defensive distillation is used to smooth the decision boundaries, which reduces the sensitivity to small perturbations.

In contribution 3, Senol et al. proposed a new method to identify tampered radio frequency transmissions by employing a suite of anomaly detection algorithms, including local outlier factor, isolation forest, variational autoencoder, traditional autoencoder, and principal component analysis. The context of the study is a LoRa-based IoT network [14]. LoRa refers to a long-range, low-power, and low-bandwidth wireless communication system. A key insight of the study is the employment of image-based tampered frequency techniques for securing LoRa transmissions.

2.3. Blockchain-Facilitated Cybersecurity

In contribution 4, Wang et al. proposed an extended robot operating system to protect the privacy of sensor data. The system utilizes blockchain [15] for data immutability protection of the data content identifiers, InterPlanetary File System (IPFS) [16] for data storage, as well as attribute-based hybrid encryption for fine-grained access control.

In contribution 5, Gao et al. also focused on privacy protection of the data using blockchain with an improved scheme for the distributed Oracle [17] data aggregation mechanism based on the Paillier encryption algorithm. In particular, the authors proposed an algorithm called PICA (Paillier-based InChain Aggregation), where the data are encrypted using the Paillier algorithm [18] and aggregated on the Chainlink blockchain [19]. Furthermore, random numbers are employed to mitigate the problem of dishonest Oracle machines.

In contribution 6, Zhao et al. provided a comprehensive review on blockchain-facilitated cybersecurity solutions for IoT devices in space-air-ground integrated networks (SAGIN) [20,21]. First, the authors identified the objectives and the context of the blockchain-based solutions for SAGIN. Second, the authors investigated how blockchain technology has been used to accomplish the objectives. Deep technical details on how blockchain has been used in this specific field were presented. Third, the authors provided a critique on the technical correctness of the blockchain-based solutions and pointed out serious technical issues in the proposed solutions. The most pervasive misconception is that higher-level trustworthiness can be achieved by using any form of blockchain, which is wrong, as elaborated in [22]. Finally, the authors proposed a guideline on when the blockchain technology can be useful for IoT and SAGIN and what types of blockchain may be useful to enhance the security of ubiquitous IoT in SAGIN.

Funding: This work was supported in part by the US NSF grant 2215388.

Conflicts of Interest: The authors declare no conflicts of interest.

List of Contributions

1. Chen, X.; Liu, M.; Wang, Z.; Wang, Y. Explainable Deep Learning-Based Feature Selection and Intrusion Detection Method on the Internet of Things. *Sensors* **2024**, *24*, 5223. <https://doi.org/10.3390/s24165223>.
2. Qi, X.; Liu, Y.; Ye, Y. Attention-Enhanced Defensive Distillation Network for Channel Estimation in V2X mm-Wave Secure Communication. *Sensors* **2024**, *24*, 6464. <https://doi.org/10.3390/s24196464>.
3. Senol, N.S.; Rasheed, A.; Baza, M.; Alsabaan, M. Identifying Tampered Radio-Frequency Transmissions in LoRa Networks Using Machine Learning. *Sensors* **2024**, *24*, 6611. <https://doi.org/10.3390/s24206611>.
4. Wang, T.; Chen, K.; Zheng, Z.; Guo, J.; Zhao, X.; Zhang, S. PrivShieldROS: An Extended Robot Operating System Integrating Ethereum and Interplanetary File System for Enhanced Sensor Data Privacy. *Sensors* **2024**, *24*, 3241. <https://doi.org/10.3390/s24103241>.
5. Gao, R.; Xue, Y.; Wang, W.; Lu, Y.; Gui, G.; Xu, S. Improved Scheme for Data Aggregation of Distributed Oracle for Intelligent Internet of Things. *Sensors* **2024**, *24*, 5625. <https://doi.org/10.3390/s24175625>.
6. Zhao, W.; Yang, S.; Luo, X. Blockchain-Facilitated Cybersecurity for Ubiquitous Internet of Things with Space–Air–Ground Integrated Networks: A Survey. *Sensors* **2025**, *25*, 383. <https://doi.org/10.3390/s25020383>.

References

1. Alamri, M.; Jhanjhi, N.; Humayun, M. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur* **2019**, *19*, 244–258.
2. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *9*, 359–383. [\[CrossRef\]](#)
3. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [\[CrossRef\]](#)
4. Lu, Y.; Da Xu, L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115. [\[CrossRef\]](#)
5. Baccour, E.; Mhaisen, N.; Abdellatif, A.A.; Erbad, A.; Mohamed, A.; Hamdi, M.; Guizani, M. Pervasive AI for IoT applications: A survey on resource-efficient distributed artificial intelligence. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2366–2418. [\[CrossRef\]](#)
6. Bourechak, A.; Zedadra, O.; Kouahla, M.N.; Guerrieri, A.; Seridi, H.; Fortino, G. At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. *Sensors* **2023**, *23*, 1639. [\[CrossRef\]](#) [\[PubMed\]](#)
7. Menon, U.V.; Kumaravelu, V.B.; Kumar, C.V.; Rammohan, A.; Chinnadurai, S.; Venkatesan, R.; Hai, H.; Selvaprabhu, P. AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. *IEEE Access* **2025**, *13*, 50296–50339.
8. Adadi, A.; Berrada, M. Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access* **2018**, *6*, 52138–52160. [\[CrossRef\]](#)
9. Chamola, V.; Hassija, V.; Sulthana, A.R.; Ghosh, D.; Dhingra, D.; Sikdar, B. A review of trustworthy and explainable artificial intelligence (XAI). *IEEE Access* **2023**, *11*, 78994–79015. [\[CrossRef\]](#)
10. Sarker, I.H.; Furhad, M.H.; Nowrozy, R. Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Comput. Sci.* **2021**, *2*, 173. [\[CrossRef\]](#)
11. Lundberg, S.M.; Lee, S.I. A Unified Approach to Interpreting Model Predictions. In Proceedings of the Advances in Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; Guyon, I., Luxburg, U.V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., Garnett, R., Eds.; Curran Associates, Inc.: Red Hook, NY, USA, 2017; Volume 30.
12. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Madeira, Portugal, 22–24 January 2018; pp. 108–116.
13. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.

14. Augustin, A.; Yi, J.; Clausen, T.; Townsley, W.M. A study of LoRa: Long range & low power networks for the internet of things. *Sensors* **2016**, *16*, 1466. [[CrossRef](#)] [[PubMed](#)]
15. Zhao, W. *From Traditional Fault Tolerance to Blockchain*; John Wiley & Sons: Hoboken, NJ, USA, 2021.
16. Muralidharan, S.; Ko, H. An InterPlanetary file system (IPFS) based IoT framework. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–2.
17. Caldarelli, G. Understanding the blockchain oracle problem: A call for action. *Information* **2020**, *11*, 509. [[CrossRef](#)]
18. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.
19. Breidenbach, L.; Cachin, C.; Chan, B.; Coventry, A.; Ellis, S.; Juels, A.; Koushanfar, F.; Miller, A.; Magauran, B.; Moroz, D.; et al. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. 2021. Available online: <https://chainlinklabs.com/> (accessed on 15 November 2025).
20. Liu, J.; Shi, Y.; Fadlullah, Z.M.; Kato, N. Space-air-ground integrated network: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2714–2741. [[CrossRef](#)]
21. Guo, F.; Yu, F.R.; Zhang, H.; Li, X.; Ji, H.; Leung, V.C. Enabling massive IoT toward 6G: A comprehensive survey. *IEEE Internet Things J.* **2021**, *8*, 11891–11915. [[CrossRef](#)]
22. Zhao, W. On blockchain: Design principle, building blocks, core innovations, and misconceptions. *IEEE Syst. Man Cybern. Mag.* **2022**, *8*, 6–14. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.