SecureCyber: An SDN-Enabled SIEM for Enhanced Cybersecurity in the Industrial Internet of Things

Panagiotis Radoglou-Grammatikis
Department of Electrical & Computer Engineering, University of Western Macedonia, Kozani 50100, Greece
pradoglou@uowm.gr

Abstract

The proliferation of smart technologies has undeniably brought forth numerous advantages. However, it has also introduced critical security issues and vulnerabilities that need to be addressed. In response, the development of appropriate and continuously adaptable countermeasures is essential to ensure the uninterrupted operation of critical environments. This paper presents an innovative approach through the introduction of an Software-Defined Networking (SDN)-enabled Security Information and Event Management (SIEM) system. The proposed SIEM solution effectively combines the power of Artificial Intelligence (AI) and SDN to protect Industrial Internet of Things (IIoT) applications. Leveraging AI capabilities, the SDN-enabled SIEM is capable of detecting a wide range of cyberattacks and anomalies that pose potential threats to IIoT environments. On the other hand, SDN plays a crucial role in mitigating identified risks and ensuring the security of IIoT applications. In particular, AI-driven insights and analysis guide the SDN-C in selecting appropriate mitigation actions to neutralize detected threats effectively. The experimental results demonstrate the efficiency of the proposed solution.

Keywords: Artificial Intelligence, Cybersecurity, Industrial Internet of Things, Security Information and Event Management, Software-Defined Networking

1. Introduction

The rise of smart technologies provides several benefits in the Industrial Internet of Things (IIoT), such as increased efficiency, cost savings, flexibility and adaptability and finally, significant environmental impact. However, this revolution raises severe cybersecurity issues that can result in catastrophic effects [1]. Widely-known cybersecurity incidents with a severe impact include WannaCry (2017) and NotPetya (2017) ransomware [2], SolarWinds supply chain attack (2020) and Colonial pipeline ransomware attack (2021) [3]. Therefore, it is evident that the development of appropriate and continuous countermeasures is necessary. In this paper, a Security Information and Event Management (SIEM) [5] system is presented, taking full advantage of Artificial Intelligence (AI) and Software-Defined Networking (SDN) [4] technologies. On the one hand, AI is used to detect potential cyberattacks and anomalies against industrial communication protocols and environments, while SDN is used to mitigate them. The following sections describe the architecture of the proposed SDN-enabled SIEM and the corresponding evaluation results. Finally, section 4 concludes this paper.

2. Architecture of the proposed SDN-enabled SIEM

Based on the SDN paradigm [6], the proposed SDN-enabled SIEM's architectural design is depicted in Figure 1. The main objective is to leverage SDN, honeypots [8, 9], and AI to effectively detect, standardize, correlate, and mitigate cybersecurity incidents in IIoT/SG environments. To achieve this, the proposed SIEM incorporates three AI-powered Intrusion Detection and Prevention Systems (IDPS) [7] that generate security events. These events are then processed by the Normalisation, Correlation, and Mitigation Engine (NCME), which normalises and correlates them, resulting in the creation of security alerts. Furthermore, the NCME provides guidance to the SDN Controller (SDN-C) and employs sophisticated mechanisms for deploying honeypots. These measures serve to mitigate malicious network flows and enhance the resilience of the underlying IIoT infrastructure.

The first component, known as Network Flow-based Intrusion Detection and Prevention System (NF-IDPS), is designed to identify cyberattacks and anomalies targeting application-layer industrial communication protocols. These protocols include Modbus/Transmission Control Protocol (TCP), Distributed Network Protocol 3 (DNP3), International Electrotechnical Commission (IEC) 60870-5-104, IEC 61850 (Generic Object-Oriented Substation Event (GOOSE)), Hypertext Transfer Protocol (HTTP), and Secure Shell (SSH). For each protocol, specific Machine Learning (ML) and Deep Learning (DL) models were implemented for intrusion detection and anomaly detection. These models were trained using both custom-

developed and publicly available datasets. The second component, referred to as Host-based Intrusion Detection and Prevention System (H-IDPS), is responsible for detecting potential anomalies by analyzing operational electricity data. Finally, the Visual Intrusion Detection and Prevention System (V-IDPS) focuses on the detection of malicious Modbus/TCP network flows. It leverages binary visual representations and an active ResNet50 Convolutional Neural Network (CNN) [10] model to effectively identify and mitigate such threats.

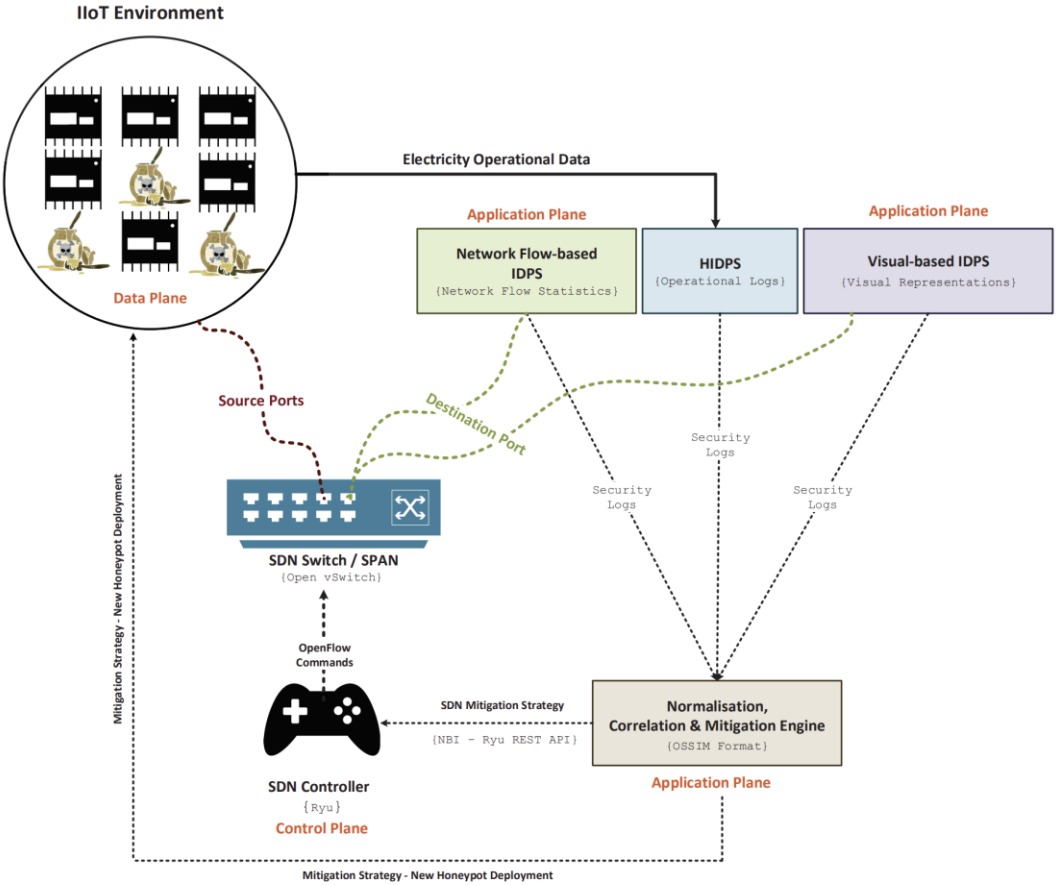


Figure 2: SDN-enabled SIEM Architecture

The next component, NCME is responsible for normalizing and correlating the security events generated by the previous IDPS components. The security events are standardized using the AlienVault Open Source SIEM (OSSIM) format, and security rules are applied to establish correlations among the events. Additionally, NCME incorporates a mechanism based on Reinforcement Learning (RL) to provide guidance to the SDN-C on dropping malicious network flows effectively. In particular, the Thompson Sampling (TS) method is used.

3. Evaluation Analysis

The following figures show the efficiency of the proposed SDN-enabled SIEM in terms of detecting and mitigating the corresponding security events. First, in Figure 2, the detection effectiveness of NF-IDPS is depicted, demonstrating the performance of the ML/DL models in detecting particular cyberattacks against a variety of industrial communication protocols. For this purpose, four metrics are used, namely Accuracy (ACC), True Positive Rate (TPR), False Positive Rate (FPR), and F1 score. Next, Figure 3 shows the detection efficiency of H-IDPS. In this case, the aforementioned metrics are used to evaluate the performance of ML/DL models for the detection of potential operational anomalies in four industrial environments: (a) hydropower plant, (b) substation, (c) power plant and (d) smart home. Next, Figure 4 illustrates how the accuracy of the active ResNet50 CNN is increased based on the queries of the active learning procedure [10]. In this case, the pool sampling method and uncertainty strategy are used. Finally, Figure 5 shows how the mitigation accuracy of the proposed TS method is improved based on the number of security events.

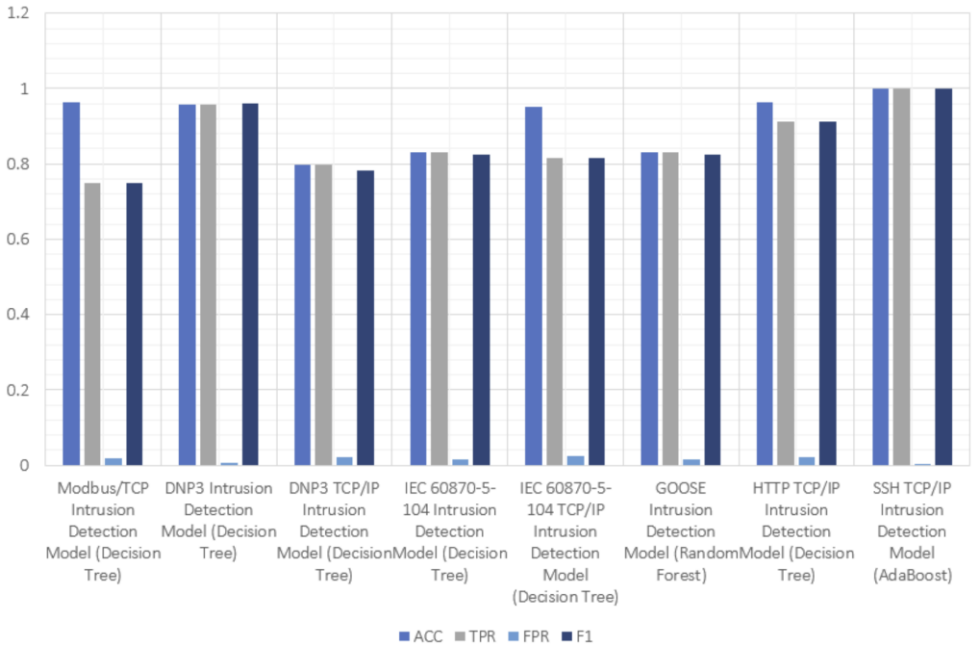


Figure 3: Evaluation Results of NF-IDPS Detection Models

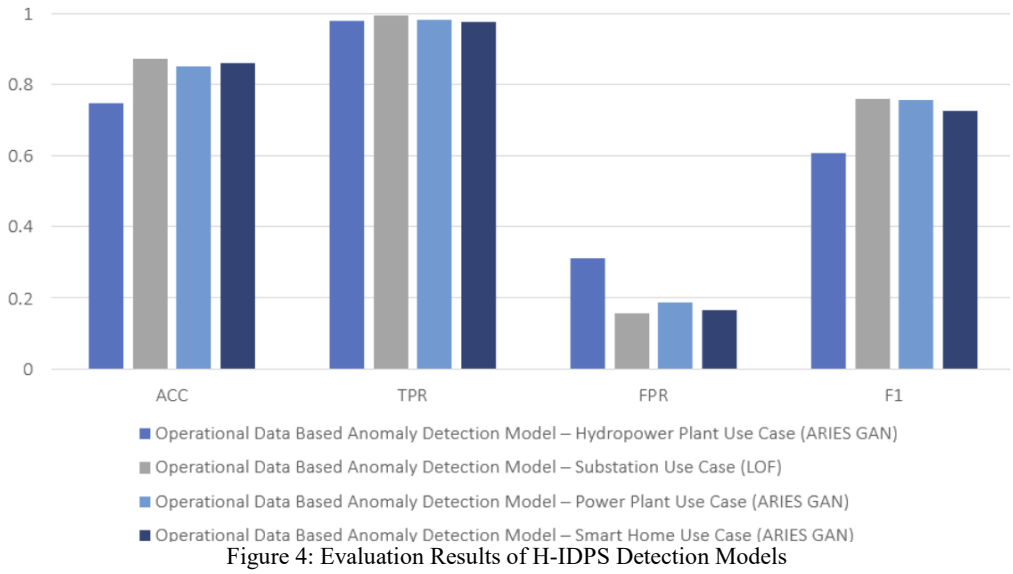


Figure 4: Evaluation Results of H-IDPS Detection Models

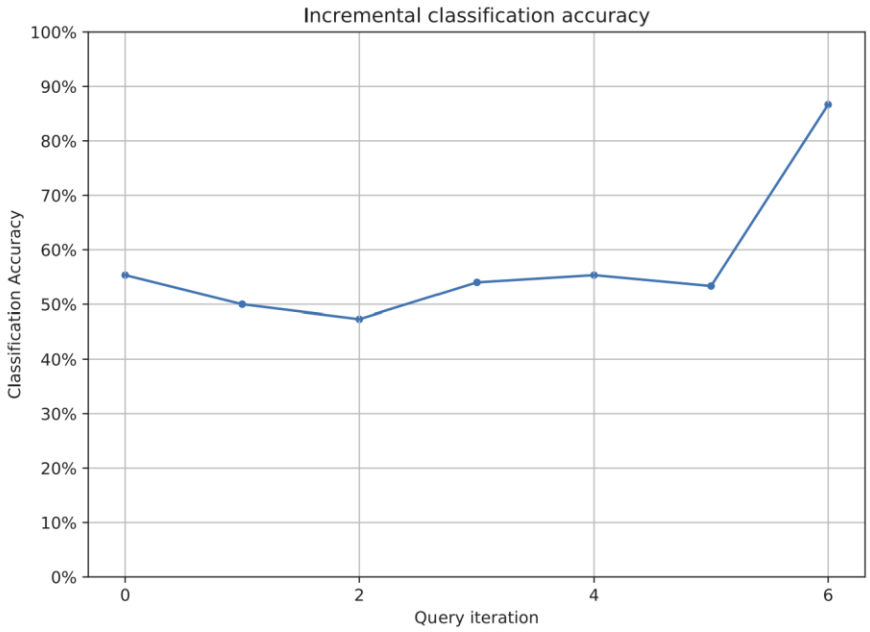


Figure 5: Accuracy Improvement in Re-Training Phases of Active ResNet50-based CNN

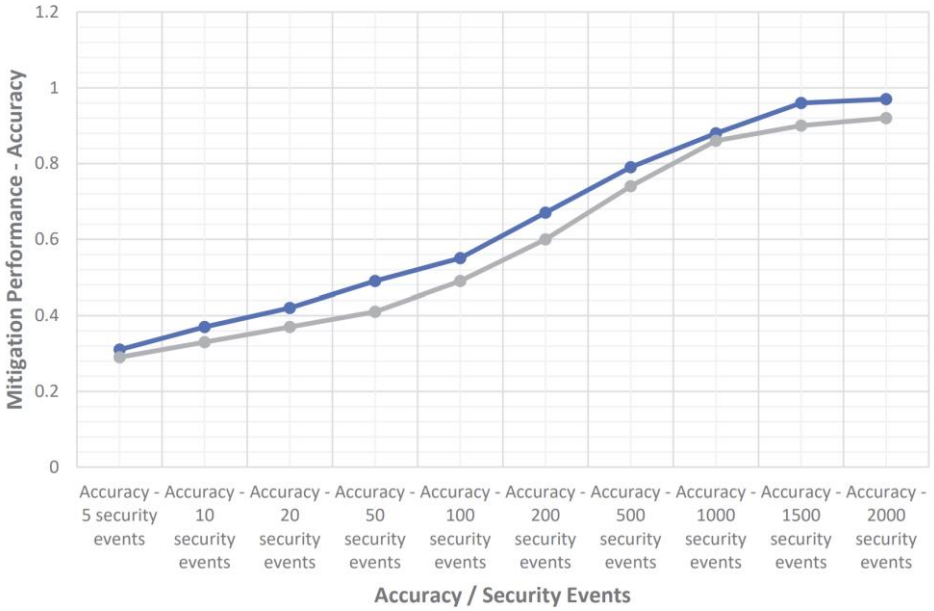


Figure 6: TS Mitigation Accuracy according to the Number of the Security Events

4. Conclusion

It is evident that the revolution of smart technologies raises critical security issues and situations, despite the wide range of advantages they provide. Consequently, the presence of appropriate and continuous adaptable countermeasures is necessary to ensure the normal operation of critical environments. In this paper, an SDN-enabled SIEM is introduced. The proposed SIEM successfully combines AI and SDN in order to protect IIoT applications. Specifically, AI is leveraged to detect a variety of cyberattacks and anomalies and guide the SDN-C to choose the appropriate mitigation actions. The experimental results demonstrate the efficiency of the proposed SDN-enabled SIEM.

Acknowledgement

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936 (ELECTRON).

References

[1] Alshamrani, S. Myneni, A. Chowdhary and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851-1877, Secondquarter 2019.

[2] S. -C. Hsiao and D. -Y. Kao, "The static analysis of WannaCry ransomware," 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 153-158.

[3] R. A. Lika, D. Murugiah, S. N. Brohi and D. Ramasamy, "NotPetya: Cyber Attack Prevention through Awareness via Gamification," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1-6.

[4] A. Liatifis, C. Dalamagkas, P. Radoglou-Grammatikis, T. Lagkas, E. Markakis, V. Mladenov and P. Sarigiannidis, "Fault-Tolerant SDN Solution for Cybersecurity Applications", 17th International Conference on Availability, Reliability and Security, 2022.

[5] S. Bhatt, P. K. Manadhata and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," in IEEE Security & Privacy, vol. 12, no. 5, pp. 35-41, Sept.-Oct. 2014.

[6] F. Bannour, S. Souihi and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 333-354, Firstquarter 2018.

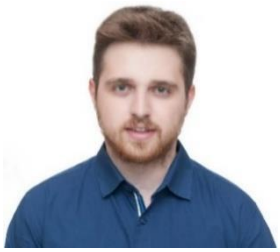
[7] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems", IEEE Access, vol. 7, pp. 46595-46620, 2019.

[8] P. Radoglou-Grammatikis, P. Sarigiannidis, P. Diamantoulakis, T. Lagkas, T. Saoulidis, E. Fountoukidis and G. Karagiannidis, "Strategic Honeypot Deployment in Ultra-Dense Beyond 5G Networks: A Reinforcement Learning Approach", IEEE Transactions on Emerging Topics in Computing, 2022.

[9] E. Grigoriou, A. Liatifis, P. Radoglou-Grammatikis, T. Lagkas, I. Moscholios, E. Markakis and P. Sarigiannidis, "Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots", IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 345-350.

[10] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis and A. Sarigiannidis, "A Self-Learning Approach for Detecting Intrusions in Healthcare Systems", ICC 2021 – IEEE International Conference on Communications, 2021, pp. 1-6.

Author Bio-data



Panagiotis Radoglou-Grammatikis received the Diploma degree (MEng, 5 years) and PhD from the Dept. of Informatics and Telecommunications Eng. (now Dept. of Electrical and Computer Eng.), Faculty of Eng., University of Western Macedonia, Greece, in 2016 and 2023, respectively. His main research interests are in the area of cybersecurity and mainly focus on cyber-AI, intrusion detection and security games. He has published more than 30 research papers in international scientific journals, conferences and book chapters, including IEEE Transactions on Industrial Informatics, IEEE Access, Computer Networks (Elsevier Publishing) and Internet of Things (Elsevier Publishing). Moreover, he has received four Best Paper Awards in IEEE CAMAD 2019, IEEE CSR 2021, WSCE 2022 and SEEDA CECNSM 2022, respectively. Recently, he was included in Stanford University's list (shared by Elsevier) of the Top 2% of Scientists in the World for 2022. He has served as a reviewer for several scientific journals and possesses working experience as a security engineer and software developer. Also, he participates in the Topical Advisory Panel of Electronics (MDPI Publishing). He is working as an R&D director at K3Y Ltd, coordinating the technical activities and strategy of K3Y in various R&D projects, including H2020 SPIDER, H2020 SANCUS, H2020 5G-INDUCE, H2020 TREEADS, H2020-MSCA Swiftv2x, TRUSTEE, INCODE, ACROSS, UP2030 and JAUNTY. He is also a research associate at the ITHACA Lab of the University of Western Macedonia, participating in several national and European-funded research projects, such as H2020 SPEAR, H2020 SDN-microSENSE, H2020 TERMINET, H2020 EVIDENT, H2020 ELECTRON, AI4CYBER and DYNABIC. Moreover, he is co-founder of MetaMind Innovations P.C., the first spin-off of the University of Western Macedonia. Finally, he is a member of IEEE, ACM and the Technical Chamber of Greece.

MMTC OFFICERS (Term 2022 — 2024)