MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
http://www.comsoc.org/~mmc

MMTC Communications - Frontiers

Vol. 18, No. 2, Mar 2023

CONTENTS

SPECIAL ISSUE ON Artificial Intelligence, Telecommunication, and Cybersecurity: A Synergistic Approach for the Revolution of the Information Systems

Guest Editors: Panagiotis Sarigiannidis[1], Dimitrios Pliatsios[1], Thomas Lagkas[2], Vasileios Argyriou[3]
[1]Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece
[2]Department of Computer Science, International Hellenic University, 65404 Kavala Campus, Greece
[3]Department of Networks and Digital Media, School of Computer Science and Mathematics, SEC, Kingston University, London KT1 2EE, UK
psarigiannidis@uowm.gr, dpliatsios@uowm.gr, tlagkas@cs.ihu.gr, vasileios.argyriou@kingston.ac.uk

The rapid evolution of the 5G networks and the Internet of Things (IoT) provide a wide range of beneficial services, such as increased efficiency, remote monitoring and control and predictive maintenance. Apart from the technological leap of communication networks, Artificial Intelligence (AI) also plays a severe role in modern society. In particular, the AI mechanisms can optimize any aspect of the computing systems, providing improved decision-making, predictive analytics and personalization mechanisms. The integration of AI, IoT, and 5G and Beyond 5G (B5G) networks can lead to the development of powerful ecosystems that will allow the collection and analysis of a vast amount of data in real-time, thus revolutionizing several aspects of daily life. As in the case of any computing system, 5G/B5G networks and IoT are characterized by cybersecurity issues due to insecure communication protocols and the necessary presence of legacy systems. Motivated by these remarks, this Special Issue is focused on a wide range of research problems related to AI, telecommunication networks, and cybersecurity.

The first paper is focused on Advanced Persistent Threats (APTs) and aims to provide a state-of-art overview regarding the detection and identification of APTs, and the respective mitigation strategies. Specifically, the authors review nine recent research and identify the main architectural components, tools, methodologies, and technologies that are utilized.

The second paper introduces HYPER, which is a healthcare cybercrime protection framework that incorporates defense mechanisms to detect medical-specific attacks and mitigate cyberthreats effectively. In more detail, the authors present a high-level architecture of the proposed framework and explain the technical details and operation of each architectural component.

The third paper presents SecureCyber, which constitutes a Security Information and Event Management (SIEM) that is tailored to the security requirements of Industrial IoT environments. Specifically, the proposed SIEM leverages AI for detecting cyberattacks and Software-Defined Networking (SDN) technologies for deploying the appropriate countermeasures.

Prof. Panagiotis Sarigiannidis is the Director of the ITHACA lab (https://ithaca.ece.uowm.gr/), co-founder of the 1st spin-off of the University of Western Macedonia: MetaMind Innovations P.C. (https://metamind.gr), and Associate Professor in the Department of Electrical and Computer Engineering in the University of Western Macedonia, Kozani, Greece. He received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively. He has published over 260 papers in international journals, conferences and book chapters, including IEEE Communications Surveys and Tutorials, IEEE Transactions on Communications, IEEE Internet of Things, IEEE Transactions on Broadcasting, IEEE Systems Journal, IEEE Wireless Communications Magazine, IEEE Open Journal of the Communications Society, IEEE/OSA Journal of Lightwave Technology, IEEE Transactions on Industrial Informatics, IEEE Access, and Computer Networks. He received 5 best paper awards. He has been involved in several national, European and international projects. He is currently the project coordinator of three H2020 projects, namely a) H2020-DS-SC7-2017 (DS-07-2017), SPEAR: Secure and PrivatE smArt gRid, b) H2020-LC-SC3-EE-2020-1 (LC-SC3-EC-4-2020), EVIDENT: bEhaVioral Insgihts anD Effective eNergy policy acTions, and c) H2020-ICT-2020-1 (ICT-56-2020), TERMINET: nexT gEneRation sMart INterconnectEd ioT, while he coordinates the Operational Program MARS: sMart fArming with dRoneS (Competitiveness, Entrepreneurship, and Innovation) and the Erasmus+ KA2 ARRANGE-ICT: SmartROOT: Smart faRming innOvatiOn Training. He also serves as a principal investigator in the H2020-SU-DS-2018 (SU-DS04-2018), SDN-microSENSE: SDN-microgrid reSilient Electrical eNergy SystEm and in three Erasmus+ KA2: a) ARRANGE-ICT: pArtneRship foR AddressiNG mEgatrends in ICT, b) JAUNTY: Joint undergAduate coUrses for smart eNergy managemenT sYstems, and c) STRONG: advanced firST RespONders traininG (Cooperation for Innovation and the Exchange of Good Practices). His research interests include telecommunication networks, internet of things and network security. He is an IEEE member and participates in the Editorial Boards of various journals.

Dr. Dimitrios Pliatsios received his diploma degree from the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Greece in 2016 and his PhD from the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani, Greece in 2022. Currently, he works as a postdoctoral researcher at the ITHACA Lab, Department of Electrical and Computer Engineering, University of Western Macedonia, in EU-funded research projects and participates in drafting research funding proposals. His research interests include resource allocation in wireless communications and edge computing environments, optimization theory, B5G/6G mobile networks, and computer & network security. He is a member of the IEEE and the Technical Chamber of Greece and he has served as a reviewer in several scientific journals (IEEE Internet of Things Journal, IEEE Communication Letters, Elsevier Computer Networks, IEEE Access, MDPI Sensors) and conferences (IEEE GLOBECOM, IEEE ICC, IEEE NetSoft, IEEE CAMAD, IEEE INFOCOM, IEEE PIMRC). His PhD research was funded by the Greek State Scholarship Foundation and he has received the 1st Research Excellence Award from the Research Committee of the University of Western Macedonia.

Dr. Thomas Lagkas is Assistant Professor of the Department of Computer Science of the International Hellenic University. He received his PhD in computer science from the Aristotle University of Thessaloniki, Greece, in 2006. He has been Lecturer and then Senior Lecturer of The University of Sheffield International Faculty - CITY College, from 2012 to 2019. He also served as Research Director of the Computer Science Department of CITY College and Leader of the ICT Track of the South-East European Research Centre. His research interests are in the broad area of IoT communications with more than 90 publications at widely recognized international scientific journals and conferences. Dr. Lagkas is Fellow of the Higher Education Academy in UK. He also participates in the Editorial Boards of respectful scientific journals and is actively involved in drafting research funding proposals, as well as in the implementation of EU projects.

Prof. Vasileios Argyriou received his BSc degree in computer science from Aristotle University of Thessaloniki, Greece, in 2001 and his MSc and PhD degrees from the University of Surrey, in 2003 and2006, respectively, both in electrical engineering working on registration. From 2001 to 2002, he held a research position at the AIIA Lab, Aristotle University, working on image and video watermarking. He joined the Communications and Signal Processing (CSP) Department, Imperial College, London, in 2007, where he was a Research Fellow working on 3D object reconstruction. Now, he is a Professor at Kingston University, working on computer vision and AI for crowd and human behavior analysis, computer games, entertainment, and medical applications. Also, research is conducted on educational games and on HCI for augmented and virtual reality (AR/VR) systems.

Exploring the Advanced Persistent Threat Detection and Correlation Landscape

Zisis Batzos, Konstantinos Kyranou, Ioannis Hadjigeorgiou, Georgios Andronikidis
Sidroco Holdings Ltd., Nicosia 1082, Cyprus
{zbatzos, kkyranou, ihadjigeorgiou, gandronikidis}@sidroco.com

Abstract

Advanced Persistent Threats (APTs) are threats that impose significant challenges to ensuring high levels of cybersecurity. Therefore, innovative approaches are required for the early identification and effective mitigation of these large-scale threats. This work explores the recent advancements in the APT mitigation techniques landscape by providing a review of state-of-art approaches that leverage prediction techniques, attack analysis, correlation methods, and visualization techniques. By providing an overview of the state-of-the-art research in APT detection and analysis, this survey aims to contribute to the design and development of effective defense strategies against APTs.

Keywords: Advanced Persistent Threats, Artificial Intelligence, Cybersecurity, Industrial Internet of Things, Machine Learning.

1. Introduction

Advanced Persistent Threats (APTs) are described as continuously evolving and stealthy cyberattacks carried out by highly skilled groups for long time periods [1]. Often, these groups are supported by governments or other organizations that have political or economic motives. Common APTs targets include governments, military and/or defense organizations, and industrial and financial organizations. Moreover, common objectives of APTs are, among others, espionage and disruption of critical services or utilities.

The life cycle of an APT consists of five stages [2], namely a) reconnaissance, where adversaries carry out research about an organization and its employees, b) breach, where potential vulnerabilities found during the reconnaissance are exploited, c) infiltration, during which, the adversaries search for confidential data and documents, d) exfiltration, during which all confidential information is transferred to an external location, and e) stealth persistence, where adversaries maintain stealthy access to the organization's network for interception of additional confidential information.

This work aims to contribute to the design of appropriate APTs countermeasures by providing an overview of the relevant state-of-art regarding the latest methodologies and approaches for the detection, identification, prediction, and mitigation of APTs.

2. Review of Advanced Persistent Threat Detection and Mitigation Strategies

This section presents an overview of state-of-the-art strategies, systems, and frameworks that leverage various techniques to enhance the detection, identification, and prediction of APTs. A summary of the research works found in the relevant state-of-art is shown in Table I.

The authors of [3] introduced a temporal correlation and traffic analysis approach that is based on three phases. During the first phase, a filtering module parses raw traffic in order to identify malicious traffic based on flow features. This phase effectively reduces the detection time when large traffic volumes are analyzed. The second phase includes a feature extraction module, that extracts the most relevant characteristics (e.g., time characteristics). Finally, the third phase constitutes an anomaly detection module that uses ML-based classification techniques, to classify traffic as malicious or benign. According to the evaluation results, the proposed method can be effective in the accurate detection and identification of APT attacks.

Table I. SUMMARY OF RESEARCH WORKS

Ref.	Year	Brief Description
[3]	2017	Temporal correlation approach for identifying and analyzing malicious traffic
[4]	2018	Machine learning-based system for real-time APT detection and prediction
[5]	2019	Real-time APT detection by correlating information flows
[6]	2019	APT attack scenario reconstruction and decoding methodology using hidden Markov models
[7]	2020	Analysis of sensors alerts to identify potential IKCs against the specified hosts
[8]	2021	Combination of three different deep learning models for APT detection
[9]	2021	Causal correlation aided semantic analysis for APT detection
[10]	2022	End-to-end method for APT reconstruction in large-scale networks based on alert and log correlation
[11]	2023	APT detection system for industrial Internet-of-Things environments

In [4], the authors present a machine learning (ML)-based system aiming to detect and predict APTs. It is able to process and analyse network traffic in real-time, without the need to store data and make early predictions of APT attacks. In more detail, MLAPT has three main phases, namely threat detection, alert correlation, and attack prediction. The threat detection phase includes modules for Tor connection detection (TorCD), scan detection (SD), domain flux detection (DFD), malicious SSL certificate detection (MSSLD), malicious IP address detection (MIPD), malicious domain name detection (MDND), malicious file hash detection (MFHD), and disguised exe file detection (DeFD). This phase generates security alerts (events), which are correlated with an APT attack scenario during the alert correlation phase. The main objective of this phase is the reduction of the false positive rate and includes three main processes, as follows: a) the alerts filtering (AF) that aims to identify redundant or repeated alerts, b) the clustering of alerts (AC) that is responsible for identifying the same APT attack scenarios, and c) the correlation indexing (CI) that evaluates the degree of correlation between alerts of each cluster. Finally, a ML-based algorithm is integrated for the APT attack prediction. The algorithm uses historical data records from the monitored network to determine the probability of the early alerts evolving into successful APT attacks.

HOLMES is a real-time APTs detection system that is based on the correlation of suspicious information flows [5]. Moreover, the proposed system provides capabilities related to alert generation, alert correlation, and attack scenario presentation. The system generates a detection alert by analyzing host audit data and mapping the stages of an ongoing APT campaign. Specifically, HOLMES maps the activities detected in host logs and organization-wide alerts to kill chain-producing alerts that are semantically related to the APT activities. The alert correlation is implemented using the information flow between low-level entities in the system. In addition, noise reduction techniques are integrated with the aim of reducing false positive alerts. Finally, HOLMES implements a graph-based interface for providing a high-level view of the attacker’s steps in real time.

Ghafir *et al.* [6] propose the use of alert correlations and hidden Markov models (HMMs) for the prediction of APTs. The proposed approach includes two phases, namely the attack scenario reconstruction phase and the attack decoding phase. During the attack scenario reconstruction, alerts are triggered for each malicious activity detected, which are filtered and clustered based on the APT scenarios. Then, a correlation indexing process is implemented that assesses the connections between the alerts of each cluster. The correlation relies on comparing the attributes of the alerts which are generated over a distinct correlation period. The attack decoding phase is based on an HMM that aims to find the most probable sequence of APTs based on a given sequence of correlated alerts using the Viterbi algorithm.

Khosravi *et al.* [7] carried out a causal analysis of the alerts generated from both security and non-security sensors to identify potential Intrusion Kill Chains (IKCs) against specified hosts. To properly place the occurring alerts in the chain, the proposed model connects the alerts with various risk categories based on causal connections. The model processes each host's events individually, rather than simulating the attack for the entire system, resulting in a reduced number of alerts over a large period of time. After receiving the alerts from the Security Information and Event

Management (SIEM) system, it ranks hosts according to their probability of being exposed to APT attacks. This is achieved by categorizing the received alerts that correlate with various IKC phases. Directed graphs are used to illustrate causal links; the graph vertices indicate occurrences at particular times, while the directed edges show their chronological reference. The rank of each host's exposure to likely APT attacks is determined by computing a normalized attack surface value for each IKC, based on the APT attacks that were carried out against the considered host.

Xuan and Dao, in [8], explored the use of various deep learning models for the detection of APTs. Specifically, the multilayer perceptron (MLP), convolutional neural network (CNN), and long short-term memory (LSTM) deep learning models are investigated. First, the network traffic is classified into network flow based on the source and destination addresses. Then, the prominent features are identified and extracted, while the aforementioned deep learning models are utilized to classify flows into malicious APTs or benign ones. The evaluation results show that the proposed approach combining three deep learning models features better performance compared to individual deep learning models, both in terms of accuracy and in terms of false positive rate.

Yang *et al.*, in [9], developed a causal correlation-aided semantic analysis system called POIROT, which aims to correlate anomalous events among large volumes of heterogeneous security data, including attack chains. The proposed system examines security logs, extracts the relevant attack indications, and identifies the respective attack. These diverse logs are initially pre-processed and structured into time-ordered alerts. Then, the initial alerts are mapped to alert-chains by determining the causality of the anomalous events. The APT attack procedures, techniques, and tactics from the initial alerts are condensed in the alert-chain structure. Document-topic semantic analysis is employed to extract the latent attack subjects from these alert-chains. Finally, a Latent Dirichlet Allocation (LDA) semantic analysis [12] is performed to accurately identify potential APT attacks from these chains and generate the corresponding alerts.

An end-to-end APT reconstruction method, based on alert and log correlation, for large-scale edge computing environments is presented in [10]. The main objective of the proposed method is to detect any key and high-impact alerts that were missed. In more detail, an alert reduction and correlation algorithm is integrated in order to reduce the number of alerts. After the aforementioned filtering takes place, an alert graph is constructed using the remaining alerts. By applying the Monte Carlo tree search algorithm to the history of alerts and logs, the key missed alerts can be identified with high confidence levels.

In [11], the authors developed an APT detection system tailored to the requirements of industrial Internet-of-Things environments. The proposed system detects and correlates various APT attack stages derived from a customized APT Attack Invariant State Machine. In this direction, based on the MITRE ATT&CK framework [13], the authors identified several attack stages/tactics which are 'invariant', namely discovery, Fieldbus scanning, command-and-control, lateral movement, and communication spoofing. Specifically, the system processes data from multiple sources, including host logs, audit logs, network traffic, and alerts generated from intrusion detection systems. Before the data are analyzed by the APT Attack Invariant State Machine, a pre-processing phase takes place, in which the highest-impact features are extracted. For its evaluation, the authors utilized APT campaigns that were designed based on real-world attack scenarios. The respective results show that the proposed system features high precision, as well as low false negative and false positive rates.

3. Conclusion

This work constitutes a state-of-art survey concerning methodologies and solutions for detecting, predicting, and analyzing APTs. The aforementioned research works leverage various approaches, such as semantic analysis, alert correlation, attack reconstruction, and ML techniques to enhance APT detection and prediction capabilities. The combination of these techniques and methodologies contributes towards developing robust APT detection and correlation systems that can identify malicious activities, reconstruct intricate attack scenarios, correlate multiple alerts, and generate prompt alerts for potential APT campaigns. This survey aims to provide an overview of the latest defensive countermeasures and strategies against the ever-evolving APTs.

Acknowledgement

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

References

[1] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851–1877, Jan. 2019.

[2] M. B. Khan, "Advanced persistent threat: detection and defence,'' 2020, arXiv:2004.10690. [Online]. Available: http://arxiv.org/abs/2004.10690.

[3] J. Lu, K. Chen, Z. Zhuo, and X. Zhang, "A temporal correlation and traffic analysis approach for APT attacks detection," Cluster Computing, vol. 22, no. S3, pp. 7347–7358, Oct. 2017.

[4] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," Future Generation Computer Systems, vol. 89, pp. 349–359, Dec. 2018.

[5] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, and V. Venkatakrishnan, "HOLMES: Real-time apt detection through correlation of suspicious information flows," IEEE Symposium on Security and Privacy (SP), Sep. 2019, pp. 1137–1152.

[6] I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh, and D. M. Diab, "Hidden Markov models and alert correlations for the prediction of advanced persistent threats," IEEE Access, vol. 7, pp. 99 508–99 520, Jul. 2019.

[7] M. Khosravi and B. T. Ladani, "Alerts correlation and causal analysis for APT based cyber attack detection," IEEE Access, vol. 8, pp. 162 642–162 656, Sep. 2020.

[8] C. D. Xuan and M. H. Dao, "A novel approach for APT attack detection based on combined deep learning model," Neural Computing and Applications, vol. 33, no. 20, pp. 13 251–13 264, Apr. 2021.

[9] J. Yang, Q. Zhang, X. Jiang, S. Chen, and F. Yang, "Poirot: Causal correlation aided semantic analysis for advanced persistent threat detection," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3546–3563, Aug. 2021.

[10] Y. Wang, Y. Guo, and C. Fang, "An end-to-end method for advanced persistent threats reconstruction in large-scale networks based on alert and log correlation," Journal of Information Security and Applications, vol. 71, p. 103373, Dec. 2022.

[11] A. Kumar and V. L. L. Thing, "RAPTOR: Advanced persistent threat detection in industrial IoT via attack stage correlation," 2023, arXiv:2301.11524. [Online]. Available: http://arxiv.org/abs/2301.11524

[12] H. Jelodar, Y. Wang, C. Yuan, X. Feng, X. Jiang, Y. Li, and L. Zhao, "Latent Dirichlet allocation (LDA) and topic modeling: models, applications, a survey," Multimedia Tools and Applications, vol. 78, no. 11, pp. 15 169–15 211, Nov. 2018.

[13] The MITRE Corporation, "Tactics - ICS — MITRE ATT&CK," [Online]. Available: https://attack.mitre.org/tactics/ics/.

Authors Bio-data

Zisis Batzos studied Electrical & Computer Engineering (integrated B.Sc. & M.Sc.) in Aristotle University of Thessaloniki (A.U.Th. Greece), where he graduated with distinction. His main research interests are in the domains of Artificial Intelligence, Deep Learning and Computer Vision. He has been also engaged in several projects including various cutting-edge technologies such as Virtual Reality, Extended Reality, Internet of Things, Robotics and Autonomous Vehicles. He is working as a Project Manager and AI Engineer at Sidroco Holdings Ltd. having managerial responsibilities and designing technical solutions in a variety of R&D projects for European research and innovation programmes (Horizon 2020, Horizon Europe, Erasmus+), including FASTER, APPRAISE, IRIS, RESPOND-A, TALON, EVIDENT, INCIDENCE.

Konstantinos Kyranou holds B.Sc. at Mathematics (AUTH) and M.Sc. at Data Science (IHU). He is engaged in a variety of projects deriving from HORIZON2020 including but not limited to AI, energy, (smart)grids & IoT. Additionally, he has significant experience working with RDBMS having consulted a major Greek bank. His key responsibilities are to administratively lead projects and provide guidance with the development exercises.

Ioannis Hadjigeorgiou holds a B.Sc at Computer Science (UNIC). He is curently involved with HORIZON2020 projects that focus on IoT, Cybersecurity, industry4.0, data analytics, AI solutions, digital diagnostics and auto-mated decision support processes for agroecology and organic farming.

George Andronikidis earned a B.Sc. degree in Computer Software Engineering from the University of Thessaly and is currently pursuing a M.Sc. degree in Data Driven Computing and Decision Making at the University of Patras. With his participation in several HORIZON2020 projects he has implemented various Machine Learning and Deep Learning algorithms in cyber security. He is passionate about research and has interests in several areas such as Machine Learning, Deep Learning, Internet-of-Things, Natural Language Processing, Autonomous driving, and Blockchain.

HYPER: Healthcare Cybercrime Protection Framework

George Amponis, Sofia Giannakidou, George Nakas, Marios Siganos, Vasileios Stamatis, Savvas Ouzounidis, George Kakamoukas, Evangelos Mourikis, Maria Zevgara, Antonios Sarigiannidis
K3Y Ltd., Sofia 1000, Bulgaria
{gamponis, sgiannakidou, gnakas, msiganos, vstamatis, souzounidis, gkakamoukas, emourikis, mzevgara, asarigia}@k3y.bg

Abstract

The rapid advancements of smart technologies, particularly in the field of the Internet of Things (IoT), have ushered the healthcare ecosystem into a new era. This new reality revolves around intelligent medical devices and applications that offer a multitude of benefits, including remote medical assistance, timely medication administration, real-time monitoring, preventive care, and health education. However, alongside these valuable advantages, there is an increase in cybersecurity and privacy concerns. Vulnerable IoT medical devices have the ability to autonomously access and handle patients' data, thereby posing a threat to data privacy. In addition, insecure communication channels among various healthcare organizations further exacerbate the risk. Furthermore, the constant evolution of cyberattacks, malware, and zero-day vulnerabilities necessitates the development of corresponding countermeasures that can effectively address the diverse cybersecurity and privacy issues present in the modernized healthcare ecosystem. To tackle these challenges, a Healthcare cYbercrime ProtEction fRamework (HYPER) is presented in this paper. HYPER composes an architectural framework that includes a range of defense mechanisms capable of identifying new attack taxonomies specific to medical settings and effectively mitigating cyberattacks, malware, and their cascading effects.

Keywords: Cybersecurity, Healthcare, Privacy-by-Design Security Analytics, Security Information and Event Management, Software-Defined Networking

1. Introduction

The rapid evolution of smart technologies and especially of the Internet of Things (IoT), has led healthcare organisations to digitise their services by adopting medical telemetry and interconnected medical devices, such as wearables and medical implantables, that autonomously collect and store patient data in Electronic Health Records (EHRs). Although this new reality offers multiple benefits such as remote medical assistance, timely administration of medication, real-time monitoring, preventive care, and health education, it also increases the existing security and privacy concerns due to the heterogeneous co-existing smart and legacy nature of these entities (both hardware and software), as well as their insecure design. Moreover, among the other Critical Infrastructures (CIs), the healthcare domain is considered the most vulnerable one due to the vast amount of sensitive personal and administrative data stored and managed by smart medical devices and EHRs software packages [1]. Based on the European Union Agency for Network and Information Security (ENISA), the healthcare sector continues to lead in the number of cybersecurity incidents [2]. In particular, compared to other sectors, such as government and finance, the healthcare domain is lagging far behind in terms of cybersecurity preparedness. A characteristic cybersecurity incident related to the health sector was the WannaCry ransomware [3], which paralysed the United Kingdom's National Health Service by encrypting multiple sensitive health data, thus locking out legitimate users until a specific amount in Bitcoin was paid. Similar to WannaCry, the NotPetya ransomware attack caused havoc in various sectors, including healthcare [4]. Therefore, the challenge of ensuring smart, safe, sustainable and efficient healthcare systems becomes challenging given the barriers. Based on the previous remarks, in this paper, a Healthcare cYbercrime ProtEction fRamework (HYPER) is proposed. HYPER is composed of several architectural components that can detect, normalise, correlate, and mitigate potential cyberattacks and anomalies against the healthcare ecosystem. The following sections of this paper describe the architectural design of HYPER, taking full advantage of novel computing technologies.

2. Architecture of HYPER: Healthcare cYbercrime ProtEction fRamework

The architecture of HYPER is depicted in Fig. 1. In particular, HYPER will exploit the multiple benefits provided by the Software-Defined Networking (SDN) technology, which discriminates the infrastructure layer (i.e., the various physical devices) from the control layer (i.e., controlling services) by utilising an SDN controller (e.g., Ryu, Opendaylight, and ONOS) [5], as well as SDN-enabled switches. Therefore, security applications located at the application layer can inform the SDN controller via Representational State Transfer (REST) or other relevant protocols concerning possible abnormalities, privacy issues, vulnerabilities and cyberattacks. Then, the SDN controller will execute the appropriate operations at the infrastructure layer utilising the OpenFlow protocol, thereby restoring the normal functionality in case of a cyberattack or a not normal activity. The SDN technology offers three valuable services to HYPER: a) central control and management of the various physical devices, b) global visibility about the overall network and c) self-healing capabilities against possible cyberthreats. HYPER is composed of 6 layers, namely a) Security Information and Event Management (SIEM), b) pRivAcy-by-design Big dAta analyTics (RABAT), c) Correlation Analysis Tool (CAT), d) Vulnerability Database (VD), e) Trust managEment aNd Self-prOtecting fRamework (TENSOR), and f) Anonymous Repository of Incidents (ARI). Apart from TENSOR, all subcomponents are located in the application layer.

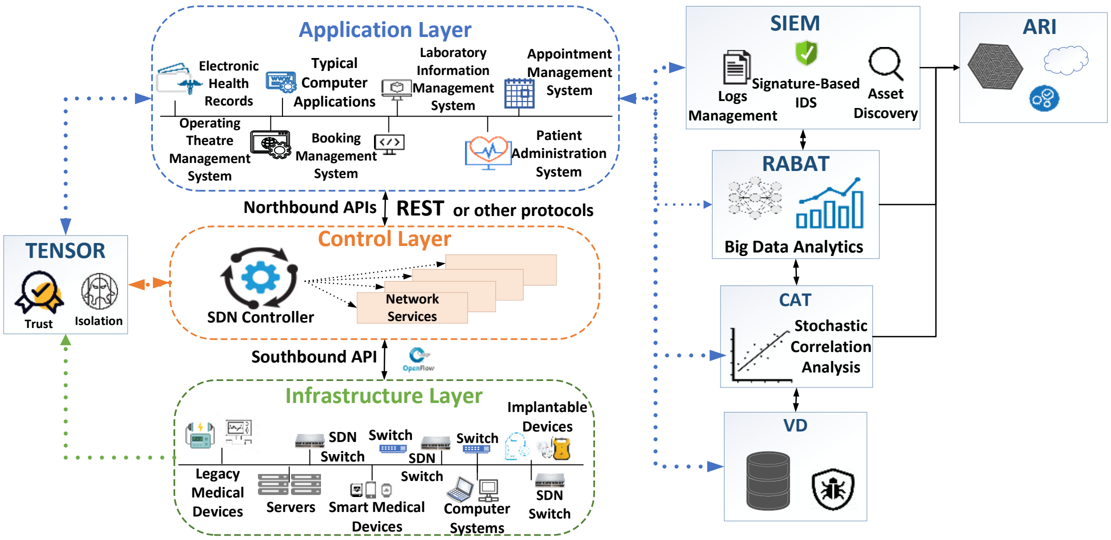


Figure 1: HYPER architecture

2.1. SIEM: Security Information and Event Management System

The SIEM is responsible for feeding with preprocessed data the components of HYPER while providing asset-discovery mechanisms and signature-based intrusion detection [6]. More specifically, the SIEM is able to deploy various probes that will monitor and control the medical devices and, in general, the actions taking place in the various networks of a healthcare organization. The collected data, including network traffic and logs, are used by the next levels of HYPER to identify possible cyberattacks, privacy-related attacks, anomalies, and vulnerabilities. The SIEM also includes both signature-based Host-based IDS (HIDS) and Network-based IDS (NIDS), which will apply signature and specification rules for detecting known cyberattacks.

2.2. RABAT: pRivAcy-by-design Big dAta analyTics

The second layer of HYPER is RABAT, which will apply big data analytics in order to identify potential cyberattacks, privacy issues, and anomalies, that cannot be detected by the signature and specification rules of the SIEM. In particular, RABAT will adopt a plethora of machine learning and deep learning algorithms in order to provide anomaly detection models capable of extracting security events by pre-processing and analysing data coming from the SIEM. In essence, RABAT will constitute an anomaly-based IDS, which will complement perfectly the signature/specification-based IDS of the SIEM. The anomaly detection models of RABAT will be able to identify possible attacks and anomalies in different network layers of Open Systems Interconnection (OSI) by analysing the attributes of the corresponding communication protocols. Particular emphasis will be given to the protocols utilised by medical IoT devices, such as MQTT [9], Zigbee [10], Bluetooth Low Energy (BLE) [11], IEEE 802.15.6 [12], etc.

Finally, RABAT will also analyse operational data, such as measurements of the various sensors.

2.3. CAT: Correlation Analysis Tool

The aim of CAT, which is the third layer of HYPER, is to identify new vulnerabilities and attack taxonomies related to the healthcare sector by analysing the security events generated by the SIEM and RABAT. The SIEM generates security events via signature-based detection, while RABAT follows anomaly-based techniques. In particular, the functionality of CAT is based on stochastic correlation analysis processes. Novel correlation directives consisting of correlation rules will be formed for the various security events and vulnerabilities. These correlation directives will be organised into multiple categories based on the characteristics of the healthcare organisation, such as "Medical IoT Devices Correlation Directives", "Legacy Medical Devices Correlation Directives", "DoS Attacks Correlation Directives", "Privacy Correlation Directives", "Bruteforce Correlation Directives", etc. The categories will constitute the medical-related attack taxonomies. In order to form the correlation directives and their rules, machine learning and deep learning techniques will be examined, such as association learning rules, clustering techniques, autoencoders, deep belief networks and feedforward convolutional neural networks.

2.4. VD: Vulnerability Database

The fourth layer of HYPER is the VD, which aims at providing a dynamic vulnerability database that will be exclusively focused on the vulnerabilities related to the healthcare sector, including both hardware and software medical assets. The VD will be based on the Malware Information Sharing Platform (MISP) Vulnerability Database [7] and will address the issues of the existing vulnerability databases, such as chronological consistency, incomplete inclusion, lack of documentation, multiple entries for a single vulnerability, as well as the separation between vulnerabilities and vulnerability detection events. Each vulnerability of VD is accompanied by many details, such as impact analysis, applicability statements, possible exploits, links to other vulnerability databases as well as specific solutions for each entry. The content of the VD will be updated continuously by zero-day vulnerabilities. Finally, a significant characteristic of the VD is that it can be used for modelling and deploying efficient Vulnerability Discovery Models (VMDs) [8], which usually employ statistical analyses processes in order to identify useful information called vulnerability detection events about the possible vulnerabilities like when the next vulnerability will be presented. Each vulnerability stored in the VD is characterised by the injection, detection, release, disclosure, and patch dates.

2.5. TENSOR: Trust managEment aNd Self-prOtecting fRamework

The fifth layer of HYPER is TENSOR, which aims to identify the untrusted security-related assets in a healthcare ecosystem as well as to address possible cascading effects. To this end, TENSOR combines all layers of the SDN architecture in order to isolate the malicious network flows. First, at the application layer, TENSOR is focused on the trust management and evaluation processes by utilising the security events generated by SIEM, RABAT and CAT. TENSOR continuously calculates the trust value of each asset and its interfaces, i.e., network flows. To compute this trust value, fuzzy logic approaches, clustering techniques and node-centric reputation algorithms can be used, taking into account the significance value of the medical assets, the impact of the security events, as well as their reliability and risk level. Next, TENSOR indicates the SDN controller which network flows are considered critical malicious and can cause cascading effects. Next, the SDN controller undertakes the isolation of the critical malicious network flows by transmitting the appropriate OpenFlow commands to the SDN-enabled switches located at the infrastructure layer. Finally, the SDN-enabled switches update their flow tables, thus rearranging the suspicious network flows and isolating the malicious assets.

2.6. ARI: Anonymous Repository of Incidents

HYPER intends to enhance the situation awareness by also creating and maintaining a repository called ARI, which will include security and privacy incidents in a healthcare environment. The rationale behind the creation of this repository is to broadcast, inform, and exchange critical information about cybersecurity and privacy incidents in healthcare organisations across Europe. In particular, ARI will further develop the idea of utilising a network of trust, where sensitive information is exchanged between organisations, by using an anonymous repository, which will be based on cloud computing technology and will integrate modern anonymisation technologies. Thus, healthcare organisations will be able to broadcast sensitive information in an anonymous way, without exposing the reputation of the organisation.

3. Conclusion

The rapid advancements in smart technologies, and especially IoT, have transformed healthcare with intelligent medical devices and applications offering benefits like remote assistance, real-time monitoring, and preventive care. However, this progress comes with increased cybersecurity and privacy concerns. Vulnerable IoT devices accessing patients' data autonomously pose data privacy risks. Insecure communication channels among healthcare organizations compound these risks. To address these challenges, this paper introduces HYPER, a healthcare cybercrime protection framework. HYPER includes defence mechanisms to detect medical-specific attacks and mitigate cyberthreats effectively.

Acknowledgement

This work has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 952672 (SANCUS).

References

[1] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3723-3768, Fourthquarter 2019.

[2] E. Lakka et al., "Incident Handling for Healthcare Organizations and Supply-Chains," IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, 2022, pp. 1-7.

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

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

[5] P. Radoglou-Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz, A. Sarigiannidis, D. Papamartzivanos, S. A. Menesidou, G. Ledakis, A. Pasias, T. Kotsiopoulos, A. Drosou, O. Mavropoulos, A. C. Subirachs, P. P. Sola, J. L. Domínguez-García, M. Escalante, M. M. Alberto, B. Caracuel, F. Ramos, V. Gkioulos, S. Katsikas, H. C. Bolstad, D.-E. Archer, N. Paunovic, R. Gallart, T. Rokkas, and A. Arce, “SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture”, Digital, vol. 1, no. 4, pp. 173–187, Sep. 2021.

[6] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” Sensors, vol. 21, no. 14, p. 4759, Jul. 2021.

[7] B. Stojkovski and G. Lenzini, "A workflow and toolchain proposal for analyzing users’ perceptions in cyber threat intelligence sharing platforms," IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 324-330.

[8] A. Shukla and B. Katt, "Change Point Problem in Security Vulnerability Discovery Model," International Conference on Software Security and Assurance (ICSSA), St. Pölten, Austria, 2019, pp. 21-26...

[9] C. -S. Park and H. -M. Nam, "Security Architecture and Protocols for Secure MQTT-SN," in IEEE Access, vol. 8, pp. 226422-226436, Dec. 2020.

[10] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 816-829, Oct. 2016.

[11] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, “Performance Evaluation of Bluetooth Low Energy: A Systematic Review,” Sensors, vol. 17, no. 12. MDPI AG, p. 2898, Dec. 2017.

[12] K. S. Kwak, S. Ullah and N. Ullah, "An overview of IEEE 802.15.6 standard," 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010), Rome, Italy, 2010, pp. 1-6.

Authors Bio-data

George Amponis received the B.Sc. degree in Electronics Engineering from the department of Information and Electronic Engineering of the International Hellenic University in 2020 and is now a PhD candidate in the Computer Science department of the same university. He is experienced in ad hoc communications and embedded control and firmware development for industrial, biomedical and aerospace applications. His research interests include UAV swarms, energy-aware routing and ad hoc networking. He is with K3Y Ltd since 2020 and currently working on various research projects (a) SPIDER (H2020-SU-DS-2018): A cybersecurity platform for virtualised 5G cyber range services, (b) RAINBOW (H2020-ICT-2019-2): An open, trusted fog computing platform facilitating the deployment, orchestration and management of scalable, heterogenous and secure IoT service and cross-cloud applications, (c) SANCUS (H2020-SU-ICT-2019: An analysis software scheme of uniform statistical sampling, audit and defence processes, (d) 5G-INDUCE (H2020-ICT-2020-2): Open cooperative 5G experimentation platforms for the industrial sector NetApps, and (e) JAUNTY (KA203-B186BA1A): Joint undergaduate courses for smart energy management systems.

Sofia Giannakidou has received her diploma in Electrical and Computer Engineering from Aristotle University of Thessaloniki. Her scope of interest includes beyond 5G networks, bioelectronics and wireless power transfer applications. Currently she is working on SANCUS (H2020-SU-ICT-2019: An analysis software scheme of uniform statistical sampling, audit and defence processes, and on 5G-INDUCE (H2020-ICT-2020-2): Open cooperative 5G experimentation platforms for the industrial sector NetApps.

Georgios Nakas received the Dipl. Eng. degree from the Department of Electrical and Computer Engineering at the Aristotle University of Thessaloniki, Greece, in 2017 and he is currently finishing his Ph.D. degree at the Department of Electronic and Electrical Engineering at the University of Strathclyde, Glasgow, U.K. His main research interests include optimization methods and machine learning applications. He joined K3Y Ltd as an AI researcher/engineer since 2022.

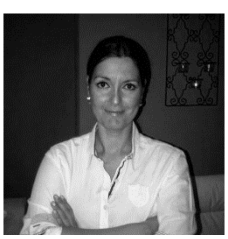
Marios Siganos is a holder of a Master's degree (MSc) in Data Science from the University of Southampton, UK. He has also received a BSc in Computer Science and Biomedical Informatics from the University of Thessaly (Lamia), Greece. His main interests are Data Science and Machine Learning / AI, Software Engineering (Python), Biomedical Informatics, as well as Digital Transformation and STEM in general. He joined K3Y Ltd as an AI Engineer/Researcher in 2022 where he is currently working on various research projects, including TRUSTEE, TREEADS, 5G-INDUCE, JAUNTY and Drones4GREEN.

Vasileios Stamatis is an AI Engineer and Researcher working on various projects. He received his undergraduate degree in Mathematics from the University of Ioannina. After that, he completed his MSc in data Analytics at the University of Strathclyde. Currently he is a PhD Candidate at the International Hellenic University. He joined K3Y in 2023 and his main research interests are Federated Learning and Data Engineering techniques.

Savvas Ouzounidis received the B.Sc. in Computer Studies and MSc in Information Technology Management from the University of Sunderland, U.K. His main research interests are IoT technologies and social media marketing. He is experienced as an Information System manager and as a lecturer in higher education. Furthermore, he is experienced in determining strategy consulting services regarding social media web pages & platforms. Currently he is also a student at the University of Western Macedonia, attending the postgraduate program MBA in Management Information Systems. He is with K3Y Ltd since 2020 and currently working on various research projects, including (a) H2020-SU-DS-2018 (SU-DS01-2018), SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services, (b) H2020-ICT-2019-2 (ICT-15-2019-2020), RAINBOW: An open, trusted fog computing platform facilitating the deployment, orchestration and management of scalable, heterogeneous and secure IoT services and cross-cloud applications, (c) H2020-SU-ICT-2019 (SU-ICT-02-2020), SANCUS: analysis software scheme of uniform statistical sampling, audit and defence processes, (d) H2020-ICT-2020-2 (ICT-41-2020), 5G-INDUCE: Open cooperative 5G experimentation platforms for the industrial sector NetApps and (e) JAUNTY (KA203-B186BA1A): Joint undergaduate courses for smart energy management systems.

Georgios Kakamoukas is a Dipl. in Computer and Telecommuncations Engineering, received the Diploma Degree from the Dept. of Informatics and Telecommunications, University of Western Macedonia, Greece, in 2013. He fulfilled his MSc studies in Information and Communication Technology in 2015 in the International Hellenic University and now he is a Ph.D student in the field of Flying Adhoc Networks (FANETs) in University of Western Macedonia. His main research interests are in the area of FANET communication protocols, FANET deployment in smart agriculture applications, supervised and unsupervised machine learning and big data analytics as well as edge-fog computing . He has been involved as a research associate of University in European (H2020) as well as National (EDK) projects.

Evangelos Mourikis has more than 8 years of professional experience in providing offensive security services. He has undertaken numerous projects as a lead tester. He is leading hacking teams for several years, providing mentoring, career growth, and leadership within the team. Moreover, he holds industry-leading certifications from OffSec and other institutions. He has done security research in several fields such as RF signals, hardware, and blockchain and he has reported numerous critical vulnerabilities and 0 days to big organizations.



Maria Zevgara has over 20 years of working experience in top-level management positions with extensive Digital project portfolios (banking industry, retail industry, insurance, etc) as well as experience managing large, complex multi-use development projects. Maria has a vast understanding of digital projects and in her role as Managing Director, Maria fosters an environment of teamwork and ensures that strategy is clearly defined while overseeing performance and maintaining morale. She is leading teams and driving growth in various industries. Her strong communication and client service skills enhance- every company's-process-driven management philosophy. Also, her excellent communication and interpersonal skills, with the ability to build and maintain strong relationships with stakeholders offer long business relationships with the clients of the company. Proven track record of implementing strategic initiatives, improving operational efficiency, and achieving financial targets.Strong leadership skills, able to motivate and guide teams to achieve common goals. Marili's education includes A General MBA – Business School of Brighton University, UK, and a Bsc Computer Science – Aristotle University of Thessaloniki, Greece.

Dr. Antonios Sarigiannidis received his B.S. and M.S. degrees in computer science from the Department of Informatics, Aristotle University of Thessaloniki. Also, he holds PhD in communication networks from the same department. He is the author or co-author of more than 35 journal papers and conference papers such as IEEE Transactions on Industrial Informatics και IEEE Communications Surveys & Tutorials. He has received 4 Best Paper Awards in international conferences, namely, IEEE CAMAD (2019), IEEE MOCAST (2020), IEEE CSR (2021). He actively participated in both national and EU funded projects such as 5G-INDUCE, SMART5GRID, EVIDENT, TERMINET, RESPOND-A , CARAMEL, SDN-microSENSE, SPEAR. He is co-founder of K3Y Ltd. His research interests include telecommunication networks, 5G networks, Internet of Things (IoT), network security and cybersecurity, software-defined networks (SDN), and smart grids. He is a certified CISCO Instructor (2020) and CEH (Certified of Ethical Hacker – 2020).

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 customdeveloped 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.

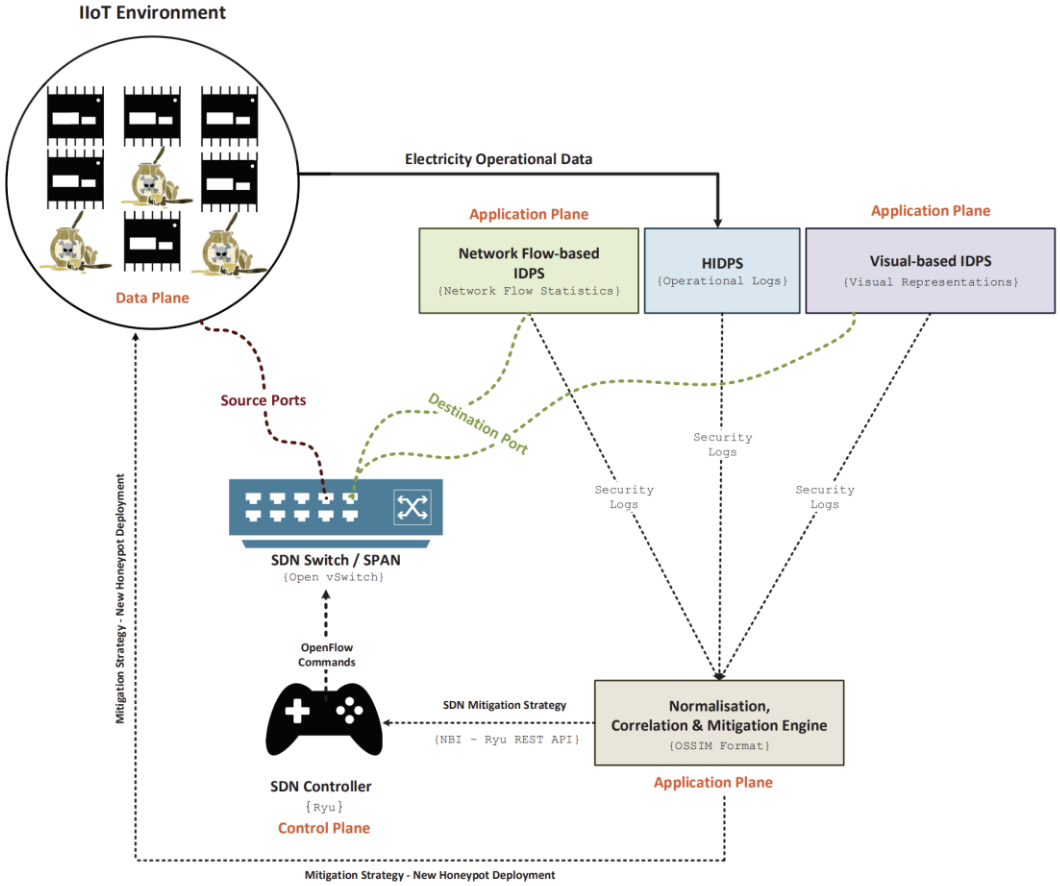


Figure 2: SDN-enabled SIEM Architecture

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.

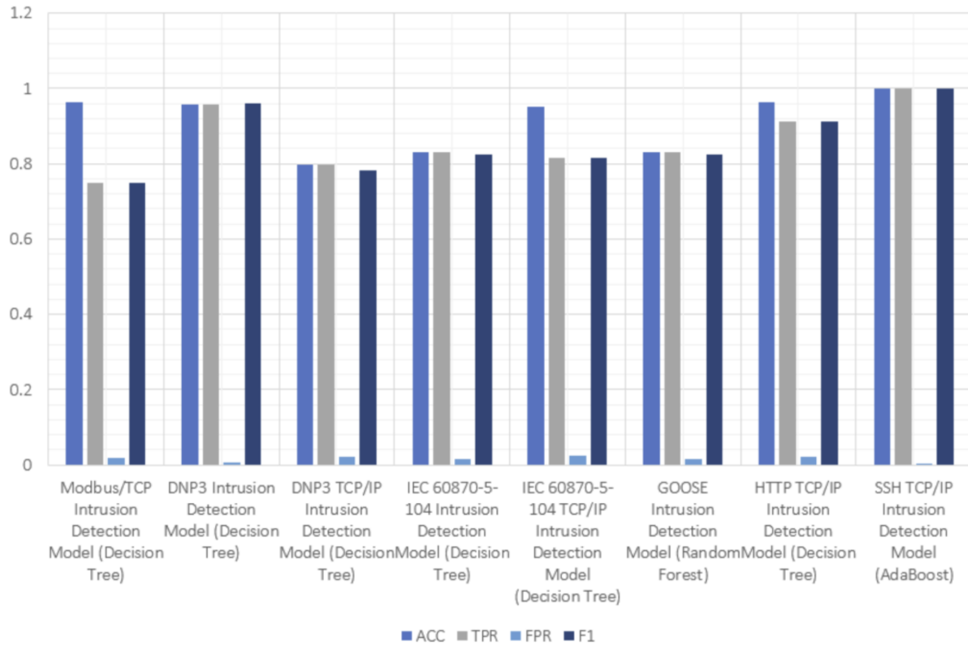


Figure 3: Evaluation Results of NF-IDPS Detection Models

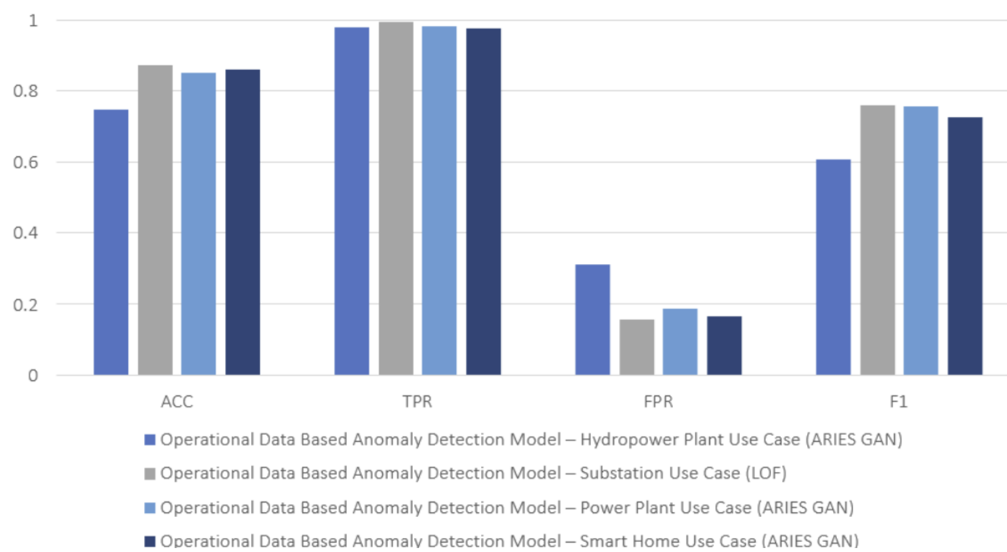


Figure 4: Evaluation Results of H-IDPS Detection Models

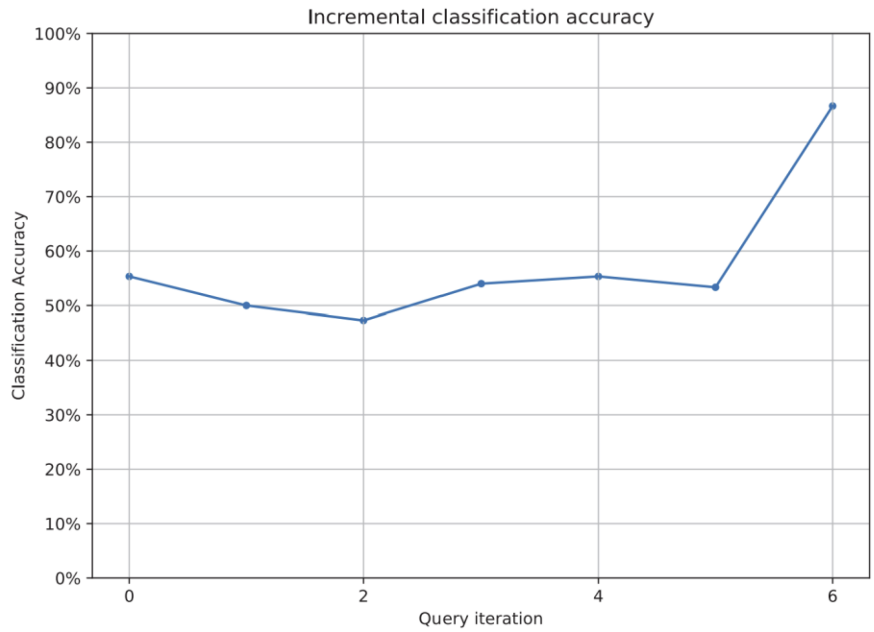


Figure 5: Accuracy Improvement in Re-Training Phases of Active ResNet50-based CNN

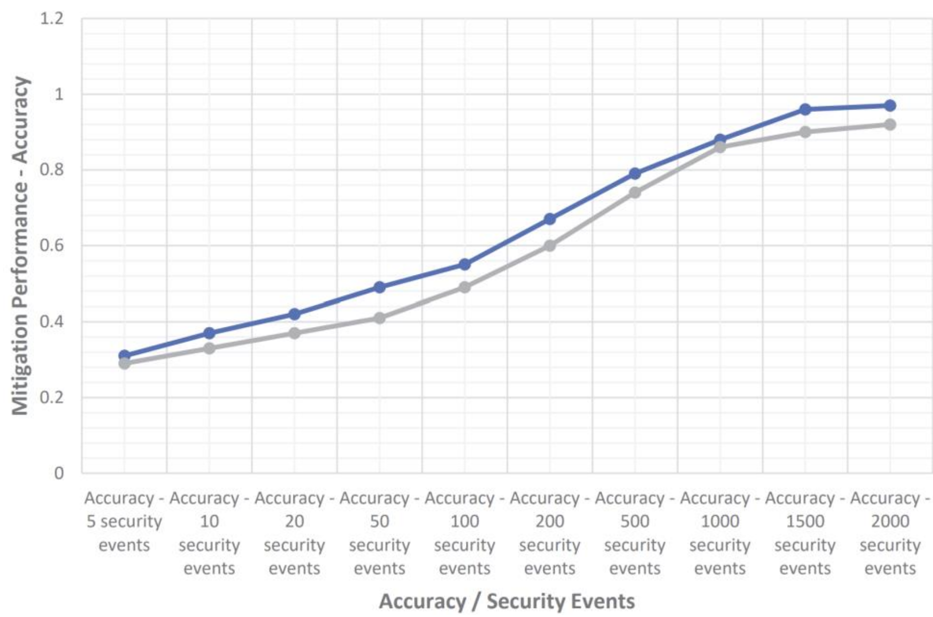


Figure 6: TS Mitigation Accuracy according to the Number of the Security Events

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.

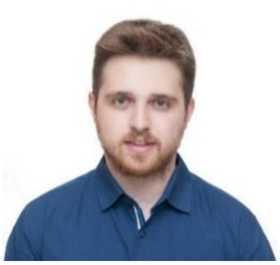
[7] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems", IEEE Access, vol. 7, pp. 46595-46620, 2019.

[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)