This paper is a preprint; it has been accepted for publication in 2022 IEEE Global Communications Conference (GLOBECOM), 2nd Workshop on Edge–AI and IoT for Connected Health, 4–8 Dec. 2022, Rio de Janeiro, Brazil.

An Intelligent Platform for Threat Assessment and Cyber-Attack Mitigation in IoMT Ecosystems

Nicholas Kolokotronis[1], Maria Dareioti[1], Stavros Shiaeles[2], and Emanuele Bellini[3]

[1] University of the Peloponnese, 22131 Tripolis, Greece
nkolok@uop.gr, m.dareioti@go.uop.gr

[2] University of Portsmouth, PO1 2UP, Portsmouth, UK
stavros.shiaeles@port.ac.uk

[3] LOGOS Ricerca e Innovazione, 50142 Florence, Italy
emanuele.bellini@logos-ri.eu

Abstract

The increasing connectivity of medical devices along with the growing complexity, heterogeneity and attack surface of healthcare ecosystems has lead to numerous severe cyber-attacks. This paper proposes a novel collaborative security platform for threat assessment, intelligent detection and autonomous mitigation. The solution leverages *machine learning* (ML) and federated learning for detecting and preventing sophisticated multi-stage attacks, as well as blockchain for supporting integrity verification and accountability to defend against advanced persistent threats. The solution uses a distributed edge approach, performing intensive computations at the edge of the network, where information is generated, to achieve real-time processing of security events. The prevention capabilities employ autonomous decision-making with optimal response strategies towards cyber-attacks and run-time adaptation; these rely on dynamic risk-based models that use real-time information about security incidents.

Keywords: Cyber-security; Intrusion detection; Intrusion response; Machine learning; Internet of medical things.

1 Introduction

The *Internet of things* (IoT) is comprised of a vast number of interconnected devices processing and sharing vast amounts of possibly sensitive or critical data with the goal of improving the quality of our life. Sensors, embedded systems, and other IoT devices, which are utilized in *industrial IoT* (IIoT) environments, complex healthcare ecosystems, and other sectors, become increasingly connected to support novel services and delivery models. In particular, this is evident in the healthcare sector, where the rapidly increasing connectivity gave plenty of room for diverse types of cyber-attacks. Indeed, the majority of the attacks targeting *Internet of medical things* (IoMT) devices have medium-to-significant severity and have rather become the norm in connected healthcare ecosystems [11]. Exploitation of insecure IoMT devices by hackers can potentially lead to all kinds of harm, putting patients' data and lives at risk — in addition to other impacts these attacks could have. Although the baseline security capabilities can typically be assured, they cannot address the numerous ways that IoMT devices are used and interface with the time-varying healthcare ecosystem,

as well as, how these security risks could result into unacceptable safety issues [22].

Intrusion detection systems (IDS) constitute the basic line of defense against attacks, as they can detect possible malicious activity and provide informative security alerts. The detection engine relies on signatures or *machine learning* (ML) models, or a combination, classifying an IDS into rule-based, anomaly-based, and hybrid respectively [10]. However, IDSs that have been deployed at various network locations and are operating in a standalone fashion cannot detect complex and multi-stage network attacks. Therefore, the new paradigm of *collaborative intrusion detection networks* (CIDN) has been developed [20] allowing various collaboration mechanisms among IDS peers to be implemented so as to increase their detection capabilities. A CIDN consists of several nodes that collect and process traffic to detect security events as well as nodes that analyze such data to raise alerts and extract *cyber-threat intelligence* (CTI) information [30]; sharing among CIDN peers may occur at any level. This collaboration has also been explored in the context of *federated learning* (FL), where ML model updates are exchanged in a privacy-preserving manner [14, 23].

In this paper, we proceed beyond the notion of the CIDN towards the complete high-level design of an *intelligent mitigation platform for advanced cyber-threats* (IMPACT) that is well-suited for the increasingly connected complex healthcare ecosystem. The proposed solution offers advanced cyber-threat modeling and reaction capabilities (see e.g. [9,12]) that allow to effectively respond against sophisticated multi-stage attacks targeting critical healthcare information systems and sensitive patients' health data [11]; the mitigation actions of the *intrusion response system* (IRS) can be optimal with respect to a well-defined objective function that balances between security and availability of healthcare infrastructure [21, 27]. The threat modeling is built upon *graph-based network security models* (GNSM), whereas the IRS decision-making process relies on game-theoretic solution concepts. An ML-based IDS, sharing data with other CIDN peers via FL, is used for providing alerts (observations) to the IRS.

The paper is organized as follows: related work is presented in Section 2, whereas the proposed solution's architecture is outlined in Section 3. The IDS/IRS design and deployment options for healthcare environments are given in Section 4. Finally, Section 5 provides the concluding remarks.

2 Related work

This section provides background on collaborative intrusion detection, intrusion response, and blockchain solutions for the healthcare sector.

Intrusion detection systems are an infrastructure's first line of defense against attacks. They are subdivided into *network based* (NIDS) and *host based* (HIDS) depending on whether the network traffic of all *local area network* (LAN) hosts or the operating system's processes of a specific host are monitored [2]. Since an IDS alone is not always able to identify large-scale attacks, the use of CIDNs has been proposed [7]. A CIDN consists of many IDS workers that collect and share security events, as well as analysis units for correlating events and extracting useful threat intelligence information [30]. The architectures that CIDNs adopt can be classified as centralized, decentralized, and distributed; they are discussed in [16] along with trust management schemes and use of blockchain to deal with insider and other prominent attacks. Many works have proposed intrusion detection systems for the IoT ecosystem; a detailed review and classification of the detection techniques, features' selection, evaluation methodologies, and deployment options is provided in [10]. The superiority of anomaly-based techniques in detecting unknown attacks and their ability to adopt to the operational environment makes them ideal for the IoMT ecosystem. Several intelligent intrusion detection systems have been proposed relying on different ML or *deep learning* (DL) algorithms [1, 3, 19, 25]. Recent studies have also considered using FL approaches to improve IDS performance for the IoMT — see e.g. [18, 24] and the references contained therein.

Intrusion response systems improve security against cyber-attacks as they can compute optimal mitigation actions at real time. A comparative analysis of IRS designs was performed in [12], where the

generation of responses from the IDS alerts were classified as *static*, *dynamic*, and *cost-sensitive*. A survey of intelligent intrusion response approaches was conducted in [15] emphasizing on the added value that game theory brings in modeling the interactions between defenders and attackers. The protection of healthcare infrastructures is a hard task. To obtain accurate threat models, a deeper understanding of the systems involved, their vulnerabilities, and their dependencies is required [13]. GNSM models, and more precisely the *attack graphs* (AG), allow correlating vulnerability exploitations so as to model multi-stage attacks and define attackers' targets; scalability problems can be dealt with variants, like *Bayesian attack graphs* (BAG) [9]. Multi-criteria approaches can also be built on top of such models to provide an IRS the ability to choose from a set of actions, such as firewall rules and other mitigation actions defined in MITRE's D3FEND framework[1], in an optimal fashion [26].

Blockchain and *distributed ledger technologies* (DLT) have found extensive applications in all domains under the umbrella of IoT since they provide the means for creating far more secure decentralized solutions [6]. Access control to *electronic health records* (EHR), and healthcare information systems, is probably among the first and most prominent applications of blockchain in healthcare [29], in addition to ensuring integrity of EHR data. Towards this direction, many applications rely on blockchain to securely store audit logs [5], or to safeguard IoT / IoMT devices' critical files [17].

3 Proposed architecture

This section presents the primary concepts of the proposed platform, called IMPACT (intelligent mitigation platform for advanced cyber-threats), which is based on three main pillars: distributed *artificial intelligence*, *software-defined networking* (SDN) and *multi-access edge computing* (MEC). In the MEC paradigm devices are categorized as: resource-constrained end IoMT devices, computationally capable edge nodes (close to end users), and the cloud platform. The high-level architecture is illustrated in Fig. 1 and is structured in four layers (bottom to top): the physical layer, the MEC layer, the application/service layer, and the access layer.

- *Physical layer*. Includes IoMT devices and networking equipment (gateways); the connectivity options are: connection to an edge node via an IoMT gateway; direct connection to the edge node, e.g. for computation offloading; and direct connection to the platform.
- *MEC layer*. Includes the edge nodes that provide a subset of the cloud platform's security services in real-time and semi-autonomous fashion.

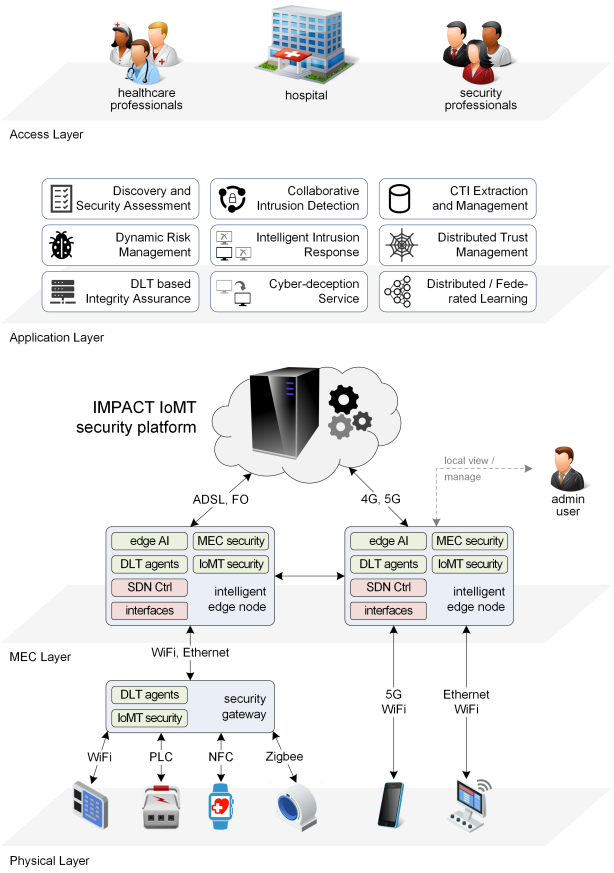

Figure 1: High-level architecture of the proposed IMPACT platform.

[1] https://d3fend.mitre.org/

Core functionality provided by the edge nodes includes: security services to end-devices and edge nodes; local aggregation of ML models used by the intelligent IDS; and other services, like DLT-based integrity verification mechanisms.

- *Application layer.* Includes the security solutions provided as-a-service to end-users by the cloud platform and the management of the platform itself — these are further elaborated next.

- *Access layer.* Delivers the services of the platform to healthcare and security professionals, hospitals, and other organizations related to IoMT services.

SDN is a core enabling technology that dynamically alters the network configuration (routing, switching) to add flexibility to infrastructure deployment, optimally adapt to network events (e.g. node failures, congestion), and isolate security threats. This flexibility also allows IMPACT to proactively employ cyber-deception and moving target defense techniques (change the infrastructure's attack surface) against more sophisticated threats, like *advanced persistent threats* (APT) and adaptive multi-stage attacks. Complimentary to MEC, collaborative and distributed ML moves the complexity of the ML engines from the cloud towards edge nodes and end-devices, depending on their capabilities. This allows to balance the high demand for resources that are needed by the computationally intensive ML algorithms, by exploiting the availability of network resources at the edge, while introducing autonomous decision-making in critical operations. IMPACT relies on FL (detailed in Section 4) for delivering a distributed intelligence model. The architectural pillars presented above (MEC, SDN and FL) allow the delivery of a platform, flexible to adapt to the heterogeneous and complex IoMT landscape and capable of providing real-time security services. Next, we present the most prominent security components.

3.1 Healthcare ecosystem's security assessment

IoMT environments are highly dynamic and thus medical devices should be identified and detailed information about them must be collected. Additionally, unauthorized end-devices should also be detected and accounted for as they might be indicators of the physical infrastructure's intrusion. In any case, they increase the network's attack surface and should be treated accordingly. The *ecosystem discovery and security assessment* (EDSA) module is a set of tools that collect, maintain, and store dynamically changing information on: a network's topology; deployed network security defenses; and protected assets and devices. Its major objectives are:

- *Network topology and host discovery.* Continuously scan a network to detect changes to its topology or hosts, including network assets dedicated to the provisioning of important services; such techniques can provide useful information about the hosts (e.g. host names, IP addresses) and their connectivity.

- *Network monitoring.* Perform network scans to enumerate open network ports (and protocols used) in medical devices and analyze the network connections established.

- *Device vulnerability assessment.* Assess with a sufficient level of automation the network hosts to discover vulnerable software or misconfigurations.

3.2 DLT-based integrity verification of medical devices

Medical *device integrity verification* (DIV) relies on the ability of blockchain to create secure, decentralized and distributed networks of IoMT devices to considerably reduce the ability of hackers to tamper with reduced-security legacy IoMT devices. The goal is to store a verified copy of files (e.g. firmware, OS kernel, etc.) being critical for the devices' reliable operation and subsequent validation and remediation whenever needed. The proposed approach will automatically

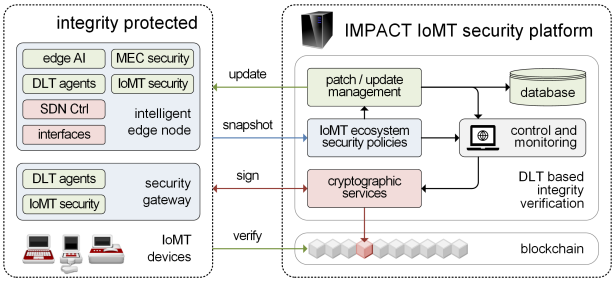

Figure 2: Block diagram of the DLT-based integrity verification.

enhance the overall security of the IoMT ecosystem as it will also prevent insider attacks; e.g., even when gaining administrative rights on a target medical system, hackers will not be able to modify the information on the blockchain without being noticed by the validators.

The solution's main building blocks are shown in Fig. 2 and include: (a) the security policies dictating how to capture a medical device's state (under integrity protection) in the form of snapshots; (b) the patch/update management services that manage snapshots, perform verification against already collected data, and securely manage updates or patches of medical devices; and (c) the cryptographic services gateway that allows to verify an IoMT device's integrity.

4 Intelligent intrusion detection and response

This section describes the functionalities related to the ML-based intrusion detection, the use of federated learning, as well as, the provisioning of advanced intrusion response by leveraging GNSM threat models.

4.1 Collaborative intrusion detection

A decentralized CIDN architecture is adopted, which allows IDS nodes to gain knowledge by sharing information, to meet the needs of complex healthcare ecosystems and increase their resiliency against sophisticated attacks. The CIDN consists of nodes with a topological structure (e.g. hierarchical), so that the analysis units (IDS workers) work as filters forwarding correlated data to the higher levels of the architecture. Efficient schemes aiming at information sharing within the CIDN via gossiping protocols (using formats such as the IDMEF), and exploration trust-based schemes supported via blockchain have been implemented [16]. The detailed block diagram of an IDS worker is illustrated in Fig. 3.

The intrusion detection engine of CIDN peers uses both signature-based and anomaly-based detection techniques for detecting known and potentially unknown cyber-threats. The anomaly-based detection technique builds upon the approach proposed in [28], where the ML module utilizes the Hilbert space-filling curve as its primary clustering algorithm; this is achieved by assigning specific colors to each byte based on its ASCII code: blue / green / red for printable / control / extended characters as well as black / white for the characters 0x00 and 0xFF respectively. These generated byte arrays are then transformed into images retaining optimal locality for pattern recognition, so as to be processed by ML image classification models [4]; samples of malicious network traffic were used to train the classifier. Then, the trained classifier is used to analyze and classify the output images as legitimate or malware. In this context, DL neural networks and more precisely *convolutional neural networks* (CNN) are ideal for processing 2D images and achieved promising results [28]. The ML-based detection algorithms have been implemented so as to extend well-known open source IDS tools (Suricata and Zeek).

The above described detection process has been extended to support FL for delivering a distributed intelligence model. Due to FL, the models are trained in three steps: (a) the medical devices / edge nodes with AI-based security operations receive the model to train from the cloud platform; (b) the models are trained using local data with model updates sent back to the IMPACT platform; and (c) the platform aggregates the received models and sends the updated parameters back to the medical devices/edge nodes. In essence, this approach allows the collaborative train-

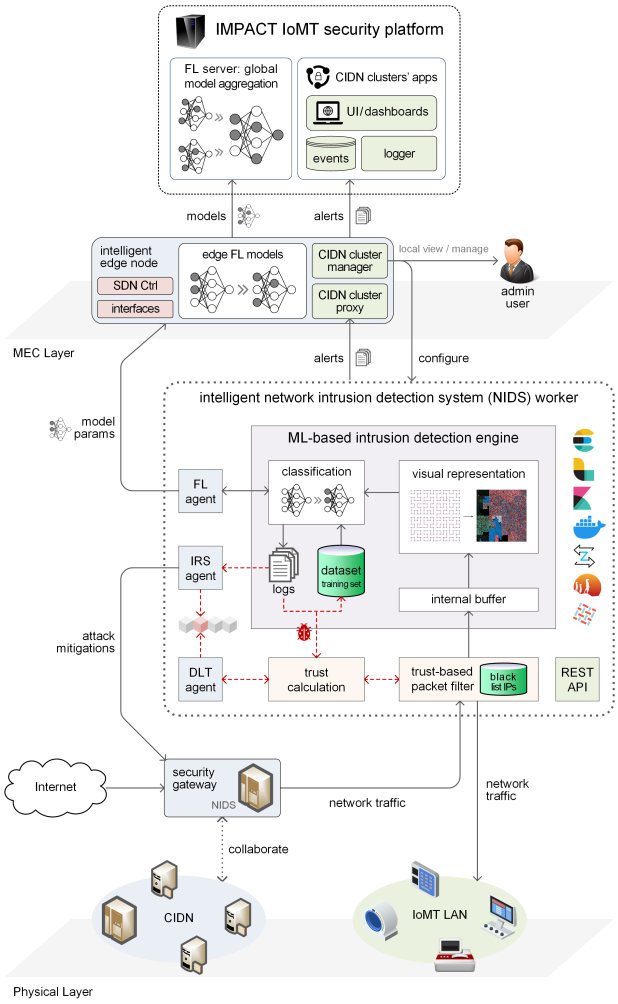

Figure 3: Detailed block diagram of the FL-based CIDN peer node.

ing of the various models used by the ML-based intrusion detection at the edge of the healthcare networks. The options considered for training the ML models include:

- *Raw data training*, in which the cloud platform directly trains the ML models with data received by the end devices; this training mode is best suited for IoMT devices lacking the resources to perform training and with no access to edge nodes.

- *FL at the edge node*, in which the edge node trains the model with data received by the end-devices and sends the updated model to the cloud platform for aggregation; as a form of computational offloading, it is best suited for resource-constrained IoMT devices with access to an edge node.

- *FL at end-devices*, in which the devices train the local models with their own data, and send the updated ones to the IMPACT platform for aggregation, possibly after having first performed model aggregation at the edge nodes (this is the case depicted in Fig. 3); this option requires high computing power, typically not possessed by the majority of IoMT devices and low-end network equipment.

4.2 Dynamic risk management

The *dynamic risk management* (DRM) and decision-making process for optimal mitigation actions aim at defending against adaptive multi-stage cyber-attacks in a fair and autonomous fashion. Simply relying on anomaly-based detection methods, like deep packet inspection or protocol and data analysis, traditional NIDS fail to detect multi-stage or sophisticated attacks —often employed by APT which are highly motivated and have access to a significant amount of resources. To address this challenge, DRM aims at modeling the complex state of a network (been seen as the relations between the end medical devices and their vulnerabilities) and continuously analyze its security status. This is achieved by relying on GNSM models, which have proven to be an extremely powerful in security applications, and in particular on a prominent type of GNSM referred to as *attack graph* (AG). Such structures are used on computing an accurate value of the risk associated with a medical device (based on information about its vulnerabilities, configuration, etc.) and the impact (technical or business) a successful attack would have. The DRM tool will communicate external repositories (e.g. implemented by the MISP platform) on vulnerabilities,

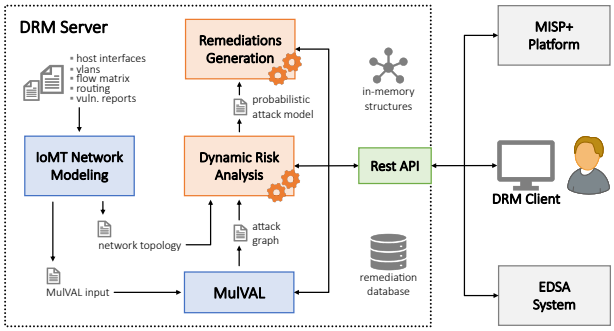

Figure 4: Detailed block diagram of dynamic risk management.

threats, and *indicators of compromise* (IoC), to calculate this risk at real-time, while automatically indicating (or applying, depending on the settings) the actions having been identified to optimally mitigate the risk. This *proactive choice* of actions will not be static, but will adapt to the particular healthcare environment that the DRM tool is being executed (more formally, the solution will be the result of a constraint optimization problem, where the constraints are set by the operational healthcare environment). In addition, the DRM tool is able to automatically update the values of the parameters that are typically used in risk analysis models, like an attack's likelihood (whether an exploit is chosen over others by an adversary) and the attack's success probability (whether the exploit succeeds into exploiting a vulnerability) among others, by leveraging knowledge on cyber-security incidents having been accumulated due to the contribution/sharing of the CIDN peers. This will be used to update information like attacker's access privileges, exploits, vulnerabilities (resp. transitions from an attack's precondition to a post-condition) that could eventually be utilized by AGs with a large number of implementation options.

The high-level architecture of the DRM tool is shown in Fig. 4, illustrating its core parts but also its link with other modules, like the EDSA (so as to receive information about the healthcare network's topology), the dynamic repositories with CTI and vulnerabilities (to get fresh information on vulnerabilities having been reported or updated ones). The proposed architecture is the base abstraction for a number intrusion response system (IRS) implementations with the following added values:

- Dynamic (risk) assessment, whilst considering the existence of attack scenarios with multiple attack goals (e.g. multi-stage attacks).
- Identification of optimal defense actions, considering the possible attack paths (i.e. the AG sub-graphs) that could be chosen by an attacker with a high probability due to high successful exploitation likelihood.
- Recognition of patterns non-detectable by traditional IDS (that possibly indicate novel attacks) — especially if they are paired with intelligent methods for attack modeling.

The tool has been evaluated in assisted living / smart home scenarios [8] and also in IIoT domains with excellent results regarding its capability to respond (in conjunction with the IRS of Section 4.3) to multi-stage attacks; however, its evaluation in the IoMT domain, following the specific architecture detailed herein, is part of the ongoing research work.

4.3 Intelligent intrusion response

The IRS is tightly coupled with the DRM tool presented above and aims to hinder target identification or further penetration of a healthcare network. This is achieved by dynamically re-composing the network topology of the healthcare infrastructure, thus changing its attack surface and adding to the attacker's required workload. In the context of the proposed solution, the IRS is applied both at the end-users' network (e.g. of the healthcare ecosystem), using more basic methods like the application of firewall rules, and also at the SDN level by recomposing the network communication channels. Typical actions that are supported by the IRS include:

- *IP address shuffling*: changing the IP address of the network host to discourage/obstruct an attacker.

- *Host connectivity changes*: changing medical devices' interconnectivity by using the dynamic routing capability of SDN or by issuing firewall rules.

- *Healthcare service changes*: changing the availability of services or functions provided by a healthcare network.

IRS actions are usually separated from cyber-deception, as the former adds randomness to the static network while the latter engages directly with the attacker — although IRS actions can be used for cyber-deception and vice versa. The IRS presented in Fig. 3 is responsible for the dynamic, real-time computation of the remediation actions based on the network's AG model; enforcement of the mitigation actions will be carried out by the security mechanism (software or hardware) that is consuming the derived rules (Fig. 3 illustrates that these rules are consumed by the IoMT gateway, but this could also include IoMT devices capable of enforcing security policies — e.g. rules for shaping the access control).

In principle, the IRS receives alerts (observations) from the IDS peer of the CIDN to update its belief about the current security status of the healthcare network (i.e. the capabilities that an attacker might have acquired through the course of a multi-stage attack). The system's adaptivity also comes in the form of optimizing the remediation actions to the end-user's needs a (e.g. in terms of the desired availability of certain healthcare network services that are deemed to be critical for the network's or certain systems' operation). To optimally choose a remediation action, the IRS uses a mathematical model of the attack, which is based on discrete-time *partially observable Markov decision processes* (POMDP), and simulates the possible adversarial actions an attacker may take (towards exploiting vulnerabilities), so as to predict the likelihood of compromise using the foreseen attack paths, or unknown ones with some probabilistic model leveraging information computed via the GNSM [8, 21].

5 Conclusions

This paper proposed a novel collaborative security platform for threat assessment, intelligent detection and mitigation of attacks. The solution employed ML/FL for detecting and preventing sophisticated multi-stage attacks, as well as blockchain for supporting integrity verification. Taking advantage of the distributed cloud networking infrastructure and especially of the data centers positioned across edge locations, the proposed solution is capable to: (a) accommodate computationally less-capable IoMT devices, which are common in the healthcare ecosystem, by offloading their computational needs to the closest edge node; (b) provide real-time security services to healthcare professionals, which is possible due to the lower network communication latency between the medical devices and the edge nodes; and (c) collaboratively adapt the platform's dynamic ML models and update its knowledge by using shared information that is distributed across the network. Individual IDS, IRS systems' evaluation results, which have been reported in authors' prior works, showcase the proposed solution's viability. The evaluation of the overall solution in the IoMT domain is part of the ongoing research work.

6 Acknowledgments

This project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements no. 833673 and 957406. The work reflects only the authors' view and the Agency is not responsible for any use that could be made from the information it contains.

References

[1] Mahmoud Abbasi, Amin Shahraki, and Amir Taherkordi. Deep learning for network traffic monitoring and analysis (NTMA): A survey. *Computer Communications*, 170:19–41, 2021. DOI: 10.1016/j.comcom.2021.01.021.

[2] Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Natalia Reka Ivanko, and Max Mühlhäuser. Towards blockchain-based collaborative intrusion detection systems. In *12th Int'l Conference on Critical Information Infrastructures Security — CRITIS*, pages 107–118. Springer, 2017. DOI: 10.1007/978-3-319-99843-5_10.

[3] Irina Baptista, Stavros Shiaeles, and Nicholas Kolokotronis. A novel malware detection system based on machine learning and binary visualization. In *53rd IEEE International Conference on Communications — ICC, DDINS Workshop*, pages 1–6. IEEE, May 2019. DOI: 10.1109/ICCW.2019.8757060.

[4] Gueltoum Bendiab, Stavros Shiaeles, Abdulrahman Alruban, and Nicholas Kolokotronis. Iot malware network traffic classification using visual representation and deep learning. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pages 444–449. IEEE, 2020. DOI: 10.1109/NetSoft48620.2020.9165381.

[5] Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, and Clément Pavué. Blockchain solutions for forensic evidence preservation in IoT environments. In *5th IEEE International Conference on Network Softwarization — NetSoft, SecSoft Workshop*, pages 110–114. IEEE, June 2019. DOI: 10.1109/NETSOFT.2019.8806675.

[6] Sotirios Brotsis, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, and Stavros Shiaeles. On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance. *Computer Networks*, 191:108005, May 2021. DOI: 10.1016/j.comnet.2021.108005.

[7] Carol J. Fung. Collaborative intrusion detection networks and insider attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1):63–74, March 2011. DOI: 10.22667/JOWUA.2011.03.31.063.

[8] Konstantinos P. Grammatikakis, Ioannis Koufos, and Nicholas Kolokotronis. Moving-target defense techniques for mitigating sophisticated IoT threats. In Gohar Sargsyan, Dimitrios Kavallieros, and Nicholas Kolokotronis, editors, *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, pages 51–73. Now Publishers, March 2022. DOI: 10.1561/9781680838350.ch4.

[9] Konstantinos-Panagiotis Grammatikakis and Nicholas Kolokotronis. Attack graph generation. In Nicholas Kolokotronis and Stavros Shiaeles, editors, *Cyber-Security Threats, Actors, and Dynamic Mitigation*, pages 281–334. CRC Press, 2021. DOI: 10.1201/9781003006145-8.

[10] Somayye Hajiheidari, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour. Intrusion detection systems in the internet of things: A comprehensive investigation. *Computer Networks*, 160:165–191, 2019. DOI: 10.1016/j.comnet.2019.05.014.

[11] Healthcare Information and Management Systems Society (HIMSS). 2021 HIMSS healthcare cybersecurity survey, Jan 2022.

[12] Zakira Inayat, Abdullah Gani, Nor B. Annuar, Muhammad K. Khan, and Shahid Anwar. Intrusion response systems: Foundations, design, and challenges. *Journal of Network and Computer Applications*, 62:53–74, 2016. DOI: 10.1016/j.jnca.2015.12.006.

[13] Sushil Jajodia, Steven Noel, and Brian O'Berry. Topological analysis of network attack vulnerability. In *Managing Cyber Threats: Issues, Approaches, and Challenges*, pages 247–266. Springer, 2005. DOI: 10.1007/0-387-24230-9_9.

[14] Vasiliki Kelli, Vasileios Argyriou, Thomas Lagkas, George Fragulis, Elisavet Grigoriou, and Panagiotis Sarigiannidis. Ids for industrial applications: A federated learning approach with active personalization. *Sensors*, 21(20):1–17, 2021. DOI: 10.3390/s21206743.

[15] Christophe Kiennert, Ziad Ismail, Herve Debar, and Jean Leneutre. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Computing Surveys (CSUR)*, 51(5):1–31, 8 2018. DOI: 10.1145/3232848.

[16] Nicholas Kolokotronis, Sotirios Brotsis, Georgios Germanos, Costas Vassilakis, and Stavros Shiaeles. On blockchain architectures for trust-based collaborative intrusion detection. In *2019 IEEE World Congress on Services — SERVICES*, pages 21–28. IEEE, July 2019. DOI: 10.1109/SERVICES.2019.00019.

[17] Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, and Romain Griffiths. Secured by blockchain: Safeguarding Internet of things devices. *IEEE Consumer Electronics Magazine*, 8(3):28–34, May 2019. Special issue:

blockchain technologies for consumer electronics, DOI: 10.1109/MCE.2019.2892221.

[18] Abdullah Lakhan, Mazin Abed Mohammed, Jan Nedoma, Radek Martinek, Prayag Tiwari, Ankit Vidyarthi, Ahmed Alkhayyat, and Weiyu Wang. Federated-learning based privacy preservation and fraud-enabled blockchain iomt system for healthcare. *IEEE Journal of Biomedical and Health Informatics*, pages 1–10, 2022. DOI: 10.1109/JBHI.2022.3165945.

[19] Nikhil Laxminarayana, Nimish Mishra, Prayag Tiwari, Sahil Garg, Bikash K. Behera, and Ahmed Farouk. Quantum-assisted activation for supervised learning in healthcare-based intrusion detection systems. *IEEE Transactions on Artificial Intelligence*, pages 1–8, 2022. DOI: 10.1109/TAI.2022.3187676.

[20] Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, and Raouf Boutaba. Collaborative security: A survey and taxonomy. *ACM Computing Surveys*, 48(1):1–42, July 2015. DOI: 10.1145/2785733.

[21] Erik Miehling, Mohammad Rasouli, and Demosthenis Teneketzis. A POMDP approach to the dynamic defense of large-scale cyber networks. *IEEE Transactions on Information Forensics and Security*, 13(10):2490–2505, 2018. DOI: 10.1109/TIFS.2018.2819967.

[22] MITRE Corporation. Playbook for threat modeling medical devices, Nov 2021.

[23] Viraaji Mothukuri, Prachi Khare, Reza M. Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, and Gautam Srivastava. Federated-learning-based anomaly detection for iot security attacks. *IEEE Internet of Things Journal*, 9(4):2545–2554, 2022. DOI: 10.1109/JIOT.2021.3077803.

[24] Yazan Otoum, Yue Wan, and Amiya Nayak. Federated transfer learning-based IDS for the Internet of medical things (IoMT). In *2021 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, 2021. DOI: 10.1109/GCWkshps52748.2021.9682118.

[25] Joseph R. Rose, Matthew Swann, Gueltoum Bendiab, Stavros Shiaeles, and Nicholas Kolokotronis. Intrusion detection using network traffic profiling and machine learning for IoT. In *7th IEEE International Conference on Network Softwarization — NetSoft, SecSoft workshop*, pages 409–415. IEEE, June 2021. DOI: 10.1109/NetSoft51509.2021.9492685.

[26] Alireza Shameli-Sendi and Michel Dagenais. ORCEF: Online response cost evaluation framework for intrusion response system. *Journal of Network and Computer Applications*, 55:89–107, 2015. DOI: 10.1016/j.jnca.2015.05.004.

[27] Alireza Shameli-Sendi, Naser Ezzati-Jivan, Masoume Jabbarifar, and Michel Dagenais. Intrusion response systems: Survey and taxonomy. *International Journal Computer Science Network Security*, 12(01):1–14, 2012.

[28] Robert Shire, Stavros Shiaeles, Keltoum Bendiab, Bogdan Ghita, and Nicholas Kolokotronis. Malware squid: a novel iot malware traffic analysis framework using convolutional neural network and binary visualisation. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pages 65–76. Springer, 2019. DOI: 10.1007/978-3-030-30859-9_6.

[29] Nattaruedee Vithanwattana, Gayathri Karthick, Glenford Mapp, and Carlisle George. Exploring a new security framework for future healthcare systems. In *2021 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, 2021. DOI: 10.1109/GCWkshps52748.2021.9681967.

[30] Yu-Sung Wu, Bingrui Foo, Yongguo Mei, and Saurabh Bagchi. Collaborative intrusion detection system (CIDS): A framework for accurate and efficient IDS. In *19th Annual Computer Security Applications Conference — ACSAC*, pages 234–244. IEEE, 2003. DOI: 10.1109/CSAC.2003.1254328.