

Fortifying industrial cybersecurity: a novel industrial internet of things architecture enhanced by honeypot integration

Oumaima El Kouari¹, Saiida Lazaar¹, Tarik Achoughi³

¹Mathematics, Computer Science and Applications Team, National School of Applied Sciences-ENSA of Tangier, Abdelmalek Essaadi University, Tetouan, Morocco

²National Institute of Applied Sciences, Lyon University, Lyon, France

Article Info

Article history:

Received Apr 17, 2024

Revised Aug 25, 2024

Accepted Sep 3, 2024

Keywords:

Cyber-attacks

Honeypot

Industrial internet of things

Industry 4.0

Intrusion detection system

Threat intelligence

ABSTRACT

The industrial internet of things (IIoT) has significantly transformed the industrial sectors by connecting devices, machines, and systems to enhance automation, efficiency, and decision-making. However, the increased interconnectivity also poses significant security challenges because IIoT devices control critical infrastructures and processes. Our work presents an implementation of a robust industrial cybersecurity strategy with a segmented network architecture, collaborative efforts between information technology (IT) and operational technology (OT) teams for enhanced resilience and effectiveness, and vertical honeypots across all Industry 4.0 levels integrated with Wazuh for log transmission and proactive threat response, alongside Snort intrusion detection system (IDS) monitoring network traffic. Additionally, we reinforce our architecture by Wazuh with Elasticsearch and Kibana as a security information and event management solution, facilitating data analysis and compliance enforcement through custom rulesets and cybersecurity threat intelligence (CTI) integration, with automatic updates for continuous adaptation against emerging threats.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Oumaima El Kouari

Mathematics, Computer Science and Applications Team, National School of Applied Sciences-ENSA of Tangier, Abdelmalek Essaadi University

Tetouan, Morocco

Email: oumaima.elkouari@gmail.com

1. INTRODUCTION

Industrial internet of things (IIoT), refers to the network of interconnected devices, sensors, machines, and systems within industrial environments such as manufacturing plants, power plants, and logistics facilities [1]. IIoT leverages the power of internet connectivity to enable the exchange of data and communication between these devices, leading to increased automation, operational efficiency, and better decision-making. In addition to this, IIoT specifically focuses on the application of internet of things (IoT) technologies in industrial sectors such as manufacturing, energy, transportation, and agriculture. IIoT aims to improve industrial processes, efficiency, and productivity by leveraging IoT technologies. It involves connecting machines, equipment, sensors, and other industrial devices to the internet to gather data, monitor performance, enable predictive maintenance, optimize operations, and facilitate intelligent decision-making in industrial settings. IIoT combines a collection of smart devices and sensors that are embedded within industrial equipment, capturing data such as temperature, pressure, vibration, energy consumption, and more. The IIoT relies on robust and secure communication networks, encompassing wired connections, wireless protocols (such as Wi-Fi, Bluetooth, Zigbee, or cellular networks), and specialized industrial communication protocols (like Modbus or OPC-UA), to facilitate seamless data exchange between devices, sensors, and backend systems.

IIoT systems often leverage cloud computing platforms for storing, processing, and analyzing the vast amount of data generated by connected devices, benefiting from scalability, accessibility, and advanced analytics capabilities. Through applying advanced algorithms and artificial intelligent (AI) techniques, IIoT enables the analysis of massive volumes of data, unveiling patterns, trends, and anomalies, thereby enabling predictive maintenance, real-time decision-making, and optimization of industrial processes. In certain scenarios, edge computing devices are employed to process data locally, closer to the source, reducing latency and enabling real-time responses for time-critical applications. The increasing digitization and connectivity in industrial sectors, driven by IIoT, have revolutionized operations, introducing efficiencies and automation. This enhanced connectivity also amplifies cyber risks, as IIoT devices become potential targets for cyber threats [2].

Security is a paramount concern in IIoT, necessitating the implementation of encryption, access control mechanisms, secure protocols, and regular updates to safeguard data, devices, and networks from cyber threats inherent in industrial operations. Therefore, it is even more important to protect the interconnected devices, data, and systems from unauthorized access, data breaches, cyber-attacks, and other potential threats. As IIoT devices often control critical infrastructure and processes, ensuring their security is of paramount importance to maintain operational integrity and prevent disruptions.

To address these challenges, it is crucial to develop new methods for detecting and rejecting attacks. Traditional defenses like firewalls and antivirus software are reactive and need updates to keep up with new threats, leaving networks vulnerable to zero-day exploits that have not been publicly disclosed yet. The rise of “bring your own device” policies and social engineering has made old-fashioned perimeter defenses less effective. With operational technology (OT) and information technology (IT) merging, these threats now extend to IIoT too. Honeypots, systems designed solely to attract and capture attacks, offer a promising solution. Unlike reactive security measures, honeypots take a proactive approach, enticing attackers to reveal their tactics and vulnerabilities. While deploying honeypots requires careful consideration to avoid legal issues like entrapment, they've proven their worth by uncovering new threats, including four zero-day exploits.

The fact that honeypots are very helpful in regular computer systems inspired researchers to try using them in industrial systems too. To this aim, we have proposed an implementation of a robust industrial cybersecurity strategy based on honeypots involves several key elements. The main contributions of our work can be summarized as follows: i) A strategy that incorporates a vertical honeypot concept across all Industry 4.0 levels. This approach provides valuable insights into potential threats and enhances the overall security posture of the organization; ii) Collaborative efforts between IT and OT teams for enhanced resilience and effectiveness; iii) Automated incident response to fortify the system's resilience; iv) Seamless integration Wazuh, Elasticsearch and Kibana as a security information and event management (SIEM) solution, facilitating data analysis; and v) First to use threat intelligence for threat classification in Industrial control system (ICS).

The rest of the present work performed in this paper is categorized into the following sections: section 2, a background of the paper, summarizing the research context. In section 3, a summary of related researches. In section 4, we present our proposed work and the architecture of the system. In section 5, discusses the related work and our proposed architecture. In section 6, we concluded the presented work.

2. BACKGROUND

2.1. IIOT and Industry 4.0

The industrial landscape is undergoing a revolutionary shift with the advent of IIoT and Industry 4.0. IIoT involves integrating sensors, devices, and machinery in industrial settings to create interconnected systems that collect data and facilitate real-time monitoring, analysis, and remote control. This results in increased efficiency, predictive maintenance, and better decision-making. Industry 4.0, initiated by the German government in 2010, combines cyber-physical systems, cloud computing, big data analytics, and artificial intelligence (AI) to transform manufacturing. Its goal is to create “smart factories” where machines, processes, and people are interconnected, leading to autonomous production, optimized supply chains, and highly customizable products. Together, IIoT and Industry 4.0 drive the digital transformation of industries, unlocking higher productivity, flexibility, and competitiveness. However, they also present challenges in terms of security, data privacy, and the need for workforce reskilling [3].

2.2. Cybersecurity challenges in Industry 4.0

In the industrial sector, cybersecurity challenges are significant and diverse. One major challenge is the convergence of IT and OT systems. IT systems focus on data processing and storage, while OT systems control physical processes like manufacturing or power generation. Integrating these systems introduces new vulnerabilities and requires specialized security measures.

Operational disruption is another concern. Cyberattacks on industrial systems can disrupt critical operations, leading to production downtime, equipment damage, or even safety hazards. Unlike in traditional

IT environments, these disruptions can have direct physical consequences. The complexity of industrial systems is also a challenge. Industrial environments consist of interconnected systems with diverse technologies and protocols. Managing cybersecurity across these heterogeneous environments requires specialized knowledge and tools. Supply chain vulnerabilities are another concern. Industrial organizations rely on a network of suppliers and vendors for equipment and services. Cyberattacks targeting these partners can indirectly affect industrial systems, making it challenging to assess and manage cybersecurity risks across the entire ecosystem [4].

Compliance with regulations and standards adds another layer of complexity. Industrial sectors are subject to various cybersecurity regulations and standards, such as national institute of standards and technology (NIST) or international organization for standardization (ISO) standards. Ensuring compliance while maintaining effective cybersecurity practices is a continuous challenge.

2.3. IIoT attacks

IIoT provides various advantages, such as improved monitoring, predictive maintenance, and increased efficiency. However, it also presents new security challenges. As IIoT devices are often interconnected across extensive industrial networks, they become vulnerable to malicious actors who may aim to disrupt operations, steal sensitive data, or cause harm. Consequently, IIoT environments face a growing risk of cyberattacks that are specifically designed to exploit their unique characteristics. These IIoT attacks can come in different forms, and each of them poses significant threats to critical infrastructure and industrial operations. Some of the common types of IIoT attacks include:

- APT attacks: advanced persistent threat (APT) attacks are a particularly dangerous form of cyberattack commonly employed against government and corporate entities. These attacks, as described in various studies, involve sophisticated methods aimed at specific targets, persisting over extended periods while evading detection due to their complexity. APT attacks demonstrate resilience by continually pursuing their objectives, adapting to defensive measures, and maintaining their interaction levels to achieve their goals over time [5].
- Denial-of-service (DoS) attacks: In a DoS attack, the attacker overwhelms a targeted IIoT system or device with a flood of traffic, rendering it unable to function properly. This can disrupt critical operations and cause financial losses [6].
- Man-in-the-middle (MitM) attacks: In a MitM attack, an attacker intercepts and alters the communication between IIoT devices or between devices and the central control system. This allows the attacker to eavesdrop on sensitive information, manipulate data, or inject malicious commands [7], [8].
- Malware: pertains to a cybersecurity incident in which malicious software, commonly referred to as malware, is deliberately introduced into IIoT systems with the explicit intention of causing disruption, damage, data theft, or unauthorized access to critical industrial processes, devices, or networks. Prevalent categories of malware employed within IIoT encompass ransomware, botnets, worms, trojans, and spyware [9], [10].
- Phishing attacks: It is a type of cyberattack in which malicious actors use deception to manipulate individuals or employees within industrial organizations, with the goal of gaining unauthorized access to critical systems, sensitive data, or control over industrial devices. Typically, these attacks take the form of phishing emails, messages, or websites that mimic legitimate and trustworthy sources to deceive their targets [11], [12].
- Authentication attacks: Authentication serves as a pivotal security component, ensuring that only authorized users or devices gain access to specific resources or perform designated actions within the IIoT environment. Authentication attacks involve malicious actions targeted at compromising or bypassing the authentication mechanisms of IIoT devices or systems. When authentication is compromised, it opens the door for attackers to gain unauthorized entry to industrial devices, networks, or sensitive data. This may lead to consequential outcomes, including operational disruptions, data breaches, and safety hazards [13].

2.4. Honeypot

A honeypot is a computer system that imitates a real target, complete with applications and data. It is purposely designed with security vulnerabilities to attract and deceive cybercriminals. Its primary objective is to entice attackers and keep an eye on their interactions with phony systems. The ultimate aim of a honeypot is to monitor hackers' conduct, collect valuable data for in-depth analyses, and to prevent future attacks. This helps to gain better knowledge of existing threats and facilitates the development of more secure systems. Honeypots are strategically placed in the network to make it seem vulnerable and defenseless. However, in reality, they are isolated and closely monitored [14]. Honeypots can be classified according to three criteria: implementation environment (research or production honeypot), level of interaction between the intruder and the system (low-interaction, medium-interaction and high interaction), and resource level

(physical or virtual honeypot). These classification criteria make it easier to understand their operations and uses when it comes to planning the implementation of a honeypot inside a network [15], [16].

3. RELATED WORK

Lopez-Morales *et al.* [17] suggested an high-interaction, flexible, malware-collecting honeypot called HoneyPLC for ICS supporting a wide range of programmable logic controller (PLC) models and suppliers. It simulates transmission control protocol/internet protocol (TCP/IP), hypertext transfer protocol (HTTP), simple network management protocol (SNMP), and S7comm protocols. To evaluate HoneyPLC, the authors used multiple tools for profiling, scanning and interaction with HoneyPLC. The results have shown that HoneyPLC exhibits a high level of camouflaging. They deployed HoneyPLC on Amazon web services (AWS), capturing numerous intriguing interactions over the Internet. This demonstrated that attackers are indeed targeting ICS systems and proved that HoneyPLC can effectively engage and deceive these attackers while collecting data samples for future analysis.

Pliatsios *et al.* [18] introduces a novel ICS honeypot based on the Conpot framework, designed to emulate physical ICS devices and attract potential attackers for security analysis. Focusing on the power generation department of a hydropower plant, the findings extend to transportation and infrastructure advantages. The system creates honeypots by mimicking actual ICS through virtual machines, replicating real devices and traffic. The honeypot emulates real remote terminal unit (RTU) devices using the Modbus protocol, configuring itself from Modbus traffic capture files and responding to attackers with realistic data. The proposed architecture includes virtual and real human-machine interface (HMI) panels, enhancing the network infrastructure's realism.

Shrivastava *et al.* [19] focus on detecting attacks on IoT devices using the Cowrie honeypot. The honeypot captures all interactions in log files and categorizes them as malicious, SSH attack, XOR DDoS attack, spying, suspicious, or clean. Shrivastava *et al.* used the support vector machine (SVM) algorithm to classify attacks and compared its performance with other supervised algorithms such as random forest, naive Bayes, and J48 decision tree. To ensure reliable classifier evaluations, they used a 10-fold cross-validation method. They analyzed the commands used by attackers through honeypot forensics to confirm attempted attacks on a system. The experimental results showed that SVM achieved a maximum accuracy of 97.39%.

In an article by Tarewal *et al.* [20], a technique for optimizing near-end strategies for IIoT intrusion detection was presented. The technique utilized a deep reinforcement learning (DRL) algorithm to merge observation and decision-making capabilities for efficient detection of various cyber-attacks on the IIoT. When combined with deep learning (DL) algorithms, the DRL-intrusion detection system proved highly effective at identifying intrusions. After conducting numerous experiments on a publicly accessible IIoT data set, the proposed system detected 99% of network attacks. Furthermore, the system's accuracy rate was 0.9%. Based on various DL models, the system's performance indicators, including accuracy, precision, and recall rate, were superior.

Anirudh *et al.* [21] have developed a system to combat DoS attacks on IoT networks. This system involves implementing a honeypot with a verification system to analyze and gather information about the attack. All requests are sent to the intrusion detection system (IDS) [22], and malicious requests are directed toward the honeypot to collect information about the attack's nature, which is then logged into a database. Legitimate requests are let into the server via IDS. If the attacker sends malicious packets repeatedly with the same IP address saved in the database, the IDS blocks the attacker from further communication with the network. If not, the IDS allows the traffic to pass through the network. The proposed model has been compared to another model without a honeypot, and the results have shown that the former works better.

4. METHOD

The architecture comprises four levels of cybersecurity measures and adapted with Industry 4.0, the detailed architecture is shown in Figure 1. In the foundational levels (levels 1 and 2), our strategy focuses on emulating PLC/RTU/HMI systems using Conpot [23] which is a low-interactive honeypot that mimics Smart Grid processes, aiding in cybersecurity defense. Its ease of implementation and support for protocols like Modbus make it attractive. Conpot's logging system tracks attacker attempts via HTTP, SNMP, and Modbus, enhancing threat detection capabilities. By meticulously crafting protocol stacks and interfaces templates, Conpot mirrors real hardware, providing a robust defense mechanism. We deploy Conpot as a sensor across the network, meticulously logging attacker attempts via HTTP, SNMP requests, and Modbus communication. Additionally, we integrate Snort IDS to strengthen our defenses by monitoring network traffic. We smoothly connect Conpot and Snort with the Wazuh agent to enrich and send logs straight to the Wazuh manager (level 4) for handling incidents and detecting threats.

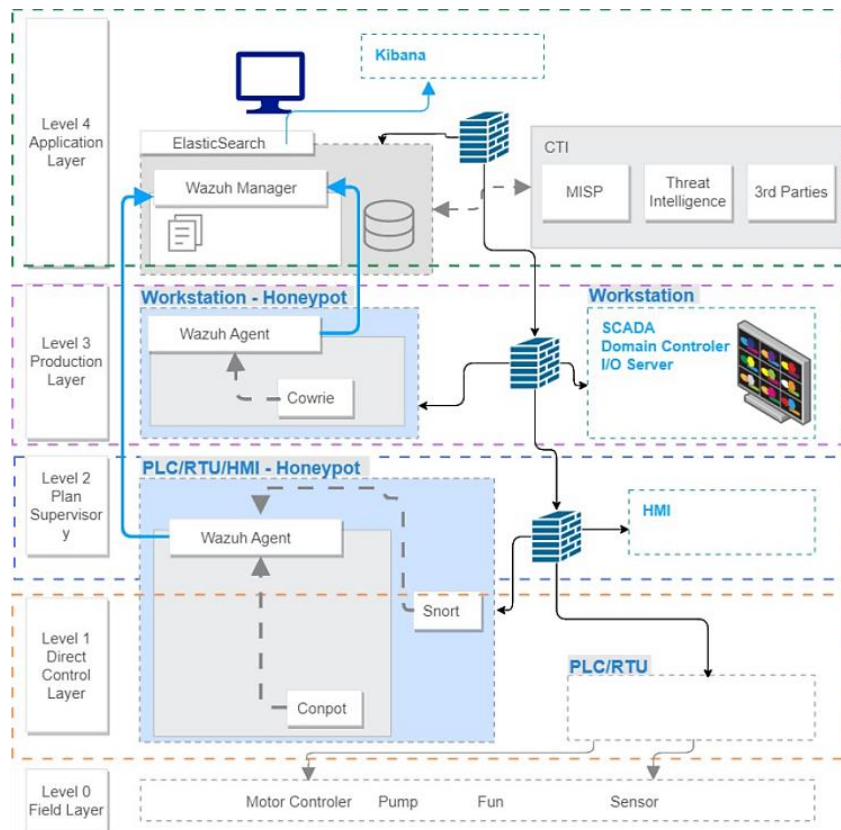


Figure 1. An overview of the proposed architecture

At level 3, we use Cowrie honeypot technology [24], capturing a spectrum of SSH server vulnerabilities and misconfiguration. The main objective is to capture and log all communicated sessions, including login attempts, executed commands, and file transfers. Cowrie's session logging captures all comprehensive data, including IP addresses, malware samples, and attack patterns. Additionally, we integrate Conpot with Wazuh agent [25] the same as we did at levels 1 and 2 to send logs directly to Wazuh manager.

At level 4, we employ a robust SIEM/security orchestration, automation and response (SOAR) solution, integrating Wazuh manager with Elasticsearch [26], Kibana and cyber threat intelligence (CTI) platform. Wazuh serves as the central hub for agent management, data collection, and analysis, offering a user-friendly dashboard for comprehensive event visualization. By using custom rulesets to extract many indicators of compromise (IOCs) [27] and coupled with CTI integration through platforms like malware information sharing platform (MISP) [28], to enrich our threat intelligence industry landscape beside of enabling proactive threat detection and response. In addition to this, leverage Wazuh's MITRE ATT&CK module by aligning with many standards such as NIST, ensuring regulatory compliance and bolstering our security posture. Finally, automatic rule list updates from threat intelligence outputs streamline response efforts, enabling continuous adaptation and mitigation against emerging threats.

Figure 2 describes the flowchart of the CTI industry honeypot. When a new connection detected to honeypot, the system first checks if IOC exist in the local extended detection and response (XDR) database (levels 1, 2, and 3). If it found, it proceeds with further checks. Otherwise, it triggers a security incident at level 4. The system then extracts threat indicators and checks if they have already been captured. If so, it executes preconfigured playbooks for actions such as applying firewall rules, triggering IoT sensor alerts. If we have not captured the threat indicator, we move on to the next step. We enrich our CTI platform by looking up information on indicators such as IP addresses, MD5, and other types of hashes. The process automatically contribute with multiple external platform such as MISP, OpenCTI, VirusTotal [27]. After gathering this information, we use custom scoring to make a decision based on IOC reputation. Either we feed the new values into our blacklist and then execute a preconfigured playbook, then we check if the IOC already exists. if the last custom IOC already captured, we enrich with more details to multiple CTI network/platform/community. However, if the last indicator has not captured yet, we treat it as a new case and feed the IOC to the connected CTI system. In both cases, we enrich the IOC with additional details by passing it through the Enrichment process using the CTI Platform and enforcing community collaboration.

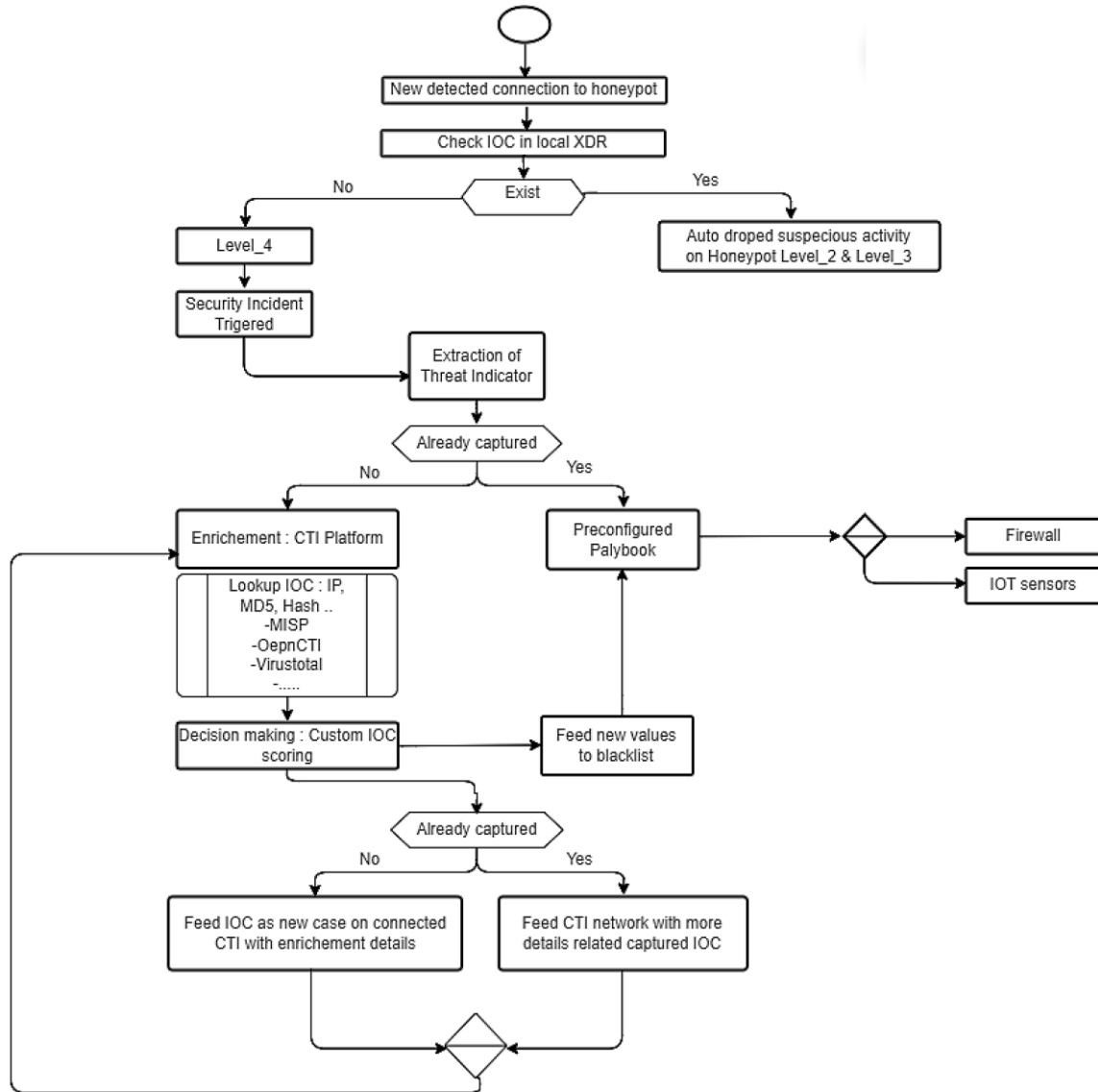


Figure 2. Flowchart CTI industry honeypot

5. RESULTS AND DISCUSSION

After analyzing the Table 1, we notice that:

- Honeypot as a Service allows businesses to leverage cutting-edge threat intelligence without the need for extensive in-house expertise or resources. This results in improved threat detection and response capabilities, fostering a more resilient cybersecurity posture.
- The integration of honeypots into industry's cybersecurity strategy not only helps in mitigating risks but also in optimizing resource allocation by reducing the false positives.
- When comparing deployment scales, it is clear that each approach has its strengths and weaknesses. The AWS test environment with Ubuntu hosts offers flexibility and scalability but may lack the realism of physical deployments. The VM environment provides a controlled setting to emulate an entire ICS infrastructure, which is great for comprehensive testing but might not capture all real-world nuances. Deploying in an information security lab for 40 days gives focused data collection but is limited in scope and duration. Using real IIoT data from the U.S. department of energy adds authenticity but could be constrained by data privacy issues. Simulating IoT environments across multiple industry levels and cloud computing areas offers a broad and detailed perspective, making it the best option. It combines realism with extensive coverage, ensuring a thorough and versatile analysis of potential threats across various settings.

- Among these capabilities, advanced real-time threat detection and monitoring inside ICS used in our work is noticeable as particularly crucial for protecting critical infrastructure. This capability ensures that any threats within industrial systems are identified immediately, allowing for swift response and mitigation. It provides essential oversight and protection against potential disruptions or compromises that could impact operations. This proactive approach to monitoring and detecting threats within ICS environments is essential for maintaining robust cybersecurity defenses.
- Each of these threat analysis methods has its strengths, but some are more comprehensive than others. Analyzing interactions with external agents and tools, and collecting attack data, is good for understanding sophisticated attack techniques. Gathering information about attackers' origins and methods provides useful context but might not always lead to actionable insights. Analyzing honeypot data to understand attack behaviors and using reinforcement learning to improve decision-making are both effective but can be complex and resource-intensive. The approach of intercepting traffic flow for real-time threat response and strengthening firewall rules is noticeable as the best. This method not only identifies threats quickly but also takes immediate action to mitigate them, offering the most practical and immediate protection.
- Among the various response mechanisms, our proposed architecture is noticeable as the best because it offers the most comprehensive and proactive approach to security. It not only detects threats in real-time but also automatically takes action to block and mitigate them from the next attack, providing immediate protection without requiring manual intervention. This is more efficient and faster compared to merely enhancing firewall and IDS functionalities or using verification systems to block repeat offenders. Optimizing intrusion detection strategies using feedback is useful but still requires ongoing adjustments and human oversight. Therefore, a self-automated approach offers the most comprehensive and timely defense by automation way against attacks.
- Our work is the first to deploy threat intelligence for threat classification in ICS. This integration further enhances cybersecurity effectiveness. By leveraging threat intelligence platforms, organizations can proactively identify emerging threats, anticipate attack patterns, and fortify defenses against sophisticated cyber adversaries, thereby bolstering the resilience of IIoT ecosystems.
- Despite the numerous advantages presented by our proposed architecture, its deployment in professional contexts, particularly in the implementation of automated firewall rules within industrial settings, necessitates meticulous consideration. The associated risks warrant evaluation from both qualitative and quantitative perspectives. When issuing rejections for IOCs such as IP addresses, hashes, domains, or URLs, it is imperative to proceed with caution. Incorrect rejection actions can lead to significant operational and business-related issues.

Figure 3 shows count of records for SSH attack per day. The results shows that our architecture demonstrated high efficacy, successfully detecting a significant number of attacks and thereby showcasing its robust detection rates. The remaining results will be presented in the forthcoming paper.

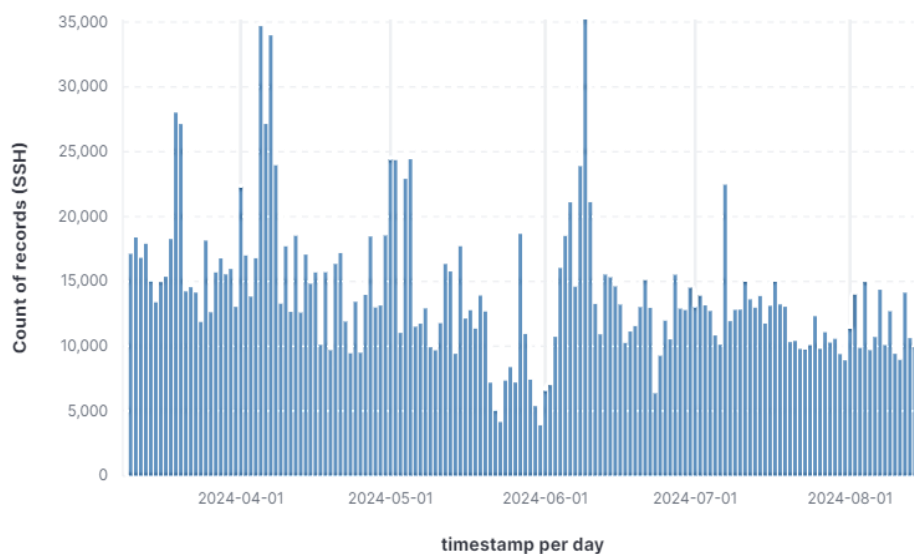


Figure 3. Graph of count of records for SSH attack against timestamp per day

Table 1. Comparative table of related work

Work	[17]	[18]	[19]	[20]	[21]	Our work
Objective	High-interaction honeypot for ICS that can capture data for recent and sophisticated attack techniques by simulating step-by-step protocol interactions and collecting detailed attack data	An interactive, proof-of-concept ICS honeypot that emulates a physical ICS device, and assess its effectiveness in a real-life hydro power plant scenario	Capture attacks on IoT devices using Cowrie and classify them using various ML algorithms	Develop an efficient IDS for the ICS using DRL	Propose a honeypot model for mitigating DoS attacks launched on IoT devices	Improve ICS security by deploying honeypots and relating with cybersecurity threat intelligence
Industry focus	ICS	Critical infrastructure, specifically smart grid infrastructure and hydro power plants	IoT environment	IIoT	IoT networks	General ICS, IIoT, Industry 4.0
Honeypot type	High-interaction	Interactive, proof-of-concept honeypot	Medium-interaction honeypot	Not explicitly mentioned, focuses on intrusion detection system	Honeypot	High-interaction and low-interaction
Deployment scale	AWS test environment with local deployments on Ubuntu 18 LTS hosts	Virtual machine (VM) environment to emulate the entire organization's ICS infrastructure	Classifies attacks into categories	Utilizes real IIoT data sets from the U.S. Department of Energy Ridge National Laboratory	Simulated IoT environment	Levels 1,2,3 and 4 into Industry 4.0 beside of cloud computing area
Detection capabilities	Engage external agents and tools, maintain covertness against state-of-the-art reconnaissance tools, and handle detailed protocol simulations	Able to attract various external attacks by emulating any smart grid device using Modbus	Captures interactions, in log files, analyzes, attacker commands	Efficient detection of various network assaults using RL combined with LightGBM for feature selection	Diverts DoS attacks to the honeypot, captures attacker information	Advanced realtime threat detection and monitoring inside ICS
Threat analysis	Analyzes interactions with external agents and tools, collects attack data to study sophisticated attack techniques	Gathers valuable information about the origin of attackers, employed methods, and attack patterns	Analyzes honeypot data to understand attack behaviors	Uses RL to improve decision-making ability and detect complex network attacks	Analyzes attacker behavior to improve security measures	Intercept traffic flow for threat classification, realtime threat response to strengthen firewall rules
Response mechanism	Not explicitly mentioned	Not explicitly mention	Enhances firewall and IDS functionalities	Optimizes intrusion detection strategies using feedback from the environment	Verification system to block repeat offenders	Self-automated detect and response protocol
Integration with existing security systems	Supports Siemens PLC Profiles, Allen-Bradley, and ABB PLCs for comprehensive profiling and simulation	Uses Conpot framework to emulate realistic ICS devices	Can be used to strengthen existing firewall and IDS systems	LightGBM for feature selection and PPO2 algorithm for intrusion detection	Works alongside IDS to divert and capture attack	Seamless integration with SIEM, IDS/IPS, CTI and firewall
Unique contribution	Provides a high-interaction honeypot for ICS with detailed protocol simulation and attack data collection	First implementation of an interactive ICS honeypot for hydro power plants using Conpot	Includes ML module to classify attacks and provides deep insights into attacker behavior	Combines DL and RL for an efficient IDS	Proposes a practical implementation of honeypots for IoT security	First to use threat intelligence for threat classification in ICS and auto-response mechanism

6. CONCLUSION





The rapid increase in new cyber threats in the era of IIoT necessitates advanced and fully automated analysis techniques. Traditional tools are too limited, especially with large amounts of data or new attack types. In this paper, we proposed a new architecture to improve ICS security by deploying honeypots and relating with cybersecurity threat intelligence. The proposed architecture across all the Industry 4.0 levels with self-automated detect and response protocol and seamless integration with SIEM, IDS/IPS, CTI and

firewall. Our results showed the effectiveness and feasibility of the proposed architecture. Notably, the role played by the honeypot is crucial in enhancing detection capabilities, as it successfully diverts potential threats and gathers valuable data to strengthen the overall security framework. As future extension, we aim to implement and execute a demonstration scenario of the proposed architecture in a real-world industrial environment. This would provide valuable insights into the effectiveness of our work.





REFERENCES

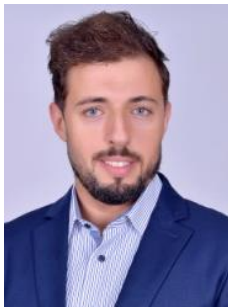
- [1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
- [2] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, May 2021, doi: 10.1109/TII.2020.3023507.
- [3] A. Karmakar, N. Dey, T. Baral, M. Chowdhury, and M. Rehan, "Industrial internet of things: a review," in *2019 International Conference on Opto-Electronics and Applied Optics (Optronix)*, Mar. 2019, pp. 1–6, doi: 10.1109/OPTRONIX.2019.8862436.
- [4] M. Humayun, N. Jhanjhib, M. N. Talib, M. H. Shahd, and G. Sussendran, "Industry 4.0 and cyber security issues and challenges," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, 2021.
- [5] K. Xing, A. Li, R. Jiang, and Y. Jia, "A review of APT attack detection methods and defense strategies," in *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*, Jul. 2020, pp. 67–70, doi: 10.1109/dsc50466.2020.00018.
- [6] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino, and S. E. Quincozes, "Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4569–4578, Mar. 2021, doi: 10.1109/ijot.2020.3028652.
- [7] A. Esfahani *et al.*, "An efficient web authentication mechanism preventing man-in-the-middle attacks in Industry 4.0 supply chain," *IEEE Access*, vol. 7, pp. 58981–58989, 2019, doi: 10.1109/access.2019.2914454.
- [8] O. Eigner, P. Kreimel, and P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," in *2016 International Conference on Software Security and Assurance (ICSSA)*, Aug. 2016, pp. 64–69, doi: 10.1109/icssa.2016.19.
- [9] A. Marzano *et al.*, "The evolution of Bashlite and Mirai IoT BotNets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2018, pp. 00813–00818, doi: 10.1109/iscc.2018.8538636.
- [10] A. Wani and S. Revathi, "Ransomware protection in IoT using software defined networking," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3166–3175, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.
- [11] G. A. Abdalrahman and H. Varol, "Defending against cyber-attacks on the internet of things," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, vol. 4, pp. 1–6, doi: 10.1109/isdfs.2019.8757478.
- [12] O. El Kouari, H. Benaboud, and S. Lazaar, "Using machine learning to deal with phishing and spam detection: an overview," in *Proceedings of the 3rd International Conference on Networking, Information Systems and Security*, Mar. 2020, vol. 2014, pp. 1–7, doi: 10.1145/3386723.3387891.
- [13] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 795–800, doi: 10.1109/wf-iot.2015.7389155.
- [14] W. Li and P. Wang, "Two-factor authentication in industrial internet-of-things: attacks, evaluation and new construction," *Future Generation Computer Systems*, vol. 101, pp. 694–708, Dec. 2019, doi: 10.1016/j.future.2019.06.020.
- [15] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security," *Proceedings of The 2011 International Conference on Communication, Computing and Security*, 2011, doi: 10.1145/1947940.1948065.
- [16] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021, doi: 10.1109/comst.2021.3106669.
- [17] E. López-Morales *et al.*, "HoneyPLC: a next-generation honeypot for industrial control systems," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2020, vol. 5, pp. 279–291, doi: 10.1145/3372297.3423356.
- [18] D. Pliatsios, P. Sarigiannidis, T. Liatifis, K. Rompolos, and I. Siniosoglou, "A novel and interactive industrial control system honeypot for critical smart grid infrastructure," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Sep. 2019, pp. 1–6, doi: 10.1109/camad.2019.8858431.
- [19] R. K. Shrivastava, B. Bashir, and C. Hota, "Attack detection and forensics using honeypot in IoT environment," in *Distributed Computing and Internet Technology*, Springer International Publishing, 2018, pp. 402–409.
- [20] S. Tharewal, M. W. Ashfaq, S. S. Banu, P. Uma, S. M. Hassen, and M. Shabaz, "Intrusion detection system for industrial internet of things based on deep reinforcement learning," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–8, Mar. 2022, doi: 10.1155/2022/9023719.
- [21] M. Anirudh, S. A. Thilleeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Jan. 2017, vol. 2, pp. 1–4, doi: 10.1109/icccsp.2017.7944057.
- [22] A. Chhaybi and S. Lazaar, "System call frequency analysis-based generative adversarial network model for zero-day detection on mobile devices," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 2, pp. 1969–1978, Apr. 2024, doi: 10.11591/ijece.v14i2.pp1969-1978.
- [23] S. Gokhale, A. Dalvi, and I. Siddavatam, "Industrial control systems honeypot: A formal analysis of Conpot," *International Journal of Computer Network and Information Security*, vol. 12, no. 6, pp. 44–56, Dec. 2021, doi: 10.5815/ijcnis.2020.06.04.
- [24] M. Oosterhof, "Cowrie," *GitHub*. <https://github.com/cowrie/cowrie> (accessed Apr 17, 2024).
- [25] S. Stanković, S. Gajin, and R. Petrović, "A review of Wazuh tool capabilities for detecting attacks based on log analysis," in *International Conference IcETRAN*, 2022, no. 6, pp. 1–5.
- [26] P. P. Bavaskar, O. Kemker, and A. K. Sinha, "A survey on: log analysis with elk stack tool," *International Journal of Research and Analytical Reviews (IJRAR)*, vol. 6, no. 4, pp. 965–968, 2019.
- [27] M. J. Haber and D. Rolls, "Indicators of compromise," in *Identity Attack Vectors*, Apress, 2019, pp. 103–105.
- [28] B. Stojkovski, G. Lenzini, V. Koenig, and S. Rivas, "What's in a cyber threat intelligence sharing platform?: a mixed-methods user experience investigation of MISP," in *Annual Computer Security Applications Conference*, Dec. 2021, vol. 11, pp. 385–398, doi: 10.1145/3485832.3488030.





BIOGRAPHIES OF AUTHORS

Oumaima El Kouari     Ph.D. student at National School of Applied Sciences of Tangier, Abdelmalek Essaâdi University, Morocco. She is a member of Mathematics, Computer Science and Applications Team (ERMIA). In 2019, she obtained a master's degree in cyber security and cyber criminality from the National School of Applied Sciences of Tangier, Morocco. Her interests include IoT and IIoT security, honeypots and machine/deep learning. She can be contacted at email: oumaima.elkouari@gmail.com.



Saiida Lazaar     holds a Ph.D. in applied mathematics from Aix Marseille I University in France and currently serves as a full professor at Abdelmalek Essaadi University in the Department of Mathematics and Computer Sciences, at ENSA of Tangier, Morocco. With extensive expertise in the field of cyber security, she has played a role as the head of the Master's program in cyber security and cybercrime. Her track record includes notable research positions such as CNRS and IFP in France, as well as ONDRAF in Belgium. Throughout her career, she has demonstrated an exceptional passion for advancing the field of cybersecurity. She can be contacted at email: slazaar@uae.ac.ma.



Tarik Achoughi     is an experienced cybersecurity architect. with more than 15 years of dedicated expertise as a practitioner and researcher in the security field. Tarik has worked with customers of different sizes and types to build, enhance, and manage best practice cybersecurity programs. He possesses a master's degree in cyber security conferred by INSA Lyon University, France. His practical experience includes engagements addressing technical, operational and strategic cyber security consulting. He can be contacted at email: achoughi.tarik@gmail.com.