Cybersecurity Testing for Cobots

Tauheed Waheed[a], Eda Marchetti[b] and Antonello Calabrò[c]
CNR-ISTI Pisa, Italy

Keywords: IoT, Cobots, Cybersecurity Testing, Vulnerabilities.

Abstract: IoT (Internet of Things) rapid evolution and interconnected nature emphasize the urgent need for robust cybersecurity measures. Cybersecurity presents considerable risks and threats for the cobots (collaborative-robots) industry. Cyber attackers can leverage these weaknesses, potentially allowing unauthorized entry and compromising critical assets. The proposed CTF (Cybersecurity Testing Framework) framework emerges as a promising answer to these issues, providing an adaptable, robust, and thorough method for cobots cybersecurity assurance. Understanding why cybersecurity testing is needed for cobots industry and how cobots users interact with the system is vital, considering the changing landscape of cyber threats.CTF seeks to enhance cobots cybersecurity by leveraging available testing suites and adhering to regulatory standards. We aim to showcase our testing framework's effectiveness and potential uses by depicting a specific testing strategy to address vulnerabilities and cyber threats in cobots. The paper details the CTF theoretical foundation and critical features and presents its initial prototype to prove its suitability.

1 INTRODUCTION

Over the years, Information Technology's (IT) role has dramatically changed in both the social and work sectors. Recent studies have shown that 90% of users need an adequate level of confidence in the cybersecurity of their IoT systems or applications (Gemalto, 2023). However, the recent advent of collaborative robots, or cobots, in many industries has increased the speed of this process. The collaborative robots domain provides an environment of working in a shared, communal workspace with human workers to keep building the trust of humans in technology, particularly robots.

The collaborative robot is accountable for humble, repetitious duties in most applications, while a human employee completes more complicated tasks. Collaborative robots' uptime, precision, and repeatability improve human worker's problem-solving skills and intelligence.

Cobots are designed to collaborate and interact with humans in shared workspace, transforming traditional production processes and increasing human productivity in various industrial and commercial areas. Indeed, cobots have several benefits, such as greater productivity, adaptability, and security. In 2021, the collaborative market size comprised $701 Million, and it will increase to $2506.90 Million in 2030 at a growth rate of 15.2% as per the prognosis period. Moreover, there is pressure to fulfill industrial needs and explore innovative ways to carry out massive widespread integration among various stakeholders to resolve complex problems through collaborative robots.

However, when integrated into intricate cyber-physical systems and commercial and industrial environments, addressing the cybersecurity and trustworthiness issues surrounding their use is critical. Malicious actors may attempt to compromise system integrity, endanger public safety, or impede vital operations by taking advantage of flaws in cobot software, communication protocols, or physical interfaces. Conventional cybersecurity testing techniques might need to adequately reflect the complexity of cobots-infused environments despite helping evaluate traditional IT systems.

To address these challenges, the paper first provides an overview of the issue and challenge of cybersecurity testing in the cobots domain. It clarifies the cybersecurity risks and vulnerabilities unique to cobots, considering technical and human-centric factors. Then, it proposes a cybersecurity testing platform explicitly tailored for cobots, focusing on en-

[a] https://orcid.org/0009-0006-0489-7697
[b] https://orcid.org/0000-0003-4223-8036
[c] https://orcid.org/0000-0001-5502-303X

Waheed, T., Marchetti, E. and Calabrò, A.
Cybersecurity Testing for Cobots.
DOI: 10.5220/0013071000003825
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 20th International Conference on Web Information Systems and Technologies (WEBIST 2024)*, pages 449-456
ISBN: 978-989-758-718-4; ISSN: 2184-3252
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

hancing trustworthiness and security resilience for industrial collaboration scenarios. By integrating insights from robotic experts, testers, cybersecurity analysts, and cognitive psychology, the proposed platform aims to bridge the gap between technical cybersecurity assessments, thereby fostering a holistic understanding of cobots trustworthiness.

Current methods ignore testing, the consequence of cyberattacks, and affecting people's trust in cobot systems. Furthermore, because cobot deployments are dynamic, proactive and adaptive testing methodologies are needed to react quickly to new threats and vulnerabilities in cyber-attacks. Consequently, it is crucial to develop specialized cybersecurity testing methodology and framework suited to cobots and their networked ecosystem.

In its exploration, the paper overviews the following research questions (RQs):

RQ 1: Why is Cybersecurity Testing Critical for Cobots?

Specifically, we examine the damage caused by inadequate testing procedures for innovative technologies like cobots and the achievable mitigation techniques.

RQ 2: What Are the Current Solutions or Frameworks for Cobots Cybersecurity Testing?

In distinct, we scrutinize and evaluate the impact of the lack of testing and processes on the users' trustworthiness and cobots' cybersecurity of products used by companies, organizations, ordinary people, and governments.

RQ 3: What Are the Main Research Gaps?

We analyze current research trends in cobots cybersecurity testing to recognize the significant gaps and guarantee the development of secure, trustworthy, and sustainable services aligned with social, inclusiveness, legal requirements, and ethical values.

RQ 4: Which Could be a Possible Solutions?

Solutions for reducing uncertainty and increasing overall reliability, cybersecurity and trustworthiness must move in two technological and societal directions.

Considering the fragile nature of cybersecurity testing, we in Section 2 have presented the current cybersecurity testing strategies for cobots, and we analyze available solutions. Moreover, we have discussed the need for cybersecurity testing for cobots in Section 3. Then, we conceptualize and discuss our Cybersecurity Testing Framework for cobots in Section 4.

Then, Section 5 comprises of CTF architecture and its components. Moreover, it discusses our CTF's workflow and implementation details for cobots. Furthermore, the Section 6 conclusion and future work.

2 BACKGROUND AND RELATED WORK

Human-robot collaboration (HRC) is a fascinating field that explores the interaction between humans and robots as they work together to achieve shared goals. cobots are more straightforward to program and reconfigure for different tasks. Any team member can train a cobot, making them more accessible than traditional industrial robots, requiring specialized programming knowledge.

Cobot involves collaborative processes where human and robot agents cooperate to perform tasks. These tasks span various domains, including offices, space exploration, homes, hospitals, and manufacturing. Autonomous vacuum cleaners such as Whiz (Rindfleisch et al., 2022) are one of the many cases where cobots already impact various industries while improving employee satisfaction. To position this work in the state-of-the-art, this section provides an overview of the main recent proposals for the cybersecurity testing of cobots.

Considering the risk-oriented approaches to assessing the cybersecurity and safety of robotic systems, in (Abakumov and Kharchenko, 2023), researchers proposed a robotics security methodology, emphasizing combining various assessment techniques. The testing strategies involve Penetration Testing (PT), Faults and Vulnerabilities Injection Testing, Risk and Vulnerabilities Assessment, Attack Tree Analysis (ATA), and their combinations to assess the cybersecurity and safety of robotic systems. However, it lacks an adequate testing strategy or framework.

In developing a methodology for addressing security and safety simultaneously, the embedded Manufacturing Function Deployment (MFD) 4.0 design Cyber-Physical Production Systems (CPPS) and Human-Robot Collaboration (HRC) systems within the e Factories of the Future (FoF) (Caruana and Francalanza, 2023). It focuses on innovative technologies, comprises six steps, and includes tools like Hazard and Risk Assessments (Saf, 2024), Morphological Charts (Mor, 2024), and Risk Score Analysis (Kandasamy et al., 2020). The testing methodology is too generic and inadequate to prevent cyber-attacks within Industry 5.0 and modern-day disruptive technologies.

To assess the safety of industrial robotic systems and emphasise the importance of addressing vulnerabilities to prevent cyberattacks and ensure safety during operation, a proposal is presented din (Abakumov and Kharchenko, 2022). The methodology includes Intrusion Modes and Criticality Analysis (IMECA) analysis with penetration testing. However, It lacks transparent testing strategies and tools for assessing Robotic Systems (RS) cybersecurity and safety.

As the previous proposal in the work presented in (Abakumov and Kharchenko, 2022), penetration testing is also considered an essential part of assessing the cybersecurity and safety of industrial robotic systems. In this work, the authors focus on information gathering, scanning, IMECA, attack, countermeasures selection, and reporting. The researchers recommended using tools like Wireshark (Wir, 2024), Nmap (Nma, 2024), Metasploit (Met, 2024), and Burp Suite Professional (Bur, 2024) to conduct penetration testing. However, It lacks (Abakumov and Kharchenko, 2022) transparent testing strategies and tools for assessing Robotic Systems (RS) cybersecurity and safety.

Considering the more generic V&V (Verification and Validation) process, researchers in (Kanak et al., 2021) focus on designing, implementing, and evaluating methods and tools to reduce the cost and time of these activities. They propose automated systems enhance safety, cybersecurity, and privacy assessment but lack human-centricity while conducting these testing activities.

The potential of cobots to work alongside humans in the shared workspace has led to the development of innovative solutions (Thummapudi et al., 2024) in Industry 4.0. Finally, considering the important role of in rising automation and enhancing productivity, especially in Industry 5.0, the proposal of (Abishek et al., 2023) focuses on the role of cobots in enhancing productivity, the importance of cybersecurity, and the potential for future advancements in manufacturing through the integration of cobots and cybersecurity measures. However, it is recommended to pay more attention to cybersecurity concerns and how they connect to the system's safety. The researchers (Hollerer et al., 2021) have conducted a security evaluation of the Franka Emika Panda. For this particular cobot, potential vulnerabilities have been explored and how they could affect parameters critical to safety.

As evidenced by this overview of related work, even if there are proposals for improving cybersecurity in several application domains, there are still gaps in the integration of cobots and cybersecurity testing and the involvement of humans in the loop. As discussed in the rest of this paper, the evidence collected motivates the current proposal.

Even if not exhaustive, the above examples evidence that only integrated quality-control testing process, associated with certification procedures, guidelines, and round-breaking to conduct collaborative research, can solve cybersecurity criticalities (Heiding et al., 2023).

3 WHY IS CYBERSECURITY TESTING CRITICAL FOR COBOTS?

As highlighted in Section 2, cobots (Nahavandi, 2019) help pave the way for effective human-robotic operations alongside humans in an interactive workspace. Cybersecurity testing of cobots refers to assessing and evaluating the security measures, vulnerabilities, and potential risks associated with cobots. It involves thoroughly examining the cobot systems, software, communication protocols, and physical interfaces to identify weaknesses that cyber-attackers or malicious actors could exploit.

Cybersecurity testing is paramount to protect organizations from cyber-attacks and ensure the continuity of their business operations. It is critical to evaluate the effectiveness of security measures(Athanasopoulos and et al., 2022; Daoudagh and Marchetti, 2023). Furthermore, cybersecurity testing significantly enhances the security and reliability of software supply chains, thereby strengthening trust in essential software systems.

It aims to ensure data integrity, confidentiality, and availability and operations within cobot-enabled environments. Moreover, the testing helps organizations identify and mitigate cybersecurity threats that could compromise the functionality of cobots, jeopardize human safety, or lead to unauthorized access to sensitive information.

Several initiatives and frameworks have been developed and standardized, particularly OWASP's Software Assurance Maturity Model (SAMM,), NIST's Secure Software Development Framework (NIST,), ETSI's standard 303 645 (ETSI,), Cybersecurity Body of Knowledge (Martin et al., 2021) (McGraw, 2006) and Microsoft's SDL (Microsoft,). It is paramount to conceive and develop (by design) quality products, which is critical to secure innovative technologies like cobots but inadequate to satisfy the final requirements: building the product right does not guarantee building the right product (Sommerville, 2016). Testing will always remain a pivotal strategy for human-robot trustworthiness and cybersecurity assurance, ensuring that a product is developed and manufactured, achieving optimum

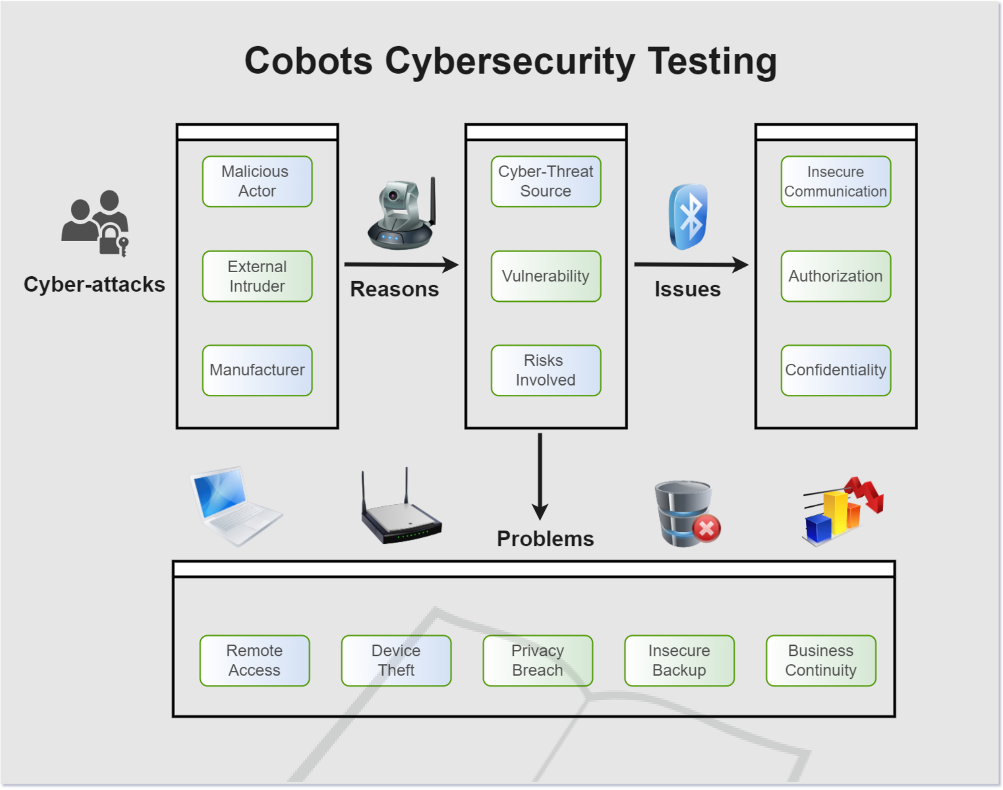

Figure 1: Cybersecurity Testing.

quality.

Indeed, the lack of testing processes can affect everyone directly or indirectly using software products. Moreover, companies or industrial sectors involving cobots in enhancing their productivity can be impacted by ransomware disguised as necessary libraries or plug-ins, government organizations, and multinationals suffering catastrophic cybersecurity attacks.

Going into details, cybersecurity testing of cobots inherits and adapts key activities typical of other application domains such as (Lonetti and Marchetti, 2018):

Vulnerability Assessment: Cobot systems, software, and infrastructure: it may include software code analysis or the execution of specific testing approaches such as access control testing, configuration testing, or penetration testing. This last is widely adopted for simulating cyber attacks and assessing the resilience of cobot systems against real-world threats. Access control testing is instead more focused on unauthorized access to cobot systems.

Specification-Based Testing: It mainly focuses on cobot behavior and may involve the analysis of cobot system configurations, access controls, and security policies to ensure compliance with specifications, cybersecurity best practices, and regulatory requirements. Specification testing helps identify gaps in security controls and provides recommendations for remediation.

Threat Modeling: Threat modeling involves identifying and prioritizing potential threats and attack vectors targeting cobot systems. Organizations can develop proactive security measures to mitigate the most significant risks by analysing the capabilities and motivations of potential adversaries.

Development Lifecycle Assessment: It involves evaluating the security practices and processes employed during the development and deployment of cobot systems. This includes reviewing coding standards, security testing methodologies, and incident response procedures to ensure that security is integrated throughout the entire lifecycle of cobots development.

Cybersecurity testing is critical in enhancing and evolving security measures to guarantee that cobots operate reliably and with enhanced security. However, it is vital to maintain operational integrity and security, with cobots indispensable in various critical operations. Moreover, this testing is essential to fortify these pivotal systems against potential threats.

Overall, cybersecurity testing of cobots is essential for safeguarding the security and reliability of cobot-enabled systems.By proactively recognizing and addressing vulnerabilities, organizations can mitigate cybersecurity risks and build trust in the safety and effectiveness of cobots technology.

In Figure 1, a schema of why cybersecuity testing is crucial for cobots is provided to better focus on the issue.

4 TESTING FRAMEWORK

The various domains of cybersecurity leverage major industrial technologies such as smart manufacturing, the Internet of Things (IoT),cobots Artificial Intelligence (AI),cyber-physical systems and cloud computing, and .However, these disruptive technologies demands updated cybersecurity measures. Moreover,implementing cybersecurity testing to establish user trustworthiness is essential.Our testing methodology and framework serves as a crucial direction for protecting the environment from potential security breaches and cyber-threats.

In the increasingly interconnected world of cobots, it is apparent that cybersecurity measures are crucial for managing risks and businesses, as depicted in Figure 1. Moreover, the industry needs ethical and proactive hackers to strengthen its defenses. Our cybersecurity testing strategy also involves close collaboration with various stakeholders to identify and address potential vulnerabilities and combat cyber threats across complex and heterogeneous systems.

It has been evident from frameworks and strategies presented in Section 2 that cobots lack a robust cybersecurity testing framework. Moreover, these frameworks do not fulfill the modern cybersecurity testing needs and requirements for cobots as discussed in Section 3.Therefore, we propose developing a cybersecurity testing framework focusing on testing and resolving cybersecurity issues in the cobot industry such as vulnerability detection. We propose a comprehensive cybersecurity testing framework to protect the system from malicious actors and enhance trustworthiness among manufacturers, users, robotic engineers, and developers to intermediate RCDI (Robotic Code Deployment Infrastructure) and various stakeholders as schematized in Figure 2.

Our proposed testing framework comprises of interconnected layers, each representing a unique set of components for conducting thorough cobots testing. The main objective is to rediscover and enhance the cybersecurity measures for the collaborative robots industry. Furthermore, our cybersecurity testing framework can leverage cobots cybersecurity and vulnerability issues as follows:

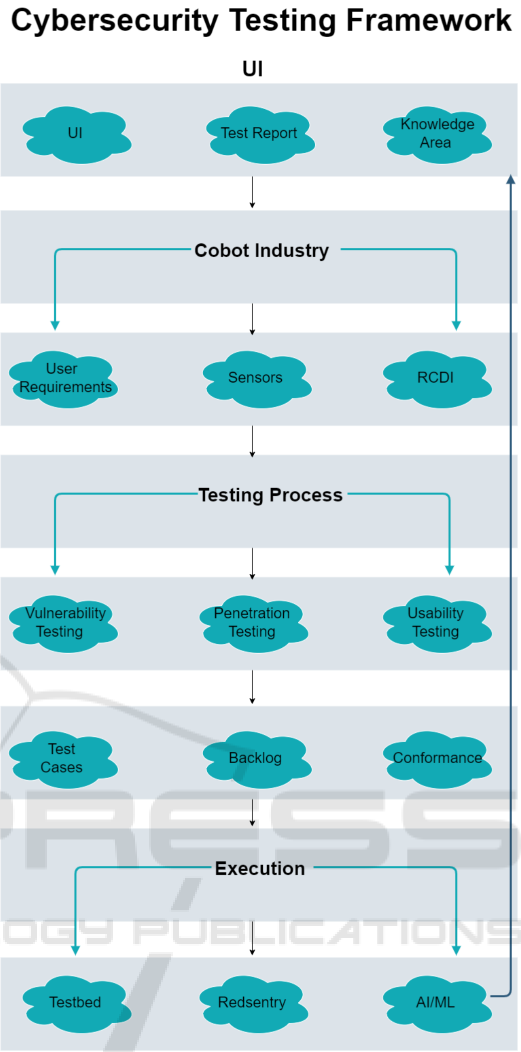

Figure 2: Testing Framework.

Software Testing: Software testing and quality assurance mechanisms are crucial to address cobot vulnerabilities. Moreover, continuous testing, stress testing, security testing, usability testing, and updated security measures are essential to minimize cobots software-related risks.

Utilizing AI: One way to improve cobots cybersecurity is to substitute traditional security and penetration testing methods with more advanced ones.For example, instead of relying on penetration testing or risk assessments, cobots can be tested using machine learning algorithms to identify potential vulnerabilities and risks frequently to be more committed to making the testing process easier to understand and implement through present AI/ML and LLM (Large Language Models) techniques.

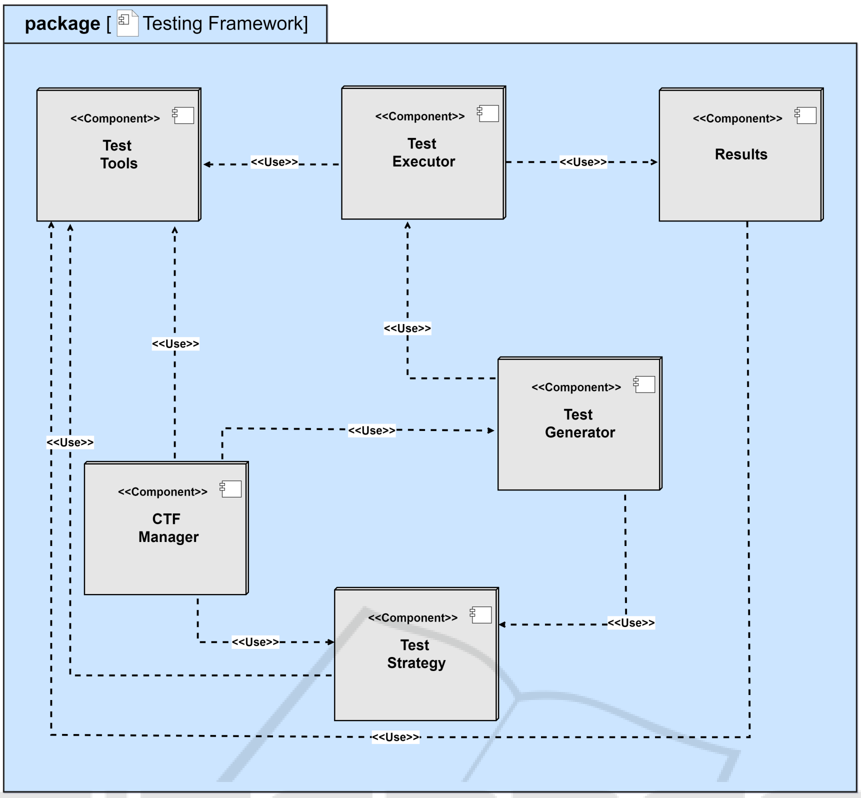

Figure 3: CTF Architecture.

Hybrid Testing Approach: Combining or amalgamating various cybersecurity testing techniques to create a more comprehensive testing approach is crucial. For instance, integrating penetration testing with vulnerability scanning or network traffic analysis can provide a clearer picture of the cobots security threats from a broader perspective.
Compatibility with Upgraded Infrastructure: cobots can be integrated with newer hardware and software technologies that improve their cybersecurity capabilities. For example, adding advanced sensors and machine learning algorithms can help cobots detect and respond to security threats more effectively.
Innovative and Unpredictable Design: Another approach is to modify the design of the cobots to make them more secure. It can involve using materials resistant to hacking attempts or adding physical barriers to prevent unauthorized cobot access.
Vulnerable Features: It may be possible to eliminate security risks by removing certain features or functions from the cobots. For instance, if a particular feature poses a significant security risk, it may be worth considering whether it is necessary for the cobots operation.

5 CTF ARCHITECTURE

CTF (Cybersecurity Testing Framework) has been developed, considering security as a collaboration and a shared responsibility among cobots developers, users, and security professionals. Moreover, it is a testing framework that offers an in-depth exploration of the cybersecurity testing process for the cobots industry from a broader perspective. It highlights the significance of cyber-attacks,recovery and resilience strategies, comprehending that breaches may emerge despite preventive measures claimed by cobots manufacturers, as discussed in our Figure 1 and Section 3.As schematized in Figure 3, CTF architecture has the following components:

CTF Manager: The role of the CTF Manager is to gather broader test requirements from cybersecurity experts, cobots manufacturers, developers, penetration testers, and robotic engineers to perform effective cybersecurity testing for cobots. Moreover, the component also manages the various decisions made during the testing activity execution, selecting test strategies and tools. Furthermore, all these activities are coordinated through a dedicated UI (User Interface) in CTF Manager.

Test Strategy: Test strategies provide testing techniques, methods, and pre-defined test cases. Moreover, it contributes to creating questionnaires utilized by the CTF Manager. Moreover, it aligns the testing process with the needs and requirements drafted in the collected questionnaires to guarantee that the derived test cases are sufficient for cobots cybersecurity testing. Furthermore, ensuring the testing process remains adaptable and resilient to new cybersecurity challenges and vulnerabilities in the cobots industry.

Test Generator: The purpose of the Test Generator is to manage and validate the selection of testing strategy through CTF Manager UI to generate test cases. Moreover, the test cases are generated by considering the specific cyber-attacks, vulnerabilities, and tools to fulfill cobots testing requirements and needs. Furthermore, the component will provide a robust test suite and help the tester select the most proficient one that aids in identifying and effectively mitigating potential cybersecurity risks and threats for cobots.

Test Executor: The purpose of this component is to execute the selected test cases or test suite. However, it depends on available testing libraries and tools to complete the test case specification and cobots testing execution environment (provided by the cobots manufacturers or retrieved through open-source proposals) to execute them effectively.Furthermore, executing test cases will guarantee the seamless, confidentiality,integrity and availability and overall cybersecurity of critical assets in functioning of cobots.

Test Tools: CTF integrates testing tools to conduct testing during test execution and selection of test strategies. However, these tools expand their pool of resources by leveraging user feedback and test reports. The components of CTF depend on this gathered knowledge, enhancing the effectiveness of the testing procedure. This component supplies adequate resources to others, such as test strategy and test results, and helps create and design predefined test case datasets and questionnaires. Furthermore, it archives and maintains user feedback and test reports, crucial in optimizing testing processes for future iterations.

Results: Once test cases are executed, analyzing the results is crucial. This analysis helps grasp the implications of any vulnerabilities found and pinpoint unnecessary pathways in RCDI, interconnected IoT devices, and external libraries or APIs. This evaluation is mostly performed through path coverage testing. Moreover, the essential duty of this component is to assess the test outcomes provided by CTF and generate test reports for users through the user interface of the UTF manager.

To thoroughly document the results of test case executions, it is crucial to maintain a comprehensive report. Moreover, this report should provide a comprehensive traceability of the test cases conducted and details regarding any detected vulnerabilities, where applicable. Furthermore, it is essential to categorize each identified vulnerability based on its severity level and to include potential recommendations for mitigating these vulnerabilities within the report.

It's important to understand that CTF architectural components require cutting-edge tools and strategies for adequate functionality. Moreover, the implementation of CTF is more focused on cobot safety and testing it against potential cyber-attacks and vulnerabilities.

6 CONCLUSION

Cybersecurity is a broad domain or never-ending argument about whether it is secure or adequately secure, but sincere efforts are still required to protect organizations' critical assets. It's crucial to understand the need for cybersecurity testing in cobots. This paper aims to enhance developers' and cobots experts' capabilities to detect vulnerabilities and counter cyber-attacks. The CTF gives them equal opportunity to be part of the system as testers. The critical analysis and documentation of test results play a pivotal role in enhancing the cobots cybersecurity and efficiency of systems, especially in environments as complex as those involving RCDI, interconnected IoT devices, and external libraries or APIs. The analysis of test results, focusing on the implications of identified vulnerabilities and the optimization of pathways, is a fundamental step toward ensuring the robustness and reliability of cobots.

In the future, several improvements will be made in CTF, particularly in integrating updated cybersecurity tools that focus on a broader set of users. It is crucial to continue advancing the methodologies and tools used in the testing and analysis phases. Furthermore, adopting more sophisticated AI (Artificial intelligence) testing tools is needed to enhance the efficiency of test case executions and vulnerability assessments. These technological advancements could offer predictive insights into potential security threats and suggest more proactive measures for vulnerability management in cobots.

ACKNOWLEDGEMENTS

This work was partially supported by the project RESTART (PE00000001) and the project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NextGenerationEU.

REFERENCES

(Access on 15th August 2024). Metasploit https://www.metasploit.com/.

(Access on 15th August 2024). Morphologycharts https://www.logos.com/product/45605/morphology-charts.

(Access on 15th August 2024). Nmap https://nmap.org/.

(Access on 15th August 2024). Portswigger https://portswigger.net/burp/pro.

(Access on 15th August 2024). Safetyculture https://safetyculture.com/topics/risk-assessment/.

(Access on 15th August 2024). Wireshark https://www.wireshark.org/.

Abakumov, A. and Kharchenko, V. (2022). Combining imeca analysis and penetration testing to assess the cybersecurity of industrial robotic systems. In *2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pages 1–7. IEEE.

Abakumov, A. and Kharchenko, V. (2023). Combining experimental and analytical methods for penetration testing of ai-powered robotic systems. In *COLINS (3)*, pages 526–538.

Abishek, B. A., Kavyashree, T., Jayalakshmi, R., Tharunkumar, S., and Raffik, R. (2023). Collaborative robots and cyber security in industry 5.0. In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, pages 1–6. IEEE.

Athanasopoulos, E. and et al. (December 2022). Cybersecurity for europe. In Markatos, E. and Rannenberg, K., editors, *Blue book*, pages 70–91. https://cybersec4europe.eu.

Caruana, L. and Francalanza, E. (2023). A safety 4.0 approach for collaborative robotics in the factories of the future. *Procedia Computer Science*, 217:1784–1793.

Daoudagh, S. and Marchetti, E. (2023). Breakthroughs in testing and certification in cybersecurity: Research gaps and open problems. In *Proc. of the 7th Italian Conference on Cyber Security, Bari, Italy, February 2nd to 5th, 2023*, CEUR Workshop Proceedings.

ETSI. Cyber; cyber security for consumer internet of things: Baseline requirements etsi en 303 645.

Gemalto (2023). Gemalto 2023: State of iot security. *Network Security*, 2019(2):4–4.

Heiding, F., Süren, E., Olegård, J., and Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, 126:103067.

Hollerer, S., Fischer, C., Brenner, B., Papa, M., Schlund, S., Kastner, W., Fabini, J., and Zseby, T. (2021). Cobot attack: a security assessment exemplified by a specific collaborative robot. *Procedia Manufacturing*, 54:191–196.

Kanak, A., Ergun, S., Yazıcı, A., Ozkan, M., Çokünlü, G., Yayan, U., Karaca, M., and Arslan, A. T. (2021). Verification and validation of an automated robot inspection cell for automotive body-in-white: a use case for the valu3s ecsel project. *Open Research Europe*, 1.

Kandasamy, K., Srinivas, S., Achuthan, K., and Rangan, V. (2020). Iot cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, 2020.

Lonetti, F. and Marchetti, E. (2018). Chapter three - emerging software testing technologies. volume 108 of *Advances in Computers*, pages 91–143. Elsevier.

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S., and Lupu, E. (2021). *The Cyber Security Body Of Knowledge*. University of Bristol. Version 1.1.0.

McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley Professional.

Microsoft. Microsoft sdl. [Accessed: 07 November 2022].

Nahavandi, S. (2019). Industry 5.0—a human-centric solution. *Sustainability*, 11(16):4371.

NIST. Secure software development framework. [Accessed: 07 November 2022].

Rindfleisch, A., Fukawa, N., and Onzo, N. (2022). Robots in retail: Rolling out the whiz. *AMS Review*, 12(3):238–244.

SAMM, O. Software assurance maturity model. [Accessed: 07 November 2022].

Sommerville, I. (2016). Software engineering 10. *Harlow: Pearson Education Limited*.

Thummapudi, L. S., Cherukuri, A. K., and Ling, T. C. (2024). Security concerns and controls of intelligent cobots of industry 4.0. In *Industry 4.0, Smart Manufacturing, and Industrial Engineering*, pages 24–35. CRC Press.