

# The Impact of IOT Cybersecurity Testing in the Perspective of Industry 5.0

Tauheed Waheed<sup>a</sup> and Eda Marchetti<sup>b</sup>

CNR-ISTI Pisa, Italy

**Keywords:** Industry 4.0, IoT Cybersecurity, Industry 5.0.

**Abstract:** The continuous advancements in IoT (Internet of Things) have various benefits. It has opened new horizons for the industrial revolution in the 21st century. Industry 4.0 and Industry 5.0 also promote using IoT devices to build better and more productive autonomous systems. The behaviour of these complex software systems evolves as they are augmented with the physical and security of IoT devices. IoT-security security and privacy benchmark systems have recently caused a financial loss in various industrial sectors. More importantly, it has damaged the trust of people in technology and IoT systems and people's distrust towards IoT, motivating rediscovering IoT cybersecurity from a brother perspective. The paper aims to enhance security and privacy by design methodology and provides an overview of the issues and challenges in cybersecurity testing. We also proposed a Cybersecurity Testing Framework (CTF) to enhance IoT cybersecurity that will help to resolve significant security and privacy challenges related to Industry 5.0.

## 1 INTRODUCTION


Recently, the Security and Privacy by Design (SPbD) approach has been proposed to target these two important attributes and ensure that IoT systems by design comply with their principles. Thus, the software industry and academia promote the concept of SPbD to build a proactive security-based culture rather than bearing the additional cost of security testing later in the development process. Even if they leverage enterprise architecture methods to improve the implementation of security during development, SPbD is still not fully implemented, and various questions and undiscovered challenges are still unsolved.


Recent research revealed that 90% of consumers need more confidence regarding the IoT cybersecurity of their systems or applications (Gem, ). Solutions for reducing uncertainty and increasing overall reliability, cybersecurity and trustworthiness must move in two technological and societal directions.

Considering the former, past solutions adopted by Industry 4.0 focused on using legacy or embedded systems to isolate them from the Internet (Casola et al., 2020), even if with a significant impact on the business and benefits. It is evident that Industry 4.0

and automation brought various business benefits, but going into Industry 5.0 our modern industrial systems will require more efficient, trusted, and secure ways of communication. Indeed, pressure from time to market often forces industries and developers towards massive use of available third-party or open-source components that could increase cybersecurity risks if not adequately tested. Additionally, if, from one side, the commonly adopted cloud solutions and data analytics (like, Google Cloud (Security, 2020), Microsoft Azure (Andrade, 2022) and Amazon (Infrastructure, 2022) improve the IOT integrability (Andrade et al., 2020), for the other still requires robust trustable and reliable solutions and components. Finally, as evidenced by the many focused call-for-proposals at the European level, one of the most effective means for preventing main criticalities and breaches is to promote the by-design adoption of cybersecurity from a broader perspective (Casola et al., 2020) (Chhetri et al., 2022)

Thus, guidelines and methodologies and specific tools for integrating cybersecurity into the entire life cycle of software development, from conception to dismantlement, have been the focus of the last year's research activity (Tahaei and Vaniea, 2023) with particular attention to tools and techniques support Agile (Bonorchis, 2022) and DevOps (Atlassian, 2023) approaches.

<sup>a</sup>  <https://orcid.org/0009-0006-0489-7697>

<sup>b</sup>  <https://orcid.org/0000-0003-4223-8036>

Among them, an important role has been taken by proposals focused on testing, analysis and verification of potentially vulnerable, insecure hardware and software components because they are considered the most effective ways to prevent, detect and control vulnerability and failures (Garousi et al., 2020).

However, considering that the overall cost of testing is around 40% of the total development costs of a typical software project (Garousi et al., 2020), in IoT and Industry 4.0, verification, validation, and assessment procedures are the first to be reduced or skipped to save cost and time if not strictly connected to safety risks.

From the societal point of view, and in line with the Internet of trust (European, 2022) principles, a human-centred and ethical development of digital and industrial technologies is currently recognised as the most effective way for improving the overall trustworthiness and supporting social innovation (European, 2022). Indeed, by 2030, 80% of citizens will use digital solutions. A two-way engagement of citizens in developing and testing technologies will assure more sustainable and secure infrastructures, systems and components.

In this paper, following the message of (Bravos et al., 2022), we focus on improving the IoT cybersecurity testing for the next generation of our industrial development processes and integrating it with human capabilities.

Considering both technological and societal directions, the proposal of this paper focuses on several areas, such as: evaluating present cybersecurity testing solutions, working in line with the intelligent iterative processes, promoting a practical IoT cybersecurity testing approach, supporting user-centric testing, improving and assessing technological development in line with social and ethical values, sustainability and user trustworthiness, adoption of standards to increase transparency and openness.

The cybersecurity market is expected to grow to 170.4 billion dollars in the coming years (Zaghoul et al., 2021). In this light, one main target of the Internet of Things is to promote connectivity between devices and objects. Recent estimations show that the number of devices connected to the Internet has increased abruptly from 0.08 to 6.58% per person, with an overall increase of 8225% in the last seven years (Gómez et al., 2021)

Indeed, this massive growth of services and possibilities certainly improves digital lives, allowing people to be connected whenever and wherever, but it calls for specific attention to security and privacy. With the new paradigm proposed by Industry 5.0, which focuses on the collaboration between robots

and humans (Adel, 2022), the emphasis on technologies will be reduced. However, security and privacy criticalities are not entirely solved (Straub, 2020) due to a lack of user involvement in IoT cybersecurity testing. The primary purpose of this paper is to develop a comprehensive cybersecurity testing framework while 'user' or 'human' should be center of focus.

In particular, in Section 2, we present the current perspectives about cybersecurity and we analyse the currently available solutions considering the impact of IOT cybersecurity testing in Industry 4.0 to move a first step from the perspective of Industry 5.0. Then we first overview the security and privacy threats and their impact on cybersecurity testing Section 4).

Then, Section 4 analyses cybersecurity from different perspectives considering various domains utilising IoT infrastructure and exploring paramount factors regarding the need for cybersecurity testing in the present era. Section 4 discusses the importance of cybersecurity testing and later proposed CTF. Moreover, it is a human-centric or user-centric cybersecurity testing framework appropriate for Industry 5.0.

## 2 BACKGROUND AND RELATED WORK

Cyber assaults (Rajabion, 2023) play a critical role in safeguarding software and hardware against intrusion and unauthorized access. Nowadays, security measures use various security strategies like access control systems, cybersecurity software, antivirus and malware, intrusion detections, firewalls, raising security awareness for system users and process optimization. The intelligent access to resources (Srujana et al., 2022) can be possible through cybersecurity appropriately. However, these transformations have made cybersecurity the most robust modern-day defence strategy against various digital threats and attacks. Therefore, various sectors are investing in enhancing security mechanisms and cybersecurity to prevent data theft, maintain regulatory compliance, secure trade secrets, and protect critical information while facilitating and improving organization operations. Exploring and understanding cybersecurity from various perspectives is essential, as cyber-attackers do not always follow the same attack strategy. In the following, some of these aspects will be discussed.

1. As reported in (Jaber and Fritsch, 2022), cybersecurity's primary focus is on defence strategies that detect, mitigate and prevent the system

from cyber-attacks, but the technology and digitalization environment is becoming more complex. Therefore, regularly updating an organization's security strategy to enhance its cybersecurity defences is essential.

2. In recent years, emerging technologies like Artificial Intelligence (AI) have been applied to solve some cybersecurity criticalities, but AI features have also been used by cyber-attacks too. Indeed, AI-driven cyber-attacks create complex challenges for cybersecurity experts, impacting overall system trustworthiness. Nowadays, cybersecurity (Pearlson and Huang, 2022) issues are detected and resolved mainly through quality-control testing, vulnerability testing and penetration testing.
3. Considering the Small and Medium-sized enterprise perspective, it has been observed that the number of hackers is increasing as they are exploiting SMEs limited resources and outdated cybersecurity infrastructure. SMEs should improve their cybersecurity approach efficiently and appropriately. a recent study demonstrates that (Varma et al., 2023) that several undiscovered cybersecurity vulnerabilities were due to lack of technical skills and knowledge in using the available facilities. Thus guidelines and roadmap should be provided to aid SMEs in adequately implementing the proper defence.
4. European Union Cybersecurity Agency (ENISA) and American National Institute of Technology (NIST) (Chiara, 2022) recognise cybersecurity certifications as one of the effective means for ensuring the right level so trust. The IoT based certifications can have a role in Industry 5.0 and become paramount for user trustworthiness as vendors must meet cybersecurity requirements before launching and selling their products (Trustmark, 2021). Additionally, as highlighted in (White-House, 2021) federal government should support the recognition of cybersecurity vulnerabilities and persistent network threats by providing proactive and visionary measures to modernize its cybersecurity strategy, including by maximizing the federal government's visibility into cybersecurity threats while protecting user privacy and rights.

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 be the solution for facing cybersecurity criticalities (Heiding et al., 2023).

### 3 WHY DO WE NEED CYBERSECURITY TESTING?

As highlighted before, cybersecurity testing will aid in further maturing the predictable security mechanisms for ensuring that the product performs its functions as intended and more securely. Cybersecurity testing will become more vital than ever for maintaining the integrity and security of critical software systems for several reasons. Cybersecurity testing can protect organizations from cyber-attacks and, more important, able to disrupt business continuity from a broader perspective (Athanasopoulos and et al., 2022; Daoudagh and Marchetti, 2023) and provide them with the level of robustness of their security strategy and efficacy of their countermeasures. Cybersecurity testing can improve the integrity and security of the software supply chain, enhancing user trustworthiness in critical software systems. In Figure 1, for a better focus on the issue, a schema of the main reasons why cybersecurity testing is important is provided.

#### 1 Achieving Auditable and verifiable Products:

The massive portion of the software components that aid in developing software services or products are extracted from third parties and, therefore can contain vulnerabilities that could compromise the overall desired security requirements. Cybersecurity testing can help to achieve verifiable and auditable products.

**2 Improving the continuous Inspections of Software:** The software system or application requires frequent updates due that could impact security, privacy, General Data Protection and Regulation (GDPR) policies and, importantly user/consumer needs. Cybersecurity testing and regression, in particular, can be used to update the software systems efficiently and improve its continuous inspections.

**3 Achieving Better Implementation of SPbD for Agile Software Development:** As we mentioned in the introduction, SPbD still needs comprehensive strategies to build a proactive security-based culture in the software industry. Therefore, specific SPbD cybersecurity testing techniques and tools should be provided to prevent cyber-attackers and intruders from compromising security requirements.

**4 Enhancing Software Reliability:** Even if in the last decade, various security measures and guidelines have been implemented to improve the reliability of industrial systems, more effort is required to meet a certain level of quality. Therefore, cybersecurity testing will be significant to pave the way to improve the reliability of our modern-day cyber-physical systems and various complex AI-driven software systems.

**5 Improving Decentralized Software Governance:** The blockchain technologies, smart contracts

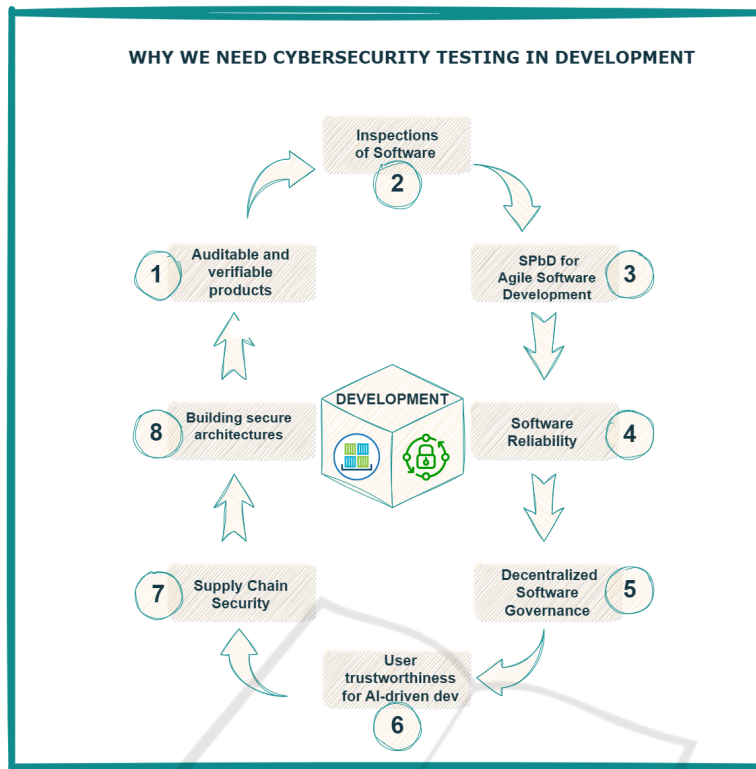


Figure 1: Cybersecurity needs.

and crypto-assets are prominent examples of software with decentralized governance in which cybersecurity testing can identify vulnerabilities and evaluate the impact of the recovery actions on the overall consensus.

**6 Exploring new Challenges and Improving user Trustworthiness in AI-driven Software Development:** In the near future, particularly going into Industry 5.0, most of the software life cycle activities will be carried out by intelligent agents increasing productivity but also cybersecurity risks. Therefore, cybersecurity testing (Pawlicka et al., 2022) will be needed to improve user trustworthiness in AI-driven software development and ultimately enhance our security strategy from a broader perspective.

**7 Improving Supply chain Security:** The integration of components and code from third parties, whose development and testing are considered outside the control, can be a risk for the overall system. During the recent pandemic, they encountered various attacks, such as the SolarWind cyber-attack (Athanasopoulos and et al., 2022). Methodology to improve supply chain security and cybersecurity testing has excellent potential to guarantee the trustworthiness of these third-party components.

**8 Building more Secure Architectures and Plat-**

**forms:** It's essential to understand that a trusted supply chain is insufficient to develop and maintain security-critical systems. Secure architectures starting from the hardware and operating system level should be developed and cybersecurity testing applied (Athanasopoulos and et al., 2022) to validate communication between components and the overall security.

As a practical example, we refer to the software system developed (Kirk et al., 2023) for modern autonomous vehicles is more advanced and complicated than desktop-based software due to increased dependencies or interconnectivity to perform various critical functions. However, these dependencies and complexities increase attack-surface area while ultimately aiding cyber-attackers. In this regard, researchers have introduced Over-The-Air (OTA) updates to mitigate and prevent cyber-attacks. The same OTA updates have also been utilized for both Android and desktop systems. Uptane is the current OTA security system for autonomous vehicles. It is designed to address the special issues vehicles must face. The working mechanism of the Uptane system particularly needs to possess a secure method for updating; if not, hackers will exploit it regularly.

Researchers have developed model-based and comprehensive security testing approaches by trans-



forming Uptane and attack models into formal models for Communicating Sequential Processes (CSP) in broader perspectives (Kirk et al., 2023). The results achieved by security testing provided the benchmark to validate some paramount vulnerabilities and security design of Uptane. Furthermore, the researchers tested Uptane system with 25 specifically conceived test cases to simulate attacks. The OTA system was stressed with a continuous bombardment of security tests during its live implementation, demonstrating unexpected vulnerabilities.

#### 4 CYBERSECURITY FRAMEWORK

The cybersecurity domains directly impact industrial technologies like smart manufacturing, the Internet of Things (IoT), cyber-physical systems, cloud computing and Artificial Intelligence. Therefore, all these industrial technologies demand updated cybersecurity measures and utilizing cybersecurity testing to build user trustworthiness is the appropriate direction to protect the environment from being attacked.

It has been evident that cybersecurity essentials for Industry 5.0 emphasize risk management and business continuity. As we move towards Industry 5.0, more white and grey hat hackers are needed. The user-centric cybersecurity testing approach will collaborate with white hat hackers to reduce vulnerability and cyber-attacks on

Cybercriminals are the first cybersecurity essential threat for Industry 5.0. Cyber-criminals are either internal, such as employees, or external, such as organized attackers (Hactivist, state-sponsored) and hackers (black, white, grey). Moreover, their motivation is financial gain; they practice cracking passwords while sending malware and viruses to steal critical financial assets, such as credit cards or any information that can be of high value. The countermeasure for cyber crimes varies as it is based on the value of data and its sensitivity.

The continuous and proactive updating of cybersecurity testing techniques are needed to counter skillful hackers, but a solution could be to ask for the help of users that are the final and most impacted by this annoying situation. Users have enormous manpower, and in the proper condition, they can work together with testers and developers for a more secure and safe life in every application domain. Our proposal is, therefore, to develop a human-centric testing that can be suitable also for Industry 5.0. We propose a continuous and hybrid cybersecurity testing framework to protect the system from cyber-attacks and increase

#### Cyber-security Testing Framework

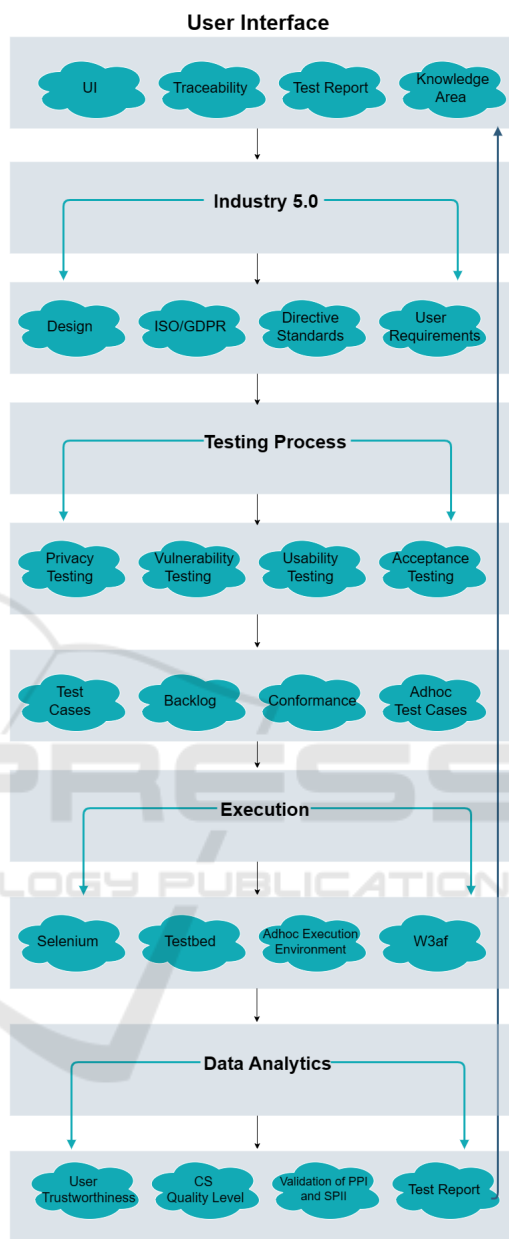


Figure 2: Conceptual Model.

user trustworthiness as schematized in Figure 2.

As in the figure our proposal comprises various layers, and different elements in each of them, to let the user be completely involved in testing and ultimately enhancing user trustworthiness.

**User Interface:** The first layer is the user interface where the users can find facilities for expressing their requirements, needs and desired functions. In this layer, there can be, but not limited to, the following elements:

- **UI:** It allows the user to interact with the system depending upon the scope and legitimacy of the user to perform some tasks.
- **Traceability:** Traceability in the user interface allows all kinds of users to be proactive while performing cybersecurity testing in every iteration.
- **Test Report:** It is generated based on testing activities and is a fundamental document for managing founded threats or bugs or future improvements.
- **Knowledge Area:** The knowledge area reports the lessons learned from previous iterations and provides a collaborative knowledge-sharing platform to all users/stakeholders interested in improving cybersecurity.

**Industry 5.0:** Represent the target domain of this paper and the proposed human-machine collaboration. The objective is to boost industrial productivity and open new horizons in technological advancements. The element we included in this layer are:

- **Design:** The design specification describes the environment, the systems, its components and how the user interacts with the system. This can guide the cybersecurity testing.
- **ISO/GDPR:** It is paramount to keep track of updates in International Organization of Standardization (ISO) and General Data Protection and Regulation (GDPR), while going into requirements elicitation.
- **Directive Standards:** The directive standards will also be considered because they provide basic safety management strategies and legal working mechanisms for various domains, e.g., health care.
- **User Requirements:** The user requirements elicitation phase provides an opportunity to understand user needs better and focus on the cybersecurity testing process.

**Testing Process:** The intention is to provide a unified platform to perform various types of cybersecurity testing to improve the security strategy from broader perspectives and with specific user facilities. It includes two sub-layer definitions of the test target and the selection of the test strategy. In particular, as reported in the figure, we considered:

- **Privacy Testing:** If focus on user privacy requirements and their implementation. It is essential for different domains and, in particular, for the health-care systems.
- **Vulnerability Testing:** It evaluates the security by recognizing and resolving application short-

comings. It is helpful to understand system behaviour for the identification of risks.

- **Usability Testing:** It focuses on system behavior while interacting with the user to detect vulnerabilities that malicious attackers can exploit.
- **Acceptance Testing:** Also referred to as pre-production testing, checks whether the software system or application satisfies the user acceptance criteria. Moreover, acceptance testing is carried out to ensure that the software developed is convenient to release by performing formal testing of user/customer requirements and business motives.
- **Test Cases:** The test cases are usually formulated and documented by software testers to fulfil all acceptance criteria requirements. The test cases can be prioritized based on their importance in acceptance criteria. This prioritization of test cases ensures that the most critical and paramount functionalities are tested first. Moreover, it must simulate the real-world scenario to test all software functionalities.
- **Backlog:** The backlog comprises a prioritized list of tasks for the cybersecurity testing team. It is extracted from the test cases and user requirements. The most critical tasks are shown at the top of the testing backlog, so the tester delivers them first. It also documents the meetings among developers, testers, users and various stakeholders.
- **Conformance:** The purpose is to review and validate test cases to ensure they are adequate and correct. As mentioned above, test cases are documented in the testing backlog and kept in a centralized position for further verification. Moreover, when all the test cases are executed, the cybersecurity testing team must review the test results to resolve the defects.
- **Adhoc Test Cases:** The purpose is to check for the completeness of the testing process and to find more defects before going into the execution process. It is an unstructured approach that doesn't follow formal documentation and test design techniques to formulate adhoc test cases. The tester should have adequate knowledge of the system under test to create quality adhoc test cases.
- **Execution:** The execution of our cybersecurity testing framework will be done through various state-of-the-art testing techniques and tools such as;
  - **Selenium:** Selenium is an open-source automated testing framework for web applications across different platforms and browsers. It is utilized to automate web applications for testing, it is supported

by vendors. The selenium will always be relevant in the perspective of our cybersecurity testing framework execution because cyber-attackers mostly prefer web applications as these are fragile and comprised of users that are newbies in terms of using technology securely.

**Test-bed:** The term test bed is more like an umbrella activity, as it captures everything from hardware equipment, and prototype machines to virtual investigative environments integrated with user requirements for continuous optimization. The test-bed environments are supported by a comprehensive network of stakeholders and domain experts. In envisaging to involve users in the testing process, the test bed should let them collaborate with various stakeholders like domain experts for keep on developing innovative solutions to adapt to Industry 5.0 effectively.

**Adhoc Execution Environment:** The purpose of adhoc execution environment is to allow the execution of the test cases without creating or going through a formal test plan. This execution environment has been widely utilized in agile testing environments and development because iterative testing is essential to deliver the product timely. The adhoc execution environment plays a massive role in ensuring quality and identifying defects in our products.

**W3af:** The W3af (Web Application Attack and Audit Framework) is basically open-source security scanner for web applications. The main purpose of W3af is to provide a framework or platform that helps us to secure our web applications by exploiting and identifying various vulnerabilities. It aids in penetration testing and provides important information about security vulnerabilities.

**Data Analytic:** The purpose of data analytics in our CTF is to extract data from our testing results after its execution and perform analysis to achieve various benefits. It a clear picture to improve the quality of our test suite and improves collaboration among various stakeholders. Moreover, it aids in exploring the causes of test failures and documenting them in the shape of cybersecurity test reports. It includes the following elements:

- **User Requirements:** It organizes and helps to improve user requirements for optimizing organizational cybersecurity strategy.
- **Cybersecurity Quality Level:** The purpose of cybersecurity testing framework is to achieve some adequate quality level. Industry 5.0 needs quality risk management strategies to understand

user/customer demands and to improve its security policies. Through the cybersecurity testing process, evidence can be collected and used for deriving the quality level provided. This measure provides the user with the data for increasing his/her trustworthiness in the tested system.

- **Validation of PII and SPII:** Another advantage data analytics will provide is validating PII (Personally Identifiable Information) and SPII (Sensitive Personally Identifiable Information) that can be utilized to distinguish one individual from another. The security and validation of these essential assets play a massive role to achieve user trustworthiness, as the consistent validation of these assets protects our users from financial theft and identity theft.
- **Test Report:** The test report achieved from our CTF is really vital for everyone, including users, security experts and various stakeholders. As schematised in Figure 2, the test report enhances the knowledge area of various users performing cybersecurity testing in the next iterations. Furthermore, the test report will help our stakeholders to analyze the errors and security loopholes efficiently.

## 5 CONCLUSION

Cybersecurity is evolving rapidly, and it's essential to understand the need for user involvement to formulate an efficient and robust cybersecurity strategy. This paper aims to enhance user trustworthiness by giving them equal opportunity to be part of the system in the tester's shape. As the number of IoT users is increasing and bringing complex challenges for cybersecurity. We tried to resolve these challenges through our CTF and its user-centricity. It will help us to educate and motivate users to take responsibility for security. We have a long road ahead in terms of building ubiquitous testing platforms to achieve adequate quality and user trustworthiness, but user-centric Cybersecurity Testing Frameworks, as the one presented here, have excellent potential to resolve cybersecurity challenges.

## ACKNOWLEDGEMENTS

This work was partially supported by the project SER-ICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

## REFERENCES

- Gemalto 2023: State of iot security. *Network Security*, 2019(2):4–4.
- Adel, A. (2022). Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. *J. of Cloud Computing*, 11(1):1–15.
- Andrade (20 December 2022). Azure identity & access security best practices microsoft learn. in azure security fundamentals documentations. <https://learn.microsoft.com>, Retrieved(July 14,2023).
- Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., and Ortiz-Garcés, I. (2020). A comprehensive study of the iot cybersecurity in smart cities. *IEEE Access*, 8:19.
- Athanasopoulos, E. and et al. (December 2022). Cybersecurity for europe. In Markatos, E. and Rannenber, K., editors, *Blue book*, pages 70–91. <https://cybersec4europe.eu>.
- Atlassian, J. (7 May 2023). Jira security issues. atlassian community. <https://community.atlassian.com/>, Retrieved(July 14,2023).
- Bonorchis (20 October 2022). Jira-issue & project tracking software. atlassian. <https://www.atlassian.com>, Retrieved(July 14,2023).
- Bravos, G., Cabrera, A. J., Correa, C., Danilović, Vasiliadis, G., and Vukobratovic, D. (2022). Cybersecurity for industrial internet of things: Architecture, models and lessons learned. *IEEE Access*, 10:124747–124765.
- Casola, V., De Benedictis, A., and Rak (2020). A novel security-by-design methodology: Modeling and assessing security by slas with a quantitative approach. *J. of Systems and Software*, 163:110537.
- Chhetri, M. B., Liu, X., Grobler, M., Hoang, T., Renaud, K., and McIntosh, J. (2022). Report on the 2nd workshop on human centric software engineering & cyber security (hese&cs 2021). *SIGSOFT Softw. Eng. Notes*, 47(2):12–14.
- Chiara, P. G. (2022). The iot and the new eu cybersecurity regulatory landscape. *Int.Review of Law, Computers & Technology*, 36(2):118–137.
- 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.
- European, U. (15 December 2022). European digitalization vision. <https://www.europarl.europa.eu>, Retrieved(July 14,2023).
- Garousi, V., Rainer, A., Lauvås Jr, P., and Arcuri, A. (2020). Software-testing education: A systematic literature mapping. *J. of Systems and Software*, 165:110570.
- Gómez, G., Espina, E., and Armas-Aguirre, J. M. M. (2021). Cybersecurity architecture functional model for cyber risk reduction in iot based wearable devices. In *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería*, pages 1–4. IEEE.
- Heiding, F., Süren, E., Olegård, J., and Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, 126:103067.
- Infrastructure, A. S. (22 November 2022). Amazon cloud security – amazon web services (aws). <https://aws.amazon.com>, Retrieved(July 14,2023).
- Jaber, A. and Fritsch, L. (2022). Towards ai-powered cybersecurity attack modeling with simulation tools: Review of attack simulators. In *Int. Conf. on P2P, Parallel, Grid, Cloud and Internet Computing*, pages 249–257. Springer.
- Kirk, R., Nguyen, H. N., Bryans, J., and Shaikh (2023). A formal framework for security testing of automotive over-the-air update systems. *J.of Logical and Algebraic Methods in Programming*, 130:100812.
- Pawlicka, A., Pawlicki, M., Kozik, R., and Choraś, M. (2022). Human-driven and human-centred cybersecurity: policy-making implications. *Transforming Government: People, Process and Policy*, 16(4):478–487.
- Pearlson, K. and Huang, K. (2022). Design for cybersecurity from the start. *MIT Sloan Management Review*, 63(2):73–77.
- Rajabion, L. (2023). Industry 5.0 and cyber crime security threats. In *Advanced Research and Real-World Applications of Industry 5.0*, pages 66–76. IGI Global.
- Security, G. C. (2 August 2020). Google cloud blogs. google cloud solutions. <https://cloud.google.com>, Retrieved(July 14,2023).
- Srujana, S., Sreeja, P., Swetha, G., and Shanmugasundaram, H. (2022). Cutting edge technologies for improved cybersecurity model: A survey. In *2022 International Conference on Applied AI and Computing (ICAAIC)*.
- Straub, J. (2020). Software engineering: The first line of defense for cybersecurity. In *2020 IEEE 11th Int. Conf. on Software Engineering and Service Science (ICSESS)*, pages 1–5. IEEE.
- Tahaei, M. and Vaniea (2023). Embedding privacy into design through software developers: Challenges and solutions. *IEEE Security & Privacy*, 21(1):49–57.
- Trustmark, I. S. (2 December 2021). Baseline iot cybersecurity requirements. <https://trustmark.tech/baseline/>, Retrieved(July 14,2023).
- Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., and Alshurideh, M. (2023). A roadmap for smes to adopt an ai based cyber threat intelligence. In *The Effect of IT on Business and Marketing Intelligence Systems*, pages 1903–1926. Springer.
- WhiteHouse, N. C. (12 May 2021). Executive order on improving the nation’s cybersecurity. <https://www.whitehouse.gov>, Retrieved(July 14 2023).
- Zaghloul, Z. S., Elsayed, N., Li, C., and Bayoumi, M. (2021). Green iot system architecture for applied autonomous network cybersecurity monitoring. In *2021 IEEE 7th World Forum on IoT (WF-IoT)*, pages 628–632. IEEE.