ACCURATE - eternAl infrastruCture for seCUrity in softwaRe and hArdware developmenT and assessmEnt

Antonello Calabrò[1][a], Eda Marchetti[1][b] and Sanaz Nikghadam-Hojjati[2][c]
[1]*Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo", CNR, Pisa, Italy*
[2]*UNINOVA-CTS and LASI, Caparica, Portugal*

Keywords: Cybersecurity, Eternal Testing, Architecture.

Abstract: This paper addresses the increasing complexity of cybersecurity and the need for compliance with evolving EU regulations, highlighting the limitations of traditional software and hardware development processes in managing security, trust, and long-term compliance. To bridge these gaps, the paper proposes a novel lifecycle and supporting architecture named ACCURATE (eternal infrastructure for security in software and hardware development and assessment). ACCURATE is inspired by the DevOps approach and integrates continuous real-time monitoring, detection, and vulnerability management throughout the entire lifecycle. ACCURATE is designed for software and hardware development, as well as post-development continuous assessment. The main novelty is conceiving the "Eternal" stage, focusing on ongoing post-deployment assessment and protection, ensuring systems remain resilient against emerging threats. ACCURATE aims to transform the security landscape by embedding continuous safeguarding mechanisms throughout the development and operational stages, ultimately ensuring the integrity and reliability of both software and hardware systems in a rapidly evolving technological environment.

1 INTRODUCTION

Traditional development methods are often insufficient to tackle the increasing complexity and frequency of cyber threats, compliance with evolving EU regulations, and the need for sovereignty. Therefore, a review of the development processes is necessary for addressing critical properties such as ethics, security, safety, trust, transparency, and privacy (Syed et al., 2022; Zimmermann et al., 2024). This includes enhancing: i) the trustworthiness of HW/SW by offering automated tools to identify evolving security threats and support the adoption of countermeasures and mitigation strategies; ii) information sharing and active collaboration among stakeholders; iii) cybersecurity awareness and certification support processes through automated documentation and reporting. Despite their continuous advancements, effectiveness, and efficacy, one critical aspect that remains underdeveloped is the continuous safeguarding of released systems, often called "eternal watch guarding." This involves ongoing monitoring and protection to preemptively address vulnerabilities and threats also during the post-deployment phase.

Currently, there are only a limited number of approaches aimed at achieving this continuous safeguarding, and they tend to be fragmented rather than integrated into the overall lifecycle (Ma, 2024). Filling this gap highlights the need for a more systematic approach to ensure trustworthiness and vulnerability management embedded at every stage of the development process, from design to deployment and beyond.

The ACCURATE (eternAl infrastruCture for seCUrity in softwaRe and hArdware developmenT and assEssment) proposal presented in this paper targets this challenge by leveraging the widely adopted development lifecycles (like DevOps and DevSecOPs) to ensure:

- continuous real-time (deployment and post-deployment) monitoring, analysis, detection, prediction, and post-deployment of (security, safety, trust, transparency, and privacy) vulnerabilities;
- eternal assessment and automated compliance updates with (new) EU regulations;
- adaptive responses to evolving security require-

[a] https://orcid.org/0000-0001-5502-303X
[b] https://orcid.org/0000-0003-4223-8036
[c] https://orcid.org/0000-0002-0839-9250

Calabrò, A., Marchetti, E. and Nikghadam-Hojjati, S.
ACCURATE - eternAl infrastruCture for seCUrity in softwaRe and hArdware developmenT and assessmEnt.
DOI: 10.5220/0013704700003985

In *Proceedings of the 21st International Conference on Web Information Systems and Technologies (WEBIST 2025)*, pages 157-164
ISBN: 978-989-758-772-6; ISSN: 2184-3252

ments;

- safeguarding and resilience against long-term vulnerabilities, evolving cyber-threats, and newly discovered cybersecurity issues;
- post-deployment solutions to continuously enhance and foster greater awareness and trust.

While inspired by the DevOps lifecycle, ACCURATE extends it with a novel *Eternal* stage, focused on post-deployment testing, assessment, and vulnerability mitigation. This addition addresses a key gap in traditional and modern models (e.g., Waterfall, Spiral, Agile (Kornecki and Zalewski, 2010; Aouni et al., 2025)) that often overlook long-term security and maintenance, leading to trust and privacy issues as new threats emerge. As further detailed in the paper, ACCURATE fills this void by establishing a structured methodology for continuous engagement and assessment, ensuring HW and SW remain resilient against new and emerging threats. It aims to transform the security landscape of software and hardware systems, minimizing vulnerabilities and ensuring the integrity and reliability of these systems, thereby paving the way for a secure and resilient future. As detailed in the following sections, the updated *DEV* stage includes threat identification, AI-based attack detection and recovery, and compliance with industry standards. The *OPs* stage ensures automated security and privacy assessments, real-time monitoring, performance evaluation, and secure deployment across distributed networks. The new *Eternal* stage extends post-deployment observability with continuous testing, verification, and self-healing mechanisms. This structured, end-to-end framework integrates security, compliance, and resilience throughout the lifecycle, addressing gaps left by current DevSecOps models. Although full validation is still in progress due to architectural complexity, implementation is underway.

The paper is structured as follows: Section 2 presents the ACCURATE lifecycle. Section 3 describes the ACCURATE architecture and its components. Section 4 overviews the currently similar solutions and the innovation the ACCURATE proposal provides. The concluding section suggests future developments that may result from our proposal.

2 ACCURATE LIFECYCLE

The ACCURATE proposal builds upon DXO4AI (Calabrò et al., 2024; Daoudagh et al., 2024), a DevOps lifecycle for AI-based software, and CI/CD methodologies (Zimmermann et al., 2024). It extends the DXO4AI DEV-X-OPs approach—where *X* includes ethics, security, and transparency—by applying these principles throughout the entire lifecycle, including the post-deployment phase. ACCURATE introduces continuous automated testing and assessment for HW/SW, enhancing security, privacy, trustworthiness, and quality of experience. Its three stages: *DEV*, *OPs*, and the novel *ETERNAL*, ensure ongoing support for specification, deployment, and assessment, providing strong protection against cyber threats and operational failures while fostering HW/SW resilience. Figure 1 illustrates the core activities across these stages.

Considering every single stage, as in Figure 1, the DEV stage includes the *Designing, TBI, Assessing*, and *Deploying* activities. These leveraged standard DEV lifecycle activities by introducing specific tasks for key enhancements of SW and HW security and trustworthiness. In particular:

- During the *Planning*, as in the standard DevOps process requirements, collections and definitions of roadmaps, milestones, and project goals are considered. The HW and SW development is scheduled into smaller sub-tasks to deliver incremental value. In addition, the ACCURATE lifecycle focuses on i) security planning and realistic forecasting of system behaviors under strain; ii) assessing SW/HW compliance against security and privacy regulations and standards and collecting certification evidence for final validation and assessment.
- the ACCURATE *Designing* includes the Code phase of the standard DevOps process. Therefore, SW/HW is developed interactively according to the established plan. Additionally, the ACCURATE lifecycle forces the adoption of specific best practices and dynamic threat modeling techniques for identifying potential vectors for attacks early in the design process, mitigating risks, and making informed design decisions.
- the ACCURATE *TBI* includes the Build phase of the standard DevOps process. SW/HW is assembled into executable components or packages, and preliminary tests are executed. Additionally, the ACCURATE lifecycle forces the integration of Machine Learning (ML) algorithms and Artificial Intelligence (AI) models for improving threat detection capabilities, analyzing data patterns and behaviors, predicting likely attack scenarios, and enhancing the agility of response mechanisms.
- the ACCURATE *Assessing* includes the Test phase of the standard DevOps process. Therefore, SW/HW is tested to ensure the quality standards and requirements. Additionally, the ACCURATE

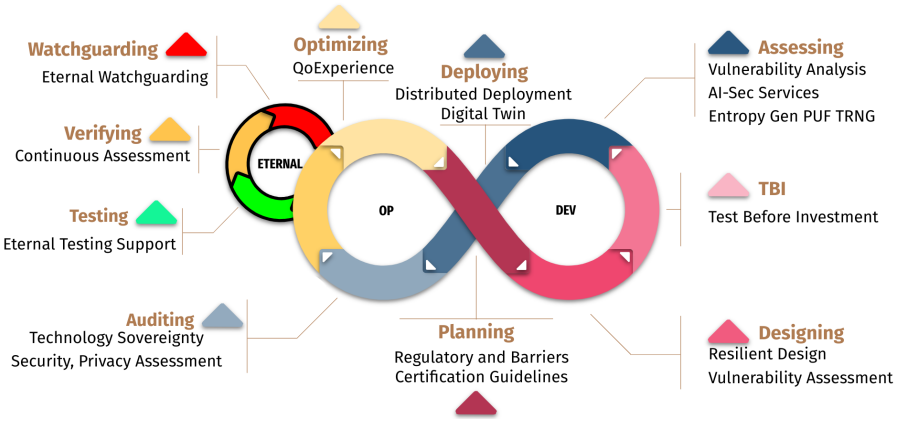

Figure 1: Proposed life cycle overview.

lifecycle forces the use of testing methodologies, including penetration testing and code audits, to validate system integrity and address vulnerabilities before they can be exploited.

- the ACCURATE *Deploying* includes the Release phase of the standard DevOps process. SW/HW is finally released, and evidence of requirements satisfaction and identified issues solved is provided. Additionally, the ACCURATE lifecycle forces the SW/HW security and privacy frameworks to be assured, as well as the regulations and standards.

The DEV phase of the ACCURATE proposal prioritizes SW/HW vulnerabilities, validates SW/HW components, and provides solutions for digital ID, entity authentication, key generation, Intellectual Property (IP) protection, and anti-counterfeiting. As in Figure 1, the OP stage includes the *Planning, Auditing*, and *Optimizing* activities. These leveraged standard OP lifecycle activities by introducing specific support for SW/HW. In particular:

- the ACCURATE *Auditing* includes the Deploy and Operate phases of the standard DevOps process. Therefore, SW/HW is deployed to the final environment, which can be a virtual, controlled, or real production environment. A monitoring and maintenance facility for managing the SW/HW performance, availability, security, and responding to incidents or issues is also considered. Additionally, the ACCURATE lifecycle forces the use of intelligent surveillance and anomaly detection to provide real-time alerts for unusual activities, allowing for instant investigation and remediation; the adoption of continuous monitoring for performance and security adherence and executing self-healing procedures as needed; simulation of real-world performance in a risk-free environment;
- the ACCURATE *Optimizing* phase is a newly introduced one focused on leveraging decision-making and optimizing the quality experience and resource allocation (Optimizing).

ACCURATE OP activities involve using a controlled environment or authentic context to detect real-time non-compliance and vulnerabilities. It also includes the assessment of the independence and performance of ecosystem components to ensure secure deployment across distributed networks.

As in Figure 1, the ETERNAL stage substitutes the Monitor phase in the standard DevOps process. It includes the *Testing, Verifying* and *Watchguarding* activities. These emphasize the importance of sustained security practices by:

- providing continuous support after SW/HW deployment against emerging vulnerability threats or new weaknesses, and automated continuous testing and regular assessments to ensure ecosystem resilience and regulatory adherence(Testing);
- leveraging feedback loops from real-world incidents and newly discovered vulnerabilities to refine security measures continually and create a self-improving security ecosystem that evolves alongside emerging cyber-threats (Verifying);
- providing regular, automated compliance assessments to ensure that SW/HW upholds industry standards and regulations, seamlessly adapting to changes in the legal landscape (Verifying)
- providing a community-driven Intelligence Sharing to distribute threat intelligence across stakeholders and benefit organizations from collective insights and strategies, leading to a more fortified security posture (Watchguarding);
- leveraging security profiles and Hyperledger technology to record all the security information produced in the three stages related to the product,

providing a centralized, homogeneous, and transparent source of information for all the supply chain stakeholders.

Through its three stages, ACCURATE strengthens system resilience and supports organizations in addressing future cybersecurity challenges. By embedding trust, security, and reliability into HW/SW, it helps meet the evolving demands of the digital landscape. The framework addresses regulatory, ethical, and security aspects early on, promoting adoption by SMEs and aligning with EU priorities. It also provides best practices to ease market access and assesses impact in terms of demand, cost savings, job creation, and productivity.

3 PROPOSED ARCHITECTURE

The ACCURATE architecture has been developed considering the lifecycle presented in the previous section and the adoption of some of the most innovative technical solutions. As depicted in Figure 2, ACCURATE implements the following best practices:

- adopting the Open Secure Architecture (OSA)[1] to ensure trustworthy, interoperable, scalable, and cost-effective environments;
- using cloud-native platforms with a Distributed Deployment Engine (DDE) for secure, scalable, and reliable deployments across cloud and edge locations;
- integrating advanced automation and contextual analysis to enhance user experience and reduce development costs;
- enforcing security through multi-factor authentication, blockchain-based audit trails, and security profiles to ensure integrity and accountability;
- supporting virtualized env for HW/SW simulation, testing, and vulnerability documentation;
- enabling continuous monitoring for dynamic risk assessment, threat adaptation, and certification support;
- following a Zero-Trust architecture: verifying all operations, minimizing access rights, and enforcing strict control and monitoring.

Figure 2 illustrates the architecture, which includes five core components: *Zero-Trust Gateway*, *DevXOp Planner*, and the virtual containers *DEV*, *OPs*, and *ETERNAL*. These are built on the Function-as-a-Service (FaaS) paradigm, supporting local, cloud, and hybrid execution with integrated storage and data persistence.

3.1 Zero-Trust Gateway

The *Zero-Trust Gateway* is the access manager of the serverless OSA architecture implemented, which includes the facilities to guarantee the zero-trust paradigm. This component should be deployed locally for higher data residency security in the target environment, where several security facilities are running. The *Ethical Monitoring and Boundary Protection System* ensures that the oversight is transparent, consensual, privacy-respecting, proportional, and compliant with laws and moral standards. The *Boundary Protection System* monitors and controls the flow of information across network boundaries, implementing data inspection, traffic filtering, and providing an encrypted and secure traffic gateway to the platform.

The *Zero-Trust Gateway* features include mechanisms that integrate Access Control Policies, ensuring access to essential resources is limited for realizing the zero-trust paradigm and Identity Management that continuously checks the right to invoke specific functionalities following the FAAS (Function as a Service) paradigm adopted in the overall OSA architecture. For implementing the *Zero-Trust Gateway* and its components, possible suggestions could rely on the integration of tools like: Perimeter81[2], Cisco Umbrella[3], Microsoft Azure, Amazon Lambda, Splunk[4].

3.2 DevXOp Planner

The *DevXOp Planner* is a component that aims to guide users to use the proposed architecture more proficiently. It is in charge of suggesting and generating interaction workflow among the components included in the three virtual containers: `DEV`, `OPs`, and `ETERNAL`. These workflows are generated taking into account *Guidelines for Certification* and *Regulatory and Barriers* components that provide information about tools and methodologies available for ensuring standards and regulation compliance (such as ISO, GDPR, Security Protocol RED Directive, AI Act, Cyber Resilience Act, Data Act).

As described in Section 2, within the proposed Serverless OSA, there are three virtual containers, called respectively `DEV`, `OPs`, and `ETERNAL`. Their

[1]https://www.opensecurityarchitecture.org/cms/about/why-have-osa

[2]https://www.perimeter81.com/

[3]https://umbrella.cisco.com/

[4]https://www.splunk.com/

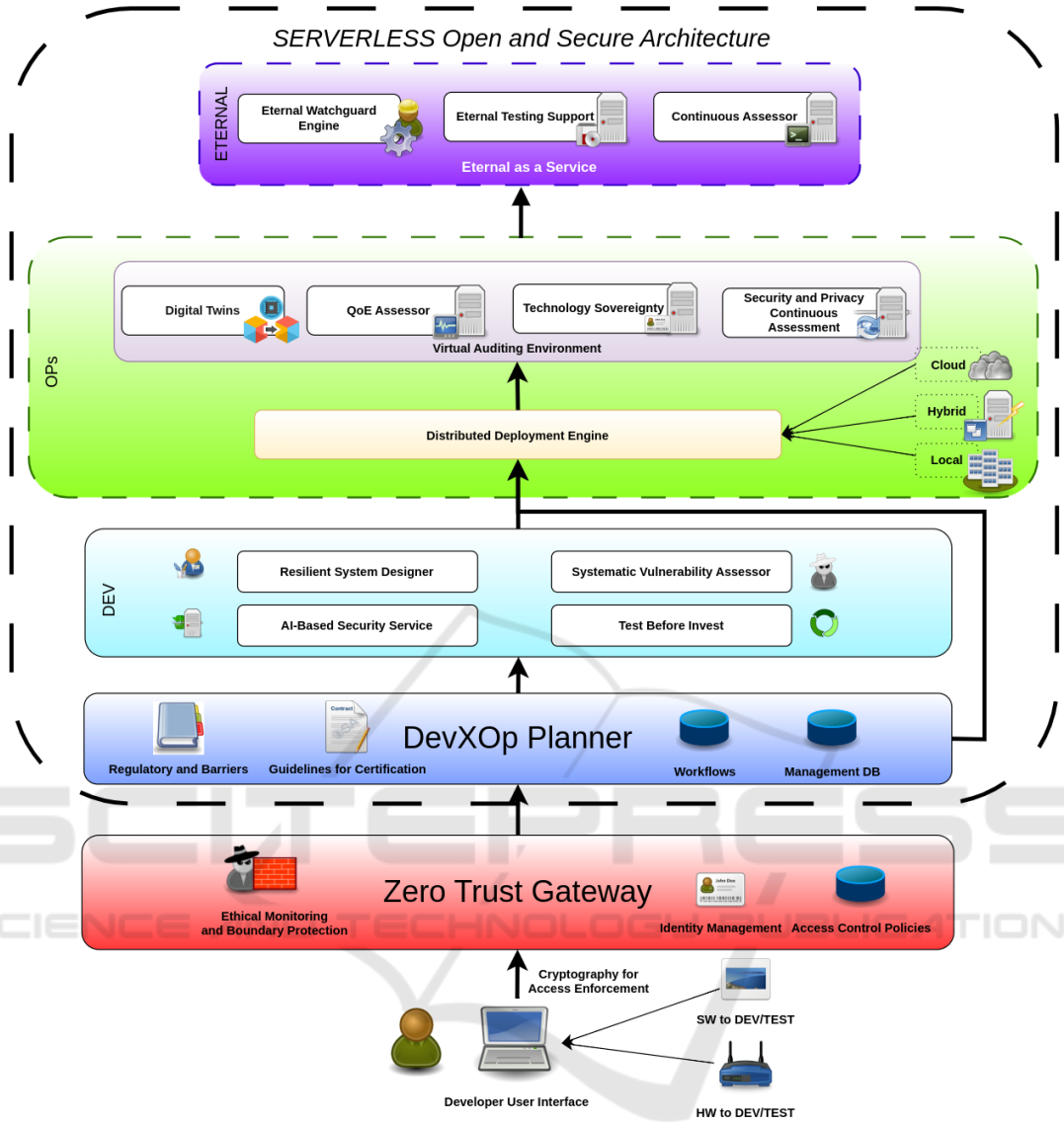

Figure 2: Accurate architecture overview.

names identify the phases in which the components instantiated on it will operate to ensure and enforce the security of the tested HW/SW. In the following subsection, each virtual container will be described.

3.3 DEV Virtual Container

The *DEV* virtual component offers HW/SW development features for threat detection, misconfiguration identification, AI-enhanced security, and AI solution assessment. The components that refer to this virtual component are used in the software lifecycle phase, in which the product is designed, developed, implemented, verified, and even certified before its release to the market or put in execution. At the end of these processes, the product is intended to be ready for execution and validation. Specifically, four components are part of this virtual container: i) *Resilient System Designer*; ii) *AI-Based Security Service*; iii) *Systematic Vulnerability Assessor*, and iv) *Test Before Invest*.

The *Resilient System Designer* analyses potential threats and vulnerabilities in the components/libraries that will be integrated to identify weak points that could compromise system resilience. It provides built-in capabilities to detect, mitigate, and recover from cyberattacks or unexpected failures, ensuring continuous operation is developed. Furthermore, the component includes features to create models that simulate various attack vectors or failures, which helps assess its ability to respond and adapt to disrup-

tions. The *AI-Based Security Service* component enhances the security of HW/SW, which has been developed using AI services. It also improves the security of systems and ecosystem components using artificial intelligence and machine learning approaches.

Systematic Vulnerability Assessor component performs automated scanning of SW and networks to identify known and unknown vulnerabilities, such as misconfigurations, outdated SW, or unpatched security flaws. It uses CVE or other data sources available in the security profile (e.g., Software Bill Of Materials (SBOM) (Kawaguchi et al., 2024)). It prioritizes vulnerabilities based on their criticality, guiding security teams on which issues to address first to mitigate the highest risks. Finally, the *Test Before Invest Profiler* tests and validates HW/SW security before making any significant investment or deployment. It also assesses HW/SW resilience, trustworthiness, and security within the ecosystem.

3.4 OPs Virtual Container

The *OP*s virtual component supports HW/SW during operational execution (runtime or in controlled environments), ensuring security, privacy, and continuous assessment of functional and non-functional properties. It prevents untrusted or malicious actions that may affect digital sovereignty. Artifacts can run in secure local, hybrid, or remote environments, including integration with Digital Twin (DT) facilities.

It includes: i) *Distributed Deployment Engine*; ii) *Digital Twins*; iii) *QoE Assessor*; iv) *Technology Sovereignty*; and v) *Security and Privacy Continuous Assessment*.

The *Distributed Deployment Engine* automates secure HW/SW deployment across distributed ecosystems, supporting fault-tolerant execution on edge or cloud infrastructures, adaptable to user requirements.

The *Virtual Auditing Environment* enables continuous monitoring of HW/SW and the supply chain, detecting vulnerabilities and ensuring compliance through automated data collection and analysis. The main OPs tools operate within this component.

The *Digital Twins* simulate threat scenarios in parallel with the deployed artifact, enabling early detection of behavioral deviations and evaluation of mitigation strategies.

The *QoE Assessor* evaluates runtime performance from the user's perspective, focusing on latency, availability, reliability, and security aspects affecting experience.

The *Technology Sovereignty* component verifies the independence of SW/HW and infrastructure from foreign or untrusted control, ensuring sovereignty over sensitive data and systems.

Lastly, the *Security and Privacy Continuous Assessment* automates compliance checks with frameworks like GDPR and ISO, focusing on encryption, access control, and policy adherence within a socio-technical context.

3.5 ETERNAL Virtual Container

The realization of the newly introduced *ETERNAL* virtual component shown in Figure 2 provides HW/SW features useful after the release of the software developed or assessed through the proposed *ACCURATE* platform. It ensures continuous and eternal testing, assessment, and monitoring of the artifact against emerging threats. Specifically, the *ETERNAL* virtual component includes the *Eternal Watchguard Engine* that ensures continuous monitoring of the system and ecosystem for any possible variation related to connected services, API, and regulation of behavior. It oversees the execution of self-healing procedures. It also includes sharing relevant security information with interested parties to preserve privacy and create a collaborative environment over the supply chain.

The *Eternal Testing Support* enables continuous and eternal deployment of automated testing of SW and system components at every development lifecycle stage, from integration to deployment and post-deployment. The strategies proposed are related to QoE testing, security testing, integration testing, load and stress testing.

Finally, the *Continuous Assessor* ensures regular assessment for vulnerabilities and compliance, leading to a more resilient ecosystem. It notifies the involved stakeholders of the continuous health and performance of the ecosystem through KPI evaluation. It ensures that organizations meet regulatory requirements without the burden of manual checks and audits. Using Hyperledger technology (Roy and Ghosh, 2024), `ACCURATE` ensures all the relevant information about the product (i.e., security profile) is available, updated, and securely stored.

4 RELATED WORK AND ACCURATE INNOVATION

This section presents an overview of the recent proposals and solutions close to the ACCURATE proposal. In particular, the solutions leveraging the DevOps approach are described in Section 4.1 while those closer to the continuous auditing support are

presented in Section 4.2. In each subsection, the innovations provided by the ACCURATE solution are also discussed.

4.1 Leveraging DEVOPs

As anticipated in the introduction, currently, a lot of attention is devoted to leveraging the DevOps processes (Azad and Hyrynsalmi, 2023; Baird et al., 2022). For example, the DevSecOps framework (Rajapakse et al., 2022) strengthens DevOps by incorporating security practices into the software development and delivery processes. The DXO4AI (Calabrò et al., 2024) model conceptualizes a DevOps lifecycle for AI-based SW applications, enabling the design, implementation, and assessment of functional, non-functional, and ethical features. The necessity to improve security and trust in response to market demands promotes approaches like Cyber Threat Intelligence (CTI) sharing (Yang et al., 2025), Structured Threat Information Expression (STIX) sharing (Sadique et al., 2018), Trusted Automated eXchange of Intelligence Information (TAXII)[5]. However, this proposal often lacks comprehensive safeguards for sensitive data, focuses on isolated aspects, such as the definition of security policies or SW composition, or creates fragmented and complex security environments. The ACCURATE project proposes innovations inspired by DXO4AI to enhance the lifecycle management of HW/SW. *ACCURATE* integrates Development (DEV), Operations (OP), and an `Eternal` stage. In particular, this: i) enables continuous analysis, testing, and evaluation throughout the lifecycle; ii) extends CI/CD methodologies to focus on security, privacy, trustworthiness, and quality of experience, introducing continuous automated testing and assessments for HW/SW; iii) supports certification processes by gathering runtime evidence, guides constant process improvement, and addresses societal and ethical concerns while improving human-centric methods and tools; iv) anticipates and mitigates risks while collecting data for future improvements and knowledge sharing; v) integrates diverse security information into unified security profiles to centralize data, enhance traceability, and streamline management; vi) fosters a secure, efficient, collaborative environment, addressing vulnerabilities and enabling improvements.

4.2 Continuous Auditing Support

Emerging technologies help manage technical and methodological challenges in hybrid, cloud, and local systems. Blockchain ensures data integrity and auditability, with tools like Merkle Trees (Kuznetsov et al., 2024) supporting tamper-proof cloud logs. AI and machine learning (Alrashdi et al., 2024) enhance anomaly detection, automate threat response, and streamline audits. Confidential computing, through Trusted Execution Environments (TEEs) (Shepherd and Markantonakis, 2024), and homomorphic encryption support secure and privacy-preserving data processing. Federated models (Hosseingholizadeh et al., 2024) help enforce policies across distributed systems, reducing fragmented practices. SIEM platforms like Splunk offer scalable, AI-enhanced threat monitoring. Risk-based auditing frameworks leverage predictive models (e.g., Bayesian Networks, Attack Trees), while services like PTaaS (Li et al., 2015) strengthen post-deployment resilience. ACCURATE addresses these challenges through a set of integrated innovations: i) adoption of Zero-Trust Architecture, ensuring compliance with GDPR, HIPAA[6]; ii) cloud-native platforms with advanced automation and AI analytics for secure remote audits; iii) multi-factor authentication and blockchain-based trails for integrity and accountability; iv) virtualized environments and security profiles for actionable insights; v) semantic analysis, digital twins, and contextual data for real-time compliance checks; vi) continuous monitoring for dynamic risk assessment; vii) secure distributed deployments via the Distributed Deployment Engine (Wurster et al., 2021); viii) integration of Kubernetes, Talos Linux[7], Headscale[8], and Wireguard[9], leveraging eBPFs[10] for fine-grained traffic policies; ix) automated deployments, self-assessment, and AI-based adaptive monitoring.

5 CONCLUSIONS

The paper presented the ACCURATE lifecycle and supporting framework to provide an innovative proposal to address the pressing challenges of cybersecurity in both software and hardware development. By integrating the DevOps principle and continuous monitoring and assessment throughout the entire lifecycle and introducing the innovative Eternal Stage, ACCURATE targeted the HW and SW trustworthiness, compliance with evolving regulations, and continuous watchguards against emerging threats during development and post-development stages. Through

[5]https://oasis-open.github.io/cti-documentation/

[6]https://www.hhs.gov/hipaa/index.html

[7]https://www.talos.dev/

[8]https://headscale.net/

[9]https://www.wireguard.com/

[10]https://ebpf.io/

its comprehensive methodology, ACCURATE enhanced the traditional continuous development processes, which often neglect the critical need for ongoing vigilance post-deployment and promote collaboration among stakeholders. Looking ahead, further research and development are needed to refine and expand the ACCURATE proposal. Key areas for future work include providing and prototype implementation of the ACCURATE architecture and conducting pilot studies to evaluate the effectiveness of ACCURATE in diverse operational contexts and refine its features based on empirical feedback. Part of the future activity is also to establish collaborations with academic, industrial, and regulatory bodies to promote awareness and best practices surrounding the ACCURATE approach, helping to establish a broader security culture within the technology sector. By pursuing these future directions, the ACCURATE initiative aims to solidify its role as a transformative force in cybersecurity, ensuring that software and hardware systems remain secure and reliable in an ever-evolving digital landscape.

ACKNOWLEDGEMENTS

This work was partially supported by the project project SERICS (PE00000014) under the NRRP MUR program funded by the NextGenerationEU.

REFERENCES

Alrashdi, I., Sallam, K. M., Alrowaily, M. A., Alruwaili, O., and Arain, B. (2024). FIDWATCH: federated incremental distillation for continuous monitoring of iot security threats. *Ad Hoc Networks*, 165:103637.

Aouni, F. E., Moumane, K., Idri, A., Najib, M., and Jan, S. U. (2025). A systematic literature review on agile, cloud, and devops integration: Challenges, benefits. *Inf. Softw. Technol.*, 177:107569.

Azad, N. and Hyrynsalmi, S. (2023). Devops critical success factors - A systematic literature review. *Inf. Softw. Technol.*, 157:107150.

Baird, A., Pearce, H., Pinisetty, S., and Roop, P. (2022). Runtime interchange of enforcers for adaptive attacks: A security analysis framework for drones. In *2022 20th ACM-IEEE MEMOCODE*, pages 1–11. IEEE.

Calabrò, A., Daoudagh, S., Marchetti, E., Aktouf, O., and Mercier, A. (2024). Human-centric dev-x-ops process for trustworthiness in ai-based systems. In García-Peñalvo, F. J., Aberer, K., and Marchiori, M., editors, *WEBIST 2024, Porto, Portugal*, pages 288–295.

Daoudagh, S., Marchetti, E., and Aktouf, O. (2024). 2hcdl: Holistic human-centered development lifecycle. *CoRR*, abs/2405.01566.

Hosseingholizadeh, A., Rahmati, F., Ali, M., Damadi, H., and Liu, X. (2024). Privacy-preserving joint data and function homomorphic encryption for cloud software services. *IEEE Internet Things J.*, 11(1):728–741.

Kawaguchi, N., Hart, C., and Uchiyama, H. (2024). Understanding the effectiveness of SBOM generation tools for manually installed packages in docker containers. *J. Internet Serv. Inf. Secur.*, 14(3):191–212.

Kornecki, A. J. and Zalewski, J. (2010). Safety and security in industrial control. In Sheldon, F. T., Prowell, S. J., Abercrombie, R. K., and Krings, A. W., editors, *CSIIRW 2010, Oak Ridge, TN, USA*, page 77. ACM.

Kuznetsov, O., Kanonik, D., Rusnak, A., Yezhov, A., and Domin, O. (2024). Adaptive restructuring of merkle and verkle trees for enhanced blockchain scalability. *CoRR*, abs/2403.00406.

Li, R., Abendroth, D., Lin, X., Guo, Y., Baek, H. W., Eide, E., Ricci, R., and van der Merwe, J. E. (2015). Potassium: penetration testing as a service. In *ACM Symposium on Cloud Computing, SoCC, Hawaii, 2015*, pages 30–42. ACM.

Ma, J. (2024). 2024 annual report on implementation. *FDD's Center on Cyber and Technology Innovation*.

Rajapakse, R. N., Zahedi, M., Babar, M. A., and Shen, H. (2022). Challenges and solutions when adopting devsecops: A systematic review. *Information and software technology*, 141:106700.

Roy, U. and Ghosh, N. (2024). Fabman: A framework for ledger storage and size management for hyperledger fabric-based iot applications. *IEEE Trans. Netw. Serv. Manag.*, 21(3):3140–3151.

Sadique, F., Cheung, S., Vakilinia, I., Badsha, S., and Sengupta, S. (2018). Automated structured threat information expression (stix) document generation with privacy preservation. In *2018 UEMCON*, pages 847–853.

Shepherd, C. and Markantonakis, K. (2024). *Trusted Execution Environments*. Springer.

Syed, N., Khan, M. A., Mohammad, N., Brahim, G. B., and Baig, Z. (2022). Unsupervised machine learning for drone forensics through flight path analysis. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE.

Wurster, M., Breitenbücher, U., and et al., A. B. (2021). Automating the deployment of distributed applications by combining multiple deployment technologies. In *CLOSER 2021*, pages 178–189. SCITEPRESS.

Yang, L., Wang, M., and Lou, W. (2025). An automated dynamic quality assessment method for cyber threat intelligence. *Comput. Secur.*, 148:104079.

Zimmermann, O., Pautasso, C., Kapferer, S., and Stocker, M. (2024). Continuous integration and delivery in open source development and pattern publishing: Lessons learned with tool setup and pipeline evolution. *IEEE Softw.*, 41(1):9–18.