Securing Networks of the Future: A Programmable Security Monitoring Platform for Cloud Continuum

José María Jorquera Valero*†, Alberto García Pérez†, Gunes Kesik‡, Ömer Faruk Tuna‡
Pietro Giardina¶, Enrico Alberti¶, Lucía Cabanillas Rodríguez‖, Ignacio Dominguez‖,
Diego Lopez‖, Dhouha Ayed§, Manuel Gil Pérez†, Gregorio Martinez Perez†
†*Dept. of Information and Communications Engineering, University of Murcia, Murcia, Spain*
‡*Ericsson Research, Istanbul, Turkey*
¶*Nextworks, Pisa, Italy*
‖*Telefónica Innovación Digital, Madrid, Spain*
§*THALES, Paris, France*

2024 IEEE Future Networks World Forum (FNWF) | 979-8-3503-7949-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/FNWF63303.2024.11028737

***Abstract*—As digital ecosystems evolve toward more integrated and complex architectures, the Cloud Continuum emerges as a vital model that intends to encompass the advantages of cloud, edge, and extreme-edge computing paradigms. This integration, whilst promising in terms of scalability and responsiveness, poses unprecedented security challenges, particularly in enforcing dynamic and adaptive security mechanisms across diverse environments. Existing security solutions may fall short in terms of real-time adaptability and unified management, necessitating a novel approach to orchestrating seamless security. Therefore, this paper presents a programmable security monitoring platform designed to bridge the gap of Cloud Continuum, offering a scalable, distributed, real-time security management framework that accommodates the dynamic nature of forthcoming 6G networks. Furthermore, such an article is also supported and powered by 6G key enablers such as AI-driven Security-as-a-Service to automate security orchestration functionalities using security closed-loops and secure dataspace management for handling and sharing data in distributed scenarios, which are parts of the main functionalities of the ROBUST-6G project.**

***Index Terms*—Security Management, Closed-Loops, Programmable Monitoring Platform, Cloud Continuum, Security Orchestration, 6G Networks**

I. Introduction

The integration of distributed computing paradigms into what is nowadays recognized as the Cloud Continuum has redefined the landscapes of computing infrastructure and data processing [1]. The Cloud Continuum encompasses a seamless security orchestration of resources and services spanning from traditional centralized data centers to edge and extreme-edge computing layers. This evolution intends to address the latency, bandwidth, and extensibility issues inherent in the cloud-only models by bringing computation closer to the data source and end-users, thus ameliorating application responsiveness and operational efficiency.

Nevertheless, as these infrastructures become more integrated, they also face increasing security vulnerabilities. The dynamic nature of the Cloud Continuum, characterized by frequent configuration changes and heterogeneous environments, presents significant challenges in maintaining robust security postures [2]. Traditional security mechanisms, designed primarily for static and well-defined network perimeters, are often ill-equipped to manage the fluid boundaries and varied requirements of contemporary cloud environments.

Despite the critical need for enhanced security measures, current solutions often lack programmability and adaptability, struggling to address the unique characteristics of the Cloud Continuum. In this vein, some solutions are unable to efficiently configure on-demand security policies across different layers of the continuum so as to adapt to the evolving threat landscape in real-time, but they leverage a static pool of security rules [3], [4]. Consequently, there is a pressing need for a programmable security monitoring platform that not only spans across various computing environments but also supports dynamic policy management based on user requirements (Security Service Level Agreements, SSLA) [5] and real-time threat intelligence [6]. In addition, forthcoming security solutions need to be well-aligned with automated security closed-loop operations, guaranteeing the fulfillment of its four phases (Observe-Orient-Decide-Act) and a suitable coordination of reactive and predictive closed-loops.

Hence, this article introduces a Programmable Security Monitoring Platform (PSMP) for 6G-oriented scenarios that needs to emphasize its programmability and adaptability across different computing environments. The platform follows a user-friendly and customizable approach that enables administrators to define and modify security monitoring tools based on users' requirements and SSLAs dynamically. Such security monitoring tools may collect information concerning services, system health, and network traffic running under different assets. Therefore, the Programmable Security Monitoring Platform allows for the real-time detection and mitigation of certain security threats, thereby minimizing the potential impact of such threats across various deployment models. Additionally, this article also presents strategies for integrating the proposed platform with cutting-edge network management and orchestration solutions, i.e., including ETSI ZSM closed-loops [7], Security-as-a-Service solutions, and secure dataspace under Data Fabric.

*Corresponding author: josemaria.jorquera@um.es. This work has been partially funded by the European Commission through the Horizon Europe/JU SNS project ROBUST-6G (Grant Agreement no. 101139068).

The remainder of this article can be outlined as follows. Section II carries out in-depth research into fundamental concepts, the utmost importance related works, and existing technologies in security for Cloud Continuum. Section III describes the parts of the Programmable Security Monitoring Platform for Cloud Continuum, allowing user flexibility and programmability in the security tool configuration. Besides, Section III-B introduces the integration of AI/ML Security-as-a-Service for network orchestration and Section III-C establishes a secure dataspace to enable security intelligence for future networks.

II. Background

Cloud Continuum is a trendy topic in the last years which has been defined in different ways depending on authors and enforcement scenarios. Yet, the most popular definition introduces Cloud Continuum as an extension of the conventional cloud towards several network paradigms (Edge and Extreme-Edge) that support analysis, processing, storage, and data generation capabilities. Thus, thousands of publications have appeared in the last four years to cope with this topics and the security concerns around it.

In this sense, Cohen et al. [8] addressed some cutting-edge Cloud Continuum challenges. In particular, they dealt with optimizing service function chains in the edge-cloud continuum, focusing on resource allocation and migration. Through this article, service chain deployment and resource allocation were faced, guaranteeing service delay and migration requirements. Besides, the authors proposed Bottom-Up-and-Push-Up (BUPU) and Get Feasible Allocation (GFA) algorithms to minimize resource usage while meeting service delay requirements in this continuum. Yet, they did not contemplate security requirements in their research. Likewise, Russo et al. [9] also investigated resource allocation in the Edge-Cloud Continuum through a scalable architecture that seamlessly integrates computing resources at both vertical (Edge to Cloud) and horizontal (among Edge nodes) levels. The authors leveraged adaptive Quality of Service (QoS)-aware policies to adjust resource allocation and prioritize latency-sensitive requests dynamically. Nonetheless, they did not address security features to support resource allocation. On another hand, Domaschka et al. [10] developed a reliable capacity provisioning system for distributed cloud that included a monitoring platform to ensure agreed performance. This platform analyzed live infrastructure data and resources like servers, virtual machines, and applications. However, it lacked the ability for consumers to reconfigure security features in real time, such as expanding monitoring tools to track new performance parameters as we do in the PSMP.

When it comes to security monitoring platforms, Mahmood et al. [11] proposed a self-adapting security monitoring system contemplating tenant's requirements for cloud environments. This solution ensured cost efficiency and responsiveness to dynamic events and supported multiple types of devices to be evaluated. The authors designed an adaptation manager in charge of interpreting high-level tenant requirements and determining whether network Intrusion Detection System (IDS), local or global firewall, and aggregators needed to be run. This solution is well aligned with our proposal although the main difference is that our PSMP offers multiple types of security monitoring tools in relation not only to the devices but also to the network paradigm. In the same direction, Jaraf and Al-Anbagi [12] also presented a real-time security monitoring platform to forecast attacks on IoT networks by leveraging CNN, LSTM, and DNN models. Even though a security monitoring platform was introduced, the authors put the spotlight on pre-processing data and achieving an accurate DL model for detecting traffic attacks reported in the IoT23 dataset. As a result, such research got a masterful 0.8699, 0.9597, and 0.9997 accuracy in detecting attacks for LSTM, CNN, and DNN models, respectively. Nevertheless, they omitted the actions concerning data collection and adaptability during monitoring since they used a public dataset.

Since automation is a crucial pillar together with programmability, many solutions have adopted security closed-loop methodologies to guarantee that their solutions autonomously complete all phases of their lifecycle. García et al. [13] developed an innovative cybersecurity framework that used intra- and inter-domain closed-loops to allow real-time adjustments and continuous feedback on security policies. Their dynamic policy-based approach addressed prediction, mitigation, prevention, and zero-day attack detection. The framework also included dynamic risk assessment graphs to manage network complexities and promote cooperation. However, the article did not specify whether these policies may be only settled in specific software or extendable to different network tools. Emphasizing the relevance of autonomous solutions, Cunha et al. [14] detailed the 6G-OPENSEC-Security project, showcasing the critical role of security closed-loops in transforming security functionalities across multi-operator network environments. Specifically, they outlined the Security Closed-Loop (SCL) framework, designed to continuously monitor, predict, and respond to security threats in real time. In conjunction with SCL, Security Closed-Loop Automation, which used data analytics and automated decision-making for threat detection and response, and Security Closed-Loop Governance, which managed and coordinated security loops, were also key components. Ergo, they fulfilled the utmost important activities of a security monitoring platform through their security closed-loop approach.

As analyzed through Section II, the programmable security monitoring platform, the Cloud Continuum, and the security closed-loops are avant-garde research lines for future 6G networks. Yet, there are not many solutions that attempt to cover all these features in a single solution. Thus, this article presents an AI/ML Security-as-a-Service to securely orchestrate Cloud Continuum, a secure dataspace for integrating and processing data from heterogeneous sources, and a PSMP to offer flexible security tool configurations for future networks (Section III).

III. 6G-ORIENTED SECURITY SOLUTIONS FOR CLOUD CONTINUUM

This section presents an overview concerning the utmost importance security actions of ROBUST-6G project. To begin with, Section III-A describes a security monitoring platform following a reactive and closed-loop approach together with additional functionalities in terms of threat detection and notification. Then, Section III-B emphasizes the importance of security closed-loops to automate security orchestration activities, and lastly, Section III-C points out the role of secure data management in a distributed environment.

A. Automatic monitoring, threat detection and alarm generation

With the rise of Cloud Continuum solutions, new 6G security requirements are emerging to minimize the attack surface of Cloud, Edge, and Extreme-Edge network paradigms. In this sense, programmability and flexibility are crucial features for developing advanced security monitoring solutions. Thereby, this section presents a Programmable Security Monitoring Platform (PSMP) that allows end-users to configure and deploy various monitoring tools based on specific security needs and on-demand network paradigms.

In particular, the PSMP puts the spotlight on automatic monitoring of service, infrastructure, and network levels to afterwards detect potential threats, and generate notifications, considering diverse network paradigms and a reactive closed-loop. When it comes to the PSMP design, it takes into account constraints coming from the emergence of recent heterogeneous devices and novel use cases, e.g., performance, processing and computational limitations that some assets close to Extreme-Edge may have. Therefore, end-users may configure the PSMP based on network paradigms to be protected and security requirements in real time. Besides, the design of PSMP bridges the gap concerning adaptability and flexibility as it enables end-user to decide whether they desire to monitor information on physical devices, containers, virtual machines, etc., at service, network, or infrastructure levels. Hence, the platform is capable of gathering data from:

- *Service level*: to protect the services hosted in devices by analyzing their logs, changes in internal files, threats, etc.
- *Infrastructure level*: to find health metrics such as latency, memory usage, or throughput, among others, to determine the health of the devices and the network.
- *Network level*: to analyze and discover unexpected behavior that could lead to potential threats using monitored network traces.

On another hand, the design of the PSMP is also composed of multiple functional modules or parts such as *Data Collector Manager*, *Communication Manager Bus*, *Aggregation and Preprocessing Manager*, *Alert Manager*, *Configuration Manager*, and *External Interface*.

1) Data Collector Manager: Following a bottom-up approach of Figure 1, the first module is the *Data Collector Manager* in charge of gathering information from available data sources in Cloud Continuum. For example, embedded or hardware-constrained devices, servers deployed on the Edge to optimize streaming services, or cloud computing resources. The *Data Collector Manager* is made up of four security monitoring tools associated with the three aforementioned levels. It is worth mentioning that colors represent the level at which a monitoring tool fits better to ensure constraints and security

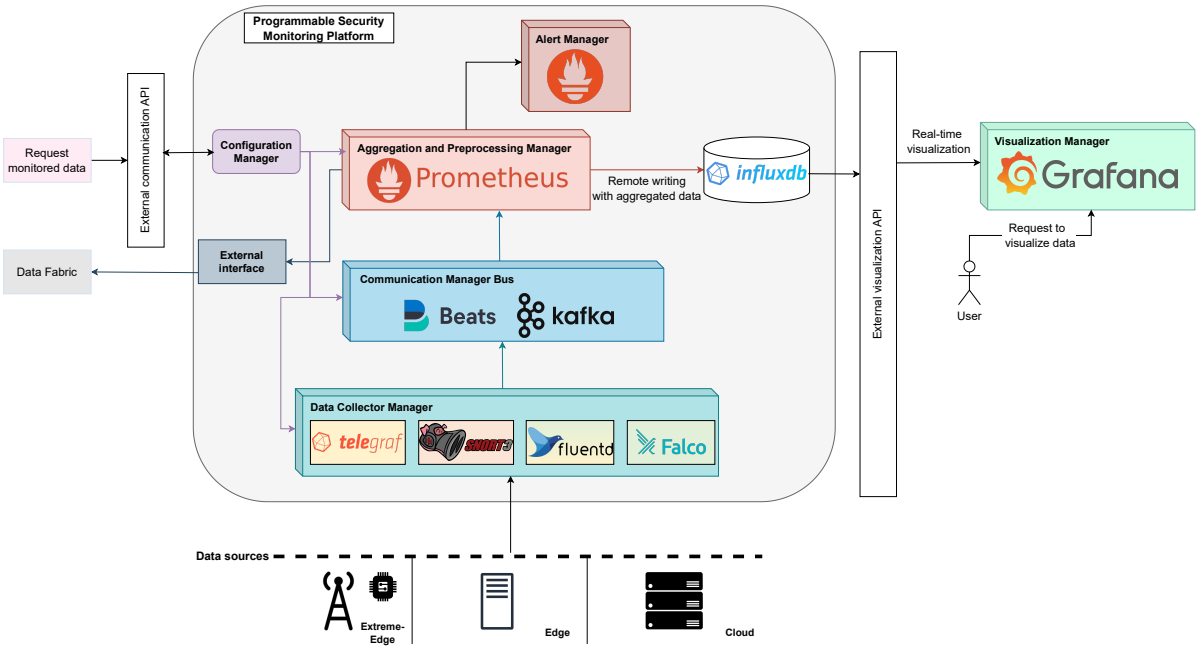

Fig. 1. High-level overview of the Programmable Security Monitoring Platform

needs, being green (service level), yellow (infrastructure level), and salmon (network level). Concretely, the *service level* is supported by Fluentd [15] to collect real-time logs and Falco to protect devices such as hosts, servers, and containers against possible threats, e.g., changes in configuration files to produce unexpected behavior. Concerning the *infrastructure level*, Telegraf [16], more suitable for Extreme-Edge, and Fluentd for Edge are contemplated to obtain on-demand security data. The rationale for having two security monitoring tools to collect health metrics on assets is because the *Data Collector Manager* to be instantiated on the Extreme-Edge needs to deal with potential resource constraints and, in consequence, to support a lightweight monitoring tool like Telegraf. On the other hand, the Edge resources use to have more resources and computing capabilities to deploy and manage Fluentd. Finally, the *network level* is covered by Snort3 [17] to sniff network traces that may act as an Intrusion Detection System (IDS) or rule-based Intrusion Prevention System (IPS) to mitigate rapidly attacks that can affect monitoring tools.

2) Communication Manager Bus: Following the natural data flow, all information extracted by the *Data Collector Manager* is forwarded through the *Communication Manager Bus* using Kafka topics to expose the information to other modules via a publish-subscribe model. Furthermore, this module also leverages FileBeats to communicate Snort3 network traces to Kafka since there is no official software to transmit the information collected by Snort3 to Kafka directly.

3) Aggregation and Preprocessing Manager: All the information sent over the communication bus is consumed by the *Aggregation and Preprocessing Manager*. In particular, this module makes use of Prometheus [18] to scrape the information exposed on the *Communication Manager Bus* and relates the information coming from different channels. Prometheus has an internal module (the *Alert Manager*) to generate alerts in case of unexpected behavior in the aggregated information. This data is also stored in a Time Series Database (TSDB) called InfluxDB. In addition, the external Visualization Manager module, which is not part of the PSMP but interacts with it, brings authorized users the chance to visualize the information, graph, statistics, etc., in real time with Grafana. Lastly, the *External Interface* pushes the aggregated information to a Data Fabric (see Section 3) to enable security intelligence for future networks.

4) Configuration Manager: Last but not least, the *Configuration Manager* performs the settings of each security monitoring tool located in the *Data Collection Manager* as well as dynamically configures other modules within the PSMP, if necessary. The configuration is dynamic because as soon as security closed-loop sends a mitigation in response to a threat, the *Configuration Manager* makes the necessary changes to modify the configuration files of the tools used on this platform. Note that the *Configuration Manager* module is not associated with the traditional orchestration activities but with the Programmable Security Monitoring Platform components. In addition, the Configuration Manager uses a rule-based engine and a monitoring capability repository to match SSLA attributes with appropriate monitoring tools based on factors like performance, security coverage, and environment. In a multi-domain setup (extreme-edge, edge, and cloud), lightweight and efficient tools are deployed at the extreme-edge focusing on high-priority security events, while complex analysis is performed in the cloud on aggregated data from the extreme-edge and edge.

B. AI/ML Security-as-a-Service for network orchestration

The NIST Cybersecurity Framework and its fundamental tasks (identify, protect, detect, respond, and recover) is a widely recognized model for assisting telecom operators in identifying, assessing, and managing cyber security threats [19]. Security management should offer the tools and capabilities required to perform security management operations in telecom networks that are aligned with the major tasks of the NIST framework. This framework serves as the foundation for determining which functions should be included within the scope of the proposed automated security management solution.

Automation plays a critical role in security as threats become more sophisticated and dispersed across various computing layers in Cloud Continuum. Automation can range from straightforward scripts that perform a repetitive process or reactive rules that act automatically based on conditions to potentially sophisticated adaptive security features that adjust security controls and their configurations in response to shifting environmental conditions. This is enabled by closed-loop security control paradigm. A potential use of closed control loop in security would be to employ feedback loops to update the security detection rules parameters in response to changing environments. For example, if an IoT network security detection set of rules is activated based on some threshold circumstances, the assumption is that such thresholds must be updated when traffic patterns change in the protected network to eliminate false positives and provide higher accuracy rates.

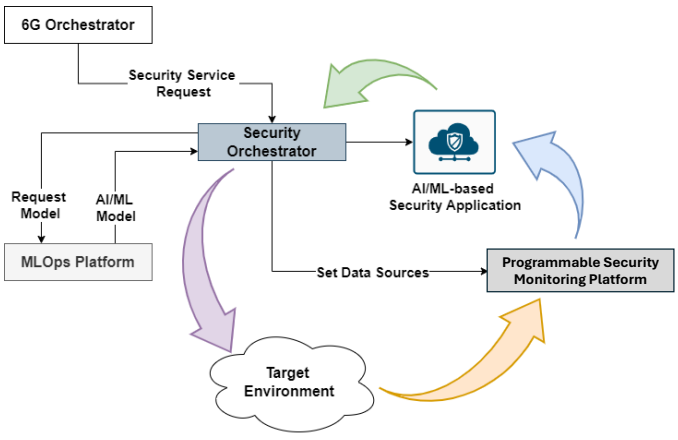

Fig. 2. Security orchestration and AI-Driven Closed-Loop

One key factor enabling the automatic security of services on mobile networks is the specification in the service description itself of certain security requirements the 6G man-

agement platform must fulfill. The key entity of the security orchestration process is the Security Orchestrator (see Figure 2), which silently, i.e., in a transparent manner, parses such security requirements and translates them in actions to be taken to enforce the requested security: in other words, it provisions a security service. The orchestration of dedicated services in charge of guaranteeing the security in the mobile network, basically consists of two steps namely i) provisioning of security i.e., specific configuration to the underlying infrastructure e.g., firewall's rules and ii) automation, i.e., those set of processes capable to guarantee the level of security agreed between the parties at runtime. Step (ii) is usually realized implementing the concept of security closed-loop which can be either reactive i.e., react to at the detection of certain anomalies, as described in Section III-A or predictive, i.e., predict potential incidents on the of the current status of the system and its history. The predictive loop achieve is goal by integrating AI/ML-based analysis/decision processes in charge of making the predictions and deciding the mitigation countermeasures. The AI/ML algorithm necessary for the creation of a security closed-loop could be already integrated in the internal logic of the orchestrator or, following a more dynamic approach, the closed-loop can be provisioned at runtime: this implies that the different stages, including the analysis and the decision, are dynamically configurable. Such an approach allows the orchestrator to select proper AI/ML models fitting the requirements of the security service to be provisioned.

In this regard, one interesting approach is to exploit the services offered by a dedicated MLOps platform, which offers specific interfaces to train, select, and provision a machine-learning base agent given the constraints specified in the request. In particular, Figure 2 displays an example of security service provisioning. The Security Orchestrator receives a request from the 6G Orchestrator, i.e., the mobile network operator orchestrator in charge of managing the 6G services, to provision a security service with certain characteristic. The Security Orchestrator analyzes the security constraints and request a specific AI/ML model to the MLOps platform, to be integrated into the AI/ML-based Security Application which continuously analyzes the state of the target environment. In parallel, the Programmable Security Monitoring Platform is programmed to collects data from certain data sources providing monitoring parameters of interest for the AI/ML-based Security Application. The AI/ML algorithm integrated in the application, continuously analyses the data, looking for potential anomalies. If an anomaly is detected and/or predicted by AI agents, the Security Application requests the Security Orchestrator to enforce corrective actions on the target environment, in order to avoid/mitigate the security issue detected.

C. Secure dataspace for handling distributed and heterogeneous data sources

The evolution of data management in 6G networks calls for advanced data infrastructures capable of integrating heterogeneous data sources and ensuring robust data governance. Such data infrastructures aim to facilitate the collection, integration, and governance of data across various levels and segments of 6G networks, ensuring trustworthy data sharing and compliance with data governance principles [20]. In this sense, this section introduces a distributed data infrastructure for enabling a 6G dataspace within the scope of ROBUST-6G, following the latest trends in data management.

The 6G dataspace leverages the data fabric and data mesh paradigms to manage and govern data flows. Data fabric provides a unified architecture for integrating and processing data from diverse sources, enhancing data accessibility and governance [21], as shown in Figure 3. Data mesh, on the other hand, advocates for managing data as a product and decentralizing data ownership, making teams accountable for governing and sharing data domains independently, promoting agility and scalability [22].

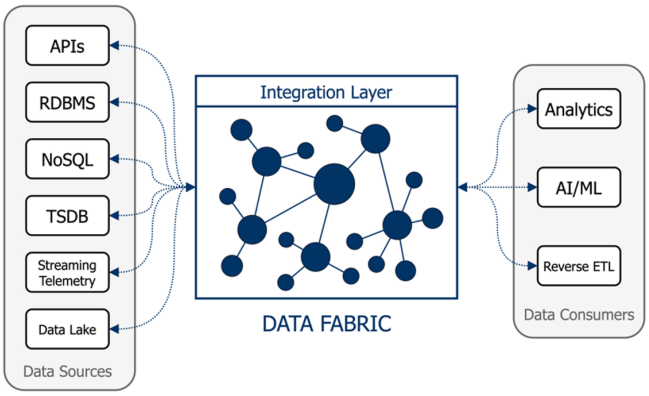

Fig. 3. Data fabric architecture

Security is a paramount concern in the 6G dataspace, and the data fabric architecture plays a crucial role in enhancing security across multiple levels. For instance, the Data Fabric enables security functions identifypotential threats by consolidating information from diverse data sources. This positions Data Fabric as a critical data source within the 6G dataspace, contributing significantly to a comprehensive security strategy, as shown in Figure 3, where the consumers of this data are machine learning models used in security applications.

A critical aspect of the 6G dataspace is the implementation of access control at the data level. This granular approach ensures that access permissions are applied directly to individual data elements rather than the data sources themselves. This fine-grained control enhances security by allowing precise regulation of who can access specific pieces of data and under what conditions.

Furthermore, decoupling authentication and authorization responsibilities further strengthen the 6G dataspace's security posture. This separation allows for more granular and adaptable policy management, ensuring that access control mechanisms remain effective against emerging security challenges without impacting authentication processes. This architectural approach mitigates the risk of unauthorized access and data breaches, providing a resilient data infrastructure.

Additionally, the 6G dataspace envisions the integration of digital signatures to ensure data integrity and provenance. Consequently, this guarantees the reliability of machine learning decisions derived from the data, as the integrity and authenticity of the data are assured. This verification process ensures that machine learning models are trained and operate on accurate and trustworthy data, leading to more reliable and valid outcomes [23].

The 6G dataspace represents a significant advancement in the management and governance of data within 6G networks. By integrating the data fabric paradigm and implementing robust access control mechanisms at the data level, the dataspace ensures secure, efficient, and trustworthy data sharing. This approach not only complies with regulatory requirements but also addresses the dynamic security challenges inherent in next-generation network environments.

IV. Conclusion and Future Work

This article presents the necessity of a comprehensive and integrated approach to ensure the security and resilience of the next-generation 6G networks. By implementing a reactive framework, the Programmable Security Monitoring Platform effectively addresses some of the security challenges posed by the Cloud Continuum environments allowing user flexibility and programmability in the security tool configuration. The automated monitoring, threat detection, and alarm generation functionalities enhance the capability to preemptively identify and mitigate potential threats across service, network, and infrastructure levels. Besides, the integration of AI/ML Security-as-a-Service for network orchestration and the establishment of a secure dataspace also enhance the platform's security of the ROBUST-6G project. AI/ML models continuously learn to predict and counteract threats, improving security posture and the secure data space, emphasizing granular access control, data integrity, and provenance, ensuring secure data management and sharing.

As future work, several avenues can be explored to enhance the capabilities and scope of the ROBUST-6G security platform. Concerning the Programmable Security Monitoring Platform, a dynamic rule configuration engine would leverage real-time user inputs and contextual data to generate customized security rules that adapt to varying security needs and scenarios. To this end, natural language processing techniques are conceived to interpret user requirements and translate them into precise, actionable rules. Regarding security orchestration, a novel E2E security orchestration system based on the ZSM approach takes control of the overall security of network domains, providing efficient security management where there is an optimum splitting and configuration of security functionalities. When it comes to dataspace, it will develop and optimize granular access control mechanisms within the 6G dataspace. This research would aim to ensure access control at the data level, allowing precise and dynamic regulation of access permissions directly on individual data elements rather than at the source level. Lastly, Proof-of-Concept deployments in real-world scenarios will provide valuable insights and feedback, guiding further refinements and enhancements, as the ROBUST-6G project is currently in month 9 addressing the design phases.

References

[1] M. A. Uusitalo et al., "Hexa-X the European 6G flagship project," in *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 580–585.

[2] P. Soumplis et al., "Resource allocation challenges in the cloud and edge continuum," in *Advances in Computing, Informatics, Networking and Cybersecurity*. Springer, 2022, pp. 443–464.

[3] M. M. M. Rahman, S. Tarek, K. Z. Azar, M. M. Tehranipoor, and F. Farahmandi, "Efficient soc security monitoring: quality attributes and potential solutions," *IEEE Design & Test*, vol. 41, pp. 26–34, 2023.

[4] R. Croft, D. Newlands, Z. Chen, and M. A. Babar, "An empirical study of rule-based and learning-based approaches for static application security testing," in *Proceedings of the 15th ACM/IEEE international symposium on empirical software engineering and measurement*, 2021, pp. 1–12.

[5] F. Qazi, D. Kwak, F. G. Khan, F. Ali, and S. U. Khan, "Service level agreement in cloud computing: Taxonomy, prospects, and challenges," *Internet of Things*, p. 101126, 2024.

[6] D. Rosendo, A. Costan, P. Valduriez, and G. Antoniu, "Distributed intelligence on the Edge-to-Cloud Continuum: A systematic literature review," *Journal of Parallel and Distributed Computing*, vol. 166, pp. 71–94, 2022.

[7] ETSI Group Specification. GS ZSM 009-1 V1.1.1: Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers. [Online]. Available: https://www.etsi.org/deliver/

[8] I. Cohen, C. F. Chiasserini, P. Giaccone, and G. Scalosub, "Dynamic service provisioning in the edge-cloud continuum with bounded resources," *IEEE Transactions on Networking*, vol. 31, no. 6, pp. 3096–3111, 2023.

[9] G. R. Russo, T. Mannucci, V. Cardellini, and F. L. Presti, "Serverledge: Decentralized function-as-a-service for the edge-cloud continuum," in *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2023, pp. 131–140.

[10] J. Domaschka et al., "Towards an architecture for reliable capacity provisioning for distributed clouds," *Managing Distributed Cloud Applications and Infrastructure: A Self-Optimising Approach*, pp. 1–25, 2020.

[11] S. Mahmood et al., "Self-adapting security monitoring in eucalyptus cloud environment," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, 2023.

[12] I. B. Jafar and I. Al-Anbagi, "Rsm: A real-time security monitoring platform for iot networks," in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2023, pp. 393–398.

[13] S. C. Garcia, E. G. D. L. C. Molina, A. M. Zarca, and A. F. S. Gomez, "Dynamic zsm multi-operator policy based security framework for b5g infrastructures," in *IEEE Future Networks World Forum*, 2023, pp. 1–6.

[14] J. Cunha et al., "Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies," *Future Internet*, vol. 16, p. 226, 2024.

[15] P. Späth, "Logging pipeline with fluentd," in *Pro Jakarta EE 10: Open Source Enterprise Java-based Cloud-native Applications Development*. Springer, 2023, pp. 427–436.

[16] P. Rattanatamrong et al., "Overhead study of telegraf as a real-time monitoring agent," in *17th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. IEEE, 2020, pp. 42–46.

[17] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source ids? snort, suricata or zeek," *Computer Networks*, vol. 213, p. 109116, 2022.

[18] T.-T. Nguyen, Y.-J. Yeom, T. Kim, D.-H. Park, and S. Kim, "Horizontal pod autoscaling in kubernetes for elastic container orchestration," *Sensors*, vol. 20, no. 16, p. 4621, 2020.

[19] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0." [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[20] European Commission, "European data governance act." [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[21] A. Gupta, "Data fabric architecture is key to modernizing data management and integration," *Gartner*, 2021.

[22] J. Christ, L. Visengeriyeva, and S. Harrer, "Data mesh architecture." [Online]. Available: https://www.datamesh-architecture.com

[23] IBM, "What if a data fabric architecture guided decision-making?" [Online]. Available: https://www.ibm.com/data-fabric