Towards privacy-first security enablers for 6G networks: the PRIVATEER approach*

Dimosthenis Masouros[1], Dimitrios Soudris[1], Georgios Gardikis[2], Victoria Katsarou[2], Maria Christopoulou[3], George Xilouris[3], Hugo Ramón[4], Antonio Pastor[4] Fabrizio Scaglione[5], Cristian Petrollini[5], António Pinto[6], João P. Vilela[6], Antonia Karamatskou[7], Nikolaos Papadakis[7], Anna Angelogianni[8], Thanassis Giannetsos[8], Luis Javier García Villalba[9], Jesús A. Alonso-López[9] Martin Strand[10], Gudmund Grov[10], Anastasios N. Bikos[11], Kostas Ramantas[11], Ricardo Santos[12], Fábio Silva[12], and Nikolaos Tsampieris[13]

[1] National Technical University of Athens, Greece
[2] R&D Department, Space Hellas S.A., Greece
[3] NCSR "Demokritos", Institute of Informatics and Telecommunications, Greece
[4] Telefonica I+D, Spain
[5] RHEA Group, Belgium
[6] INESC TEC, Portugal
[7] Infili Technologies S.A., Greece
[8] Ubitech Ltd., Digital Security Trusted Computing Group, Greece
[9] Universidad Complutense de Madrid, Spain
[10] Norwegian Defence Research Establishment (FFI), Norway
[11] Iquadrat Informatica S.L., Barcelona, Spain
[12] Polytechnic of Porto, Portugal
[13] ERTICO-ITS Europe, Belgium

Contact: privateer-contact@spacemaillist.eu

Abstract. The advent of 6G networks is anticipated to introduce a myriad of new technology enablers, including heterogeneous radio, RAN softwarization, multi-vendor deployments, and AI-driven network management, which is expected to broaden the existing threat landscape, demanding for more sophisticated security controls. At the same time, privacy forms a fundamental pillar in the EU development activities for 6G. This decentralized and globally connected environment necessitates robust privacy provisions that encompass all layers of the network stack. In this paper, we present PRIVATEER's approach for enabling "privacy-first" security enablers for 6G networks. PRIVATEER aims to tackle four major privacy challenges associated with 6G security enablers, i.e., i) processing of infrastructure and network usage data, ii) security-aware orchestration, iii) infrastructure and service attestation and iv) cyber threat intelligence sharing. PRIVATEER addresses the above by introducing several innovations, including decentralised robust security analytics, privacy-aware techniques for network slicing and service orchestration and distributed infrastructure and service attestation mechanisms.

Keywords: B5G & 6G Networks · Security & Privacy · Horizon Europe

* This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the EU Horizon Europe programme PRIVATEER under Grant Agreement No. 101096110. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the EU or SNS JU.

1 Introduction

The widespread adoption of 5G networks has brought significant advancements in connectivity, catering for the escalating demands of mobile users and emerging technologies. However, as the number of devices connected to the network continues to skyrocket [29], and the demands of deployed applications grow increasingly complex, characterized by higher bandwidth and lower latency requirements [13], it is becoming apparent that 5G's capabilities may not be sufficient to meet all the demands of this quickly changing digital environment. To this end, the development and implementation of Beyond 5G (B5G) and 6G networks have become imperative. By pushing the boundaries of wireless communication, 6G will play a pivotal role in meeting the escalating demands of IoT devices and supporting the strict requirements of next-generation applications [12, 24].

While 6G networks hold immense promise in meeting the evolving connectivity needs, they also bring forth new challenges, particularly in the realm of security [19]. The expanded scope and complexity of 6G, encompassing diverse technologies such as heterogeneous radio, RAN softwarization, multi-vendor deployments and AI-driven network management, introduce novel security vulnerabilities and threats [12, 15]. As the network becomes more distributed and interconnected, ensuring robust security measures becomes crucial to safeguard against potential cyber threats and privacy breaches.

On top of that, privacy holds a prominent position in the European Union's research and development endeavors towards 6G networks, reflecting its significance as a fundamental societal concern within the EU's vision for 6G [5]. The envisioned 6G landscape is characterized by a decentralized, zero-trust framework, fostering a globally interconnected network of diverse environments involving multiple stakeholders across the service chain, including infrastructure providers and service providers. In this multifaceted setting, privacy assumes a pivotal role, extending its significance beyond end users to encompass all involved parties, necessitating its recognition as a critical prerequisite across the entire network stack, encompassing security mechanisms as well. From the above, it is evident that novel frameworks are required to tackle this multi-level security and privacy requirements imposed both by end-users as well as societal factors.

To this end, in this paper we present an overview of the PRIVATEER[14] Horizon Europe project. PRIVATEER aims to provide a privacy-centric security framework specifically designed for future 6G networks. As 6G networks are anticipated to facilitate more advanced use cases with increased user involvement, the sharing of sensitive data among various stakeholders, such as service providers, infrastructure providers, third parties, and even users themselves, is expected to grow rapidly. To safeguard the privacy of stakeholders' sensitive data, PRIVATEER leverages and enhances existing technologies, including decentralized federated learning powered by edge AI acceleration, distributed ledger technology (DLT) integrity controls, privacy- and resource-driven optimization of service orchestration, and threat sharing utilizing searchable encryption.

[14] https://www.privateer-project.eu/

2 PRIVATEER's Goals & Addressed Challenges

The ultimate goal of PRIVATEER can be summarized in the following sentence:

The mission of PRIVATEER is to pave the way for 6G "privacy-first security" by studying, designing and developing innovative security enablers for 6G networks, following a privacy-by-design approach.

More specifically, PRIVATEER aims to tackle four distinct privacy challenges that are closely linked to the security enablers that have been introduced in the existing 5G landscape, i.e.,:

1. **Privacy concerns in the processing of infrastructure and network usage data for security analytics:** The highly heterogeneous and distributed nature of B5G/6G network components generates a vast amount of diverse data, including logs, flow data, and monitoring information, which, when analyzed in a timely manner, can effectively detect security incidents. *PRIVATEER will adopt a decentralized approach to security analytics, utilizing anti-adversarial AI techniques for more robust models.* This decentralization will leverage edge computing and federated AI techniques to distribute storage and processing. Moreover, Explainable AI (XAI) will be employed to enable human operators to align operations with privacy constraints.
2. **Privacy concerns in the slicing and security orchestration processes:** Network slicing and dynamic orchestration of security services have facilitated tenant isolation and "security as a service" (SecaaS) [28]. *PRIVATEER aims to enable privacy-aware slicing and security service orchestration, considering the user's privacy intent and constraints as input for intent-based networking.* This involves placing core and edge components in trusted infrastructure domains and ensuring the integrity of the traffic path through proof-of-transit verification.
3. **Privacy concerns in infrastructure and service attestation and integrity check procedures:** In the context of 6G, a multi-actor environment is expected, where the network service chain traverses infrastructures from multiple providers and involves various developers. Trust is crucial in such a diverse ecosystem, necessitating attestation and integrity verification processes. *PRIVATEER proposes a distributed approach, leveraging verifiable credentials and decentralized identifiers (DIDs).* Using a permissioned blockchain as decentralized storage, stakeholders can prove the integrity of their assets through recorded certificates and proofs of attestation.
4. **Privacy concerns in cyber threat intelligence (CTI) sharing:** To enhance the detection and response capabilities of 6G stakeholders, the timely exchange of cyber threat information is crucial, including specific insights related to 6G components. *PRIVATEER aims to overcome this challenge by implementing searchable encryption and distributed indexing mechanisms.* These technologies enable fine-grained control over information exposure, ensuring privacy by facilitating policy-based sharing of threat information stored in MISP platforms [23].

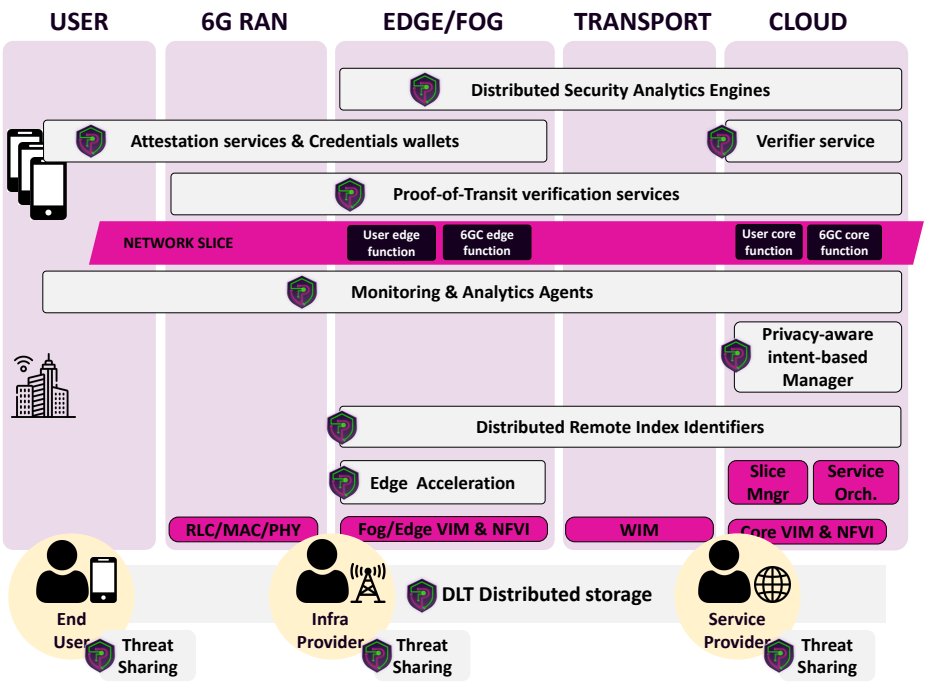

Fig. 1: High-level architecture identifying PRIVATEER's Security Enablers

3 PRIVATEER's Architecture

Figure 1 presents an overview of the PRIVATEER framework, where the existing B5G infrastructure is represented in color, while the value-added components of PRIVATEER are highlighted with the projects's logo in grey boxes. PRIVATEER introduces advancements in three primary domains, namely, *i)* Decentralised and robust security analytics, *ii)* Privacy-aware slicing and orchestration and *iii)* Distributed attestation and threat sharing. Next, we provide a high-level overview of PRIVATEER's architecture and, then, we describe in more detail the technical details for each one of the enablers considered.

3.1 High-Level Overview

The framework identifies three main stakeholder roles, i.e., 1) End Users, 2) Infrastructure Providers/Neutral Hosts and 3) Service Providers, each belonging to distinct administrative domains. These stakeholders can share cyberthreat intelligence using established platforms (e.g., MISP [23]), employing searchable encryption to protect sensitive information [3, 8]. PRIVATEER framework encompasses five security management domains, spanning from the User, to the Radio Access Domain (RAN), to the Edge/Fog Domain, to the Transport Network and up to the Core Cloud. The User Domain is treated as a separate entity

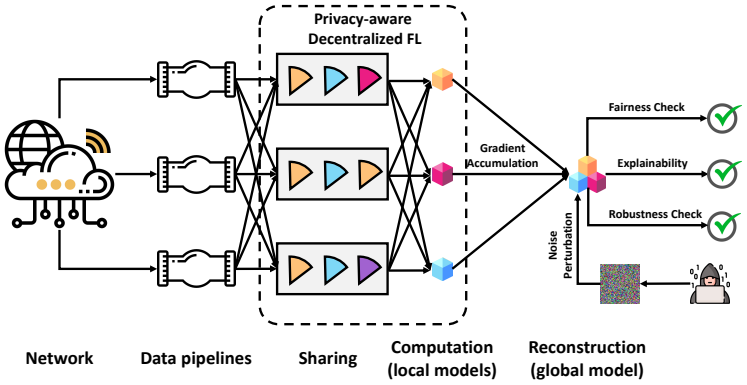

Fig. 2: Privacy-aware, decentralized FL framework for security analytics

where local analytics engines operate on the user's infrastructure, utilizing local AI/ML models for generating insights. These local models are then distributed to the Edge/Fog Domain, enabling the training of global AI/ML models through federated learning with the support of Edge AI acceleration. This approach preserves user privacy and enhances local data storage capacity. Within each management domain, a verification service for Proof-of-Transit (PoT) is implemented to ensure secure validation of service paths. Moreover, Service Providers utilize an attestation service to authenticate devices/services provided by Infrastructure Providers, confirming the integrity of the host's core-edge continuum through a distributed attestation mechanism driven by DLT, eliminating the reliance on a central authority. The authentication of stakeholder credentials by external verifier services is facilitated by decentralized identifiers, represented as a credentials wallet, enabling the verification process without the direct sharing of sensitive user data.

3.2 Decentralised Robust Security Analytics

PRIVATEER builds upon the existing knowledge and expertise in 5G security analytics, specifically focusing on the utilization of AI techniques to detect and classify network threats, including analyzing traffic information, logs, and metrics from multiple network points, utilizing specialized Monitoring and Analytics agents distributed throughout the network continuum. To enhance the privacy aspect of security analytics, PRIVATEER adopts the principles of decentralized federated learning (FL), enhanced with additional data analytics pipelines and features to address key trustworthiness requirements, including privacy and fairness, robustness, and explainability, as shown in Figure 2.

► In the context of *privacy and fairness preservation*, PRIVATEER focuses on balancing the fairness-privacy tradeoff, by incorporating the latest advancements in training strategies and protocols for the development of both private and fair learners [9, 11], which aim to find the optimal combination between these two

conflicting concepts for classification purposes. Moreover, in the context of *outlier detection*, PRIVATEER utilizes fair machine learning models like Deep Fair SVDD [25], FairOD [21], and FairLOF [2], coupled with privacy-preserving techniques such as anonymization, cryptography, and perturbation. To address class imbalances, ensemble techniques like bagging and boosting are employed during pre-processing and post-processing stages, aiming to create discrimination-free models while maintaining high detection performance.

▶ With respect to the *adversarial AI robustness evaluation*, PRIVATEER addresses both private information leaking and poisoning attacks, through cryptographic methods and adversarial techniques. First, the framework employs multiparty computation (MPC) [20] and differential privacy (DP) [10] for secure gradient sharing in decentralized collaborative settings, which allows computing nodes to output the completed model without being able to learn any information about the private gradients of each individual. Second, the framework also adopts GAN-based techniques to decentralized federated learning (FL) to enhance robustness against adversarial inference and poisoning attacks [26, 18]. By combining robustness metrics (based on needed perturbations on input data to change its classification) with metrics that use latent space performance metrics the framework provides feedback to the federated learning (FL) architecture, enhancing system robustness and improving the FL model's performance against adversarial attacks.

▶ For *explainability*, PRIVATEER considers and combines several different approaches from the Explainable AI (XAI) domain, which aims to make ML models understandable, interpretable, and transparent. First, PRIVATEER adopts ML approaches that are explainable by design (a.k.a. "white-box models"), e.g., decision trees, random forests and statistically based algorithms, which allow human experts to audit and interpret results directly from their structure. For "black-box" models (e.g., Deep Learning models) different strategies are employed such as scope (global vs local model interpretability); method (backpropagation or perturbance strategy); and usage (intrinsic or post-hoc methods) to build explanation models [7]. PRIVATEER leverages a comprehensive combination of these approaches to improve explainability, enabling 6G security operators to make more efficient decisions. The goal is to enhance various properties including causality, transferability, informativeness, confidence, fairness, accessibility, interactivity, as well as privacy awareness or its absence.

3.3 Privacy-aware Slicing and Orchestration

In the context of slicing and orchestration, PRIVATEER introduces several novel components that enable privacy awareness and users' intent in the process, as well as securing the service path. Specifically, the PRIVATEER framework will focus on enabling trustworthy network topologies and providing privacy-aware orchestration mechanisms based on user-specific requirements. Figure 3 shows an overview of PRIVATEER's approach w.r.t. network slicing and orchestration, where the components included in dashed boxes show the innovations introduced

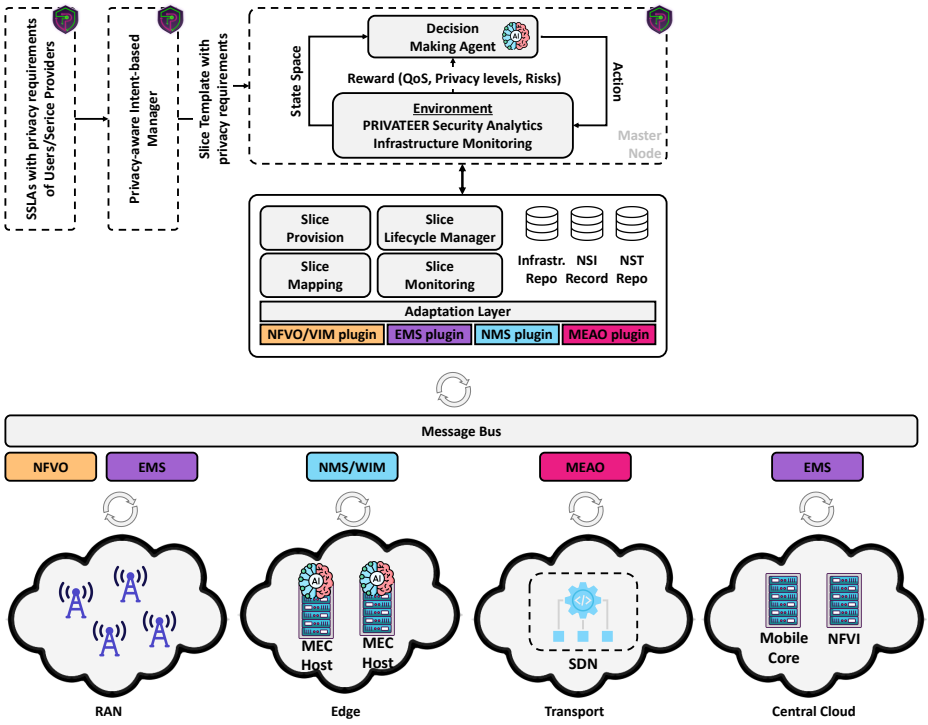

Fig. 3: End-to-end privacy aware slicing and security orchestration

by PRIVATEER (SSLAs, Privacy-aware intent based manager and Network resource orchestrator), while the rest of the components show the underlying SW and HW infrastructure.

▶ Regarding *trustworthy network topologies*, the PRIVATEER framework incorporates Proof-of-Transit (PoT) verification services distributed across the network to verify service chains and their paths, by adding secure meta-data (using keys obtained from a controller over a secure channel) to all packets that traverse a network path [6]. On top of that, PRIVATEER also exploits decentralization using DLT/Blockchain for sharing unverifiable path/service chain information, enhancing trust and fault tolerance, as well as scalability for increasing number of users [4]. Moreover, privacy-preserving technologies such as searchable encryption and homomorphic encryption are also employed to protect PoT information, where dedicated controllers determine which information is searchable and what operations can be performed on it.

▶ In the context of *privacy-aware orchestration*, PRIVATEER aims to create a secure and trusted environment for slice deployment, management, and orchestration in 6G networks while prioritizing user privacy and requirements. The framework utilizes AI-driven mechanisms to establish an autonomous network through closed control loops, emphasizing privacy throughout the service life-

cycle management, by exploiting reinforcement learning and transfer learning to automate end-to-end Privacy-aware slicing and security orchestration [16]. On top of the orchestrator, the framework employs a privacy-aware intent-based manager to translate customer Security SLAs (SSLAs) into data model formats, incorporating privacy levels as additional fields. PRIVATEER builds upon the Katana Slice Manager [14] and provides all the required extension for supporting decision-making and explainable capabilities for Privacy-Aware Slicing and Orchestration. Specifically, a DRL agent is developed on top of Katana to perform closed control loop operations, measuring KPIs, learning from the environment, and making appropriate reactive or proactive decisions to preserve Quality of Service (QoS) and privacy in dynamically changing networks. Last, privacy-aware policies are implemented, by considering user intents and constraints, trusted infrastructure domains, and traffic path integrity, while also federated learning techniques are utilized to decentralize control loop operations across multiple domains without exchanging privacy-sensitive data.

3.4 Distributed Attestation

PRIVATEER delivers several mechanisms for privacy-preserving attestation and identification in a distributed manner, as well as privacy-preserving threat sharing. Specifically, the framework provides *i)* a set of mechanisms for distributed verification, based on digital trusted wallets and verifiable credentials and *ii)* the required components for remote attestation of 6G services as well as the underlying heterogeneous hardware infrastructure. Figure 4 illustrates the decentralized attestation and identity concept advocated by PRIVATEER, which builds upon the "trust triangle" concept introduced by Decentralized Identifiers (DID) and applies it to enable the secure sharing of identity evidence and attestation while preserving privacy.

▶ In the context of *distributed verification and verifiable credentials*, PRIVATEER utilizes Decentralized Identifiers (DIDs) to store attestation results as Verifiable Credentials (VCs) in the 6G ecosystem [17], and explores their potential in future 6G authentication and authorization procedures. A distributed storage component based on Distributed Ledger Technology (DLT) is employed as a reliable attestation log and messaging platform for 6G infrastructure nodes, applications, and verifier services. Hybrid storage approaches are utilized to optimize data storage, while advanced data representation schemes and trusted Credentials Wallet components ensure credibility, traceability, and minimal overhead. PRIVATEER aims to enhance privacy in mobile networks, introduce Self-Sovereign Identity (SSI) concepts with DLT, and provides a novel framework for decentralized authentication and authorization management in B5G/6G environments, adhering to W3C-compatible SSI ecosystem standards.

▶ PRIVATEER also focuses on *infrastructure and service attestation*, which involves real-time supervision and verification of the operational assurance of the entire application graph, including trusted virtual network functions (VNFs) and Trusted Component-enabled edge devices. To achieve this, PRIVATEER explores existing attestation mechanisms, models, and protocols, such as binary,

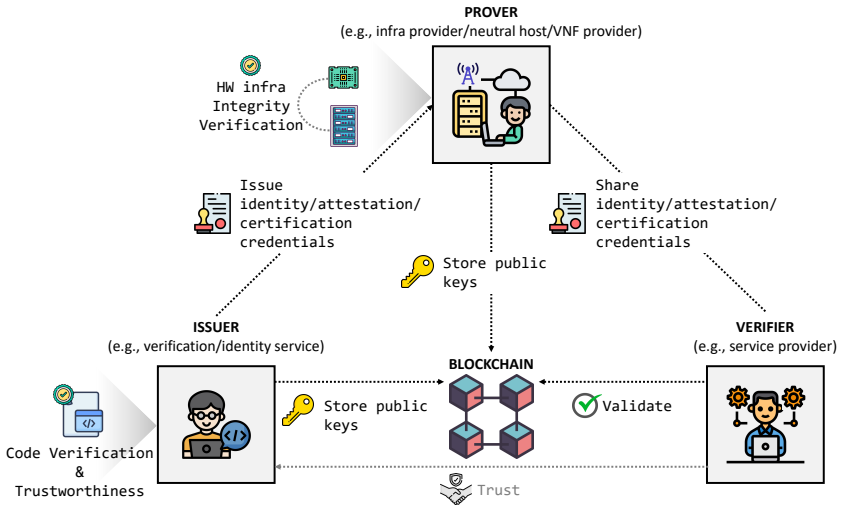

Fig. 4: PRIVATEER's "Trust Triangle" for privacy-preserving distributed identity and attestation

property-based, and control-flow attestation [22]. Moreover, PRIVATEER also tackles the attestation of heterogeneous edge infrastructures with custom AI accelerators, providing data integrity, authenticity, and secure execution of accelerated applications by ensuring the verification and trustworthiness of edge hardware and code, as well as the identification of trusted devices. PRIVATEER adopts a tight-coupled hardware-software verification approach to ensure the integrity and trustworthiness of accelerated kernels deployed on the edge infrastructure and the identification and integrity of physical devices. For code verification and trustworthiness, the framework leverages cryptographic schemes in order to verify that the design has been correctly imported into the acceleration devices. [1]. Device identification will be ensured through device-specific encryption and embedding of unique device identifiers into kernels, allowing execution only on trusted edge devices [27].

4 PRIVATEER's Use-Cases

The PRIVATEER framework will be evaluated through representative user stories and scenarios. The purpose of these scenarios is to showcase the actual value of the project results and their alignment with stakeholder needs and requirements. While PRIVATEER results are not specific to any vertical industry, the demonstration phase will focus on two vertical domains: *i)* Intelligent Transportation Systems (ITS) and *ii)* Smart Cities, with 5 different use case scenarios, as described below:

▶ **Scenario 1 (ITS – Edge service compromise):** In this scenario, a Service Provider (SP) deploys a 6G network slice for a road operator, including

low-latency edge functions for automated driving. An attacker exploits a vulnerability, hijacking the edge functions and accessing sensitive vehicle data. The PRIVATEER security analytics mechanism detects the attack as an anomaly, enabling quick identification and remedial actions by the SP security operators. PRIVATEER's privacy-friendly CTI sharing is used to inform the road operator without revealing sensitive information. Finally, decisions can then be made to ensure road user safety, such as disabling sensor sharing.

▶ **Scenario 2 (ITS – Privacy-friendly security service orchestration for logistics):** In this scenario, a cargo company requires a 6G network slice for its logistics operations, with distributed resources and virtualized security functions. The company prioritizes distributed security and communication privacy and it utilizes the PRIVATEER privacy-preserving slice orchestration mechanism to manage the slice resources across different domains, placing critical components on trusted infrastructure segments. The company also employs the PRIVATEER proof-of-transit mechanism to prevent traffic diversion and ensure secure communication with clients.

▶ **Scenario 3 (ITS – Verification of mass transportation application):** A mass transportation company has leased a multi-domain 6G network slice to support its transportation services. Ensuring the integrity of both the application and infrastructure is crucial for passenger safety. The service provider regularly conducts remote attestation of the software and hardware components, issuing verifiable credentials upon successful attestation and the infrastructure operators present these credentials to the transportation company without revealing sensitive details. If an integrity violation occurs, the incident is reported using the privacy-preserving CTI sharing feature to maintain confidentiality.

▶ **Scenario 4 (Smart City – Onboarding of a "neutral host" edge network):** A municipality has deployed a network of "smart lamps" to provide shared access infrastructure for multiple Service Providers. The municipality seeks a trusted third party to conduct a comprehensive integrity check and certify the infrastructure. The attestation result is stored as a verifiable credential and presented to the Service Providers using the infrastructure. An attacker exploits a vulnerability in outdated firmware of some smart lamps, but the PRIVATEER distributed analytics framework detects this activity as an outlier. The attestation credentials are immediately invalidated due to the integrity breach. While recovering from the attack, the municipality's security operators issue a threat notification to other operators using PRIVATEER's CTI sharing features, while maintaining the confidentiality of sensitive information about the attack.

▶ **Scenario 5 (Smart City – Multi-domain infrastructure verification for a new 6G smart city app):** A startup has developed a smart city 6G application and plans to deploy it as a pilot project in two neighboring cities. To support this application, the startup leases a multi-domain network slice that utilizes the neutral-host infrastructure provided by the municipalities. PRIVATEER's privacy-aware orchestration mechanism is utilized by the startup to strategically place the more sensitive components of the application on nodes with a higher level of trust. The two infrastructure providers issue a PoT attes-

tation, which is then presented as a verifiable credential to the startup and city clients, thanks to PRIVATEER's distributed attestation/certification capability.

5 Conclusion

In this paper, we presented an overview of the PRIVATEER Horizon Europe project, which provides "privacy-first" security enablers for future B5G/6G networks. PRIVATEER introduces several innovations for strengthening security and privacy in the B5G era, including decentralised and robust security analytics, privacy-aware network slicing and orchestration as well as distributed attestation mechanisms. The evaluation of the framework will be performed through 5 different use-case scenarios in the context of Intelligent Transportation Systems and Smart Cities.

References

1. AMD-Xilinx, "Using Encryption and Authentication to Secure an UltraScale/UltraScale+ FPGA Bitstream". https://docs.xilinx.com/r/en-US/xapp1267-encryp-efuse-program/Using-Encryption-and-Authentication-to-Secure-an-UltraScale/UltraScale-FPGA-Bitstream-Application-Note, accessed: 15/5/2023
2. Abraham, S.S.: Fairlof: fairness in outlier detection. Data Science and Engineering **6**, 485–499 (2021)
3. Araújo, R., Pinto, A.: Secure remote storage of logs with search capabilities. Journal of Cybersecurity and Privacy **1**(2), 340–364 (2021). https://doi.org/10.3390/jcp1020019, https://www.mdpi.com/2624-800X/1/2/19
4. Benčić, F.M., Skočir, P., Žarko, I.P.: Dl-tags: Dlt and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. IEEE access **7** (2019)
5. Bernardos, C.J., Uusitalo, M.A.: European vision for the 6g network ecosystem (Jun 2021). https://doi.org/10.5281/zenodo.5007671, https://doi.org/10.5281/zenodo.5007671
6. Brockners, F., Bhandari, S., Mizrahi, T., Dara, S., Youell, S.: Proof of transit. Internet Engineering Task Force, Internet-Draft draft-ietf-sfcproof-of-transit-06 (2020)
7. Das, A., Rad, P.: Opportunities and challenges in explainable artificial intelligence (xai): A survey. arXiv preprint arXiv:2006.11371 (2020)
8. Fernandes, R., Bugla, S., Pinto, P., Pinto, A.: On the performance of secure sharing of classified threat intelligence between multiple entities. Sensors **23**(2) (2023). https://doi.org/10.3390/s23020914, https://www.mdpi.com/1424-8220/23/2/914
9. Hu, H., Liu, Y., Wang, Z., Lan, C.: A distributed fair machine learning framework with private demographic data protection. In: 2019 IEEE International Conference on Data Mining (ICDM). pp. 1102–1107. IEEE (2019)
10. Iwahana, K., Yanai, N., Cruz, J.P., Fujiwara, T.: Spgc: Integration of secure multiparty computation and differential privacy for gradient computation on collaborative learning. Journal of Information Processing **30**, 209–225 (2022)
11. Jagielski, M., Kearns, M., Mao, J., Oprea, A., Roth, A., Sharifi-Malvajerdi, S., Ullman, J.: Differentially private fair learning. In: International Conference on Machine Learning. pp. 3000–3008. PMLR (2019)
12. Jiang, W., Han, B., Habibi, M.A., Schotten, H.D.: The road towards 6g: A comprehensive survey. IEEE Open Journal of the Communications Society **2** (2021)

13. Katz, M., Pirinen, P., Posti, H.: Towards 6g: Getting ready for the next decade. In: 2019 16th International symposium on wireless communication systems (ISWCS). pp. 714–718. IEEE (2019)
14. Kourtis, M.A., Sarlas, T., Xilouris, G., Batistatos, M.C., Zarakovitis, C.C., Chochliouros, I.P., Koumaras, H.: Conceptual evaluation of a 5g network slicing technique for emergency communications and preliminary estimate of energy trade-off. Energies **14**(21), 6876 (2021)
15. Lee, Y.L., Loo, J., Chuah, T.C., Wang, L.C.: Dynamic network slicing for multi-tenant heterogeneous cloud radio access networks. IEEE Transactions on Wireless Communications **17**(4), 2146–2161 (2018)
16. Li, R., Zhao, Z., Sun, Q., Chih-Lin, I., Yang, C., Chen, X., Zhao, M., Zhang, H.: Deep reinforcement learning for resource management in network slicing. IEEE Access **6**, 74429–74441 (2018)
17. Lux, Z.A., Thatmann, D., Zickau, S., Beierle, F.: Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). pp. 71–78. IEEE (2020)
18. Mothukuri, V., Parizi, R.M., Pouriyeh, S., Huang, Y., Dehghantanha, A., Srivastava, G.: A survey on security and privacy of federated learning. Future Generation Computer Systems **115**, 619–640 (2021)
19. Nguyen, V.L., Lin, P.C., Cheng, B.C., Hwang, R.H., Lin, Y.D.: Security and privacy for 6g: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials **23**(4), 2384–2428 (2021)
20. Pentyala, S., Railsback, D., Maia, R., Dowsley, R., Melanson, D., Nascimento, A., De Cock, M.: Training differentially private models with secure multiparty computation. arXiv preprint arXiv:2202.02625 (2022)
21. Shekhar, S., Shah, N., Akoglu, L.: Fairod: Fairness-aware outlier detection. In: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (2021)
22. Steiner, R.V., Lupu, E.: Attestation in wireless sensor networks: A survey. ACM Computing Surveys (CSUR) **49**(3), 1–31 (2016)
23. Wagner, C., Dulaunoy, A., Wagener, G., Iklody, A.: Misp: The design and implementation of a collaborative threat intelligence sharing platform. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. pp. 49–56 (2016)
24. You, X., Wang, C.X., Huang, J., Gao, X., Zhang, Z., Wang, M., Huang, Y., Zhang, C., Jiang, Y., Wang, J., et al.: Towards 6g wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences **64**, 1–74 (2021)
25. Zhang, H., Davidson, I.: Towards fair deep anomaly detection. In: Proceedings of the 2021 ACM conference on fairness, accountability, and transparency (2021)
26. Zhang, J., Chen, J., Wu, D., Chen, B., Yu, S.: Poisoning attack in federated learning using generative adversarial nets. In: 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). pp. 374–380. IEEE (2019)
27. Zhang, J., Qu, G.: Recent attacks and defenses on fpga-based systems. ACM Transactions on Reconfigurable Technology and Systems (TRETS) **12**(3), 1–24 (2019)
28. Zhang, S.: An overview of network slicing for 5g. IEEE Wireless Communications **26**(3), 111–117 (2019)
29. Zikria, Y.B., Ali, R., Afzal, M.K., Kim, S.W.: Next-generation internet of things (iot): Opportunities, challenges, and solutions. Sensors **21**(4), 1174 (2021)