Multi-Partner Project: Secure Hardware Accelerated Data Analytics for 6G Networks: the PRIVATEER Approach

Ilias Papalamprou*, Aimilios Leftheriotis†, Apostolos Garos‡, Georgios Gardikis‡, Maria Christopoulou§, George Xilouris§, Lampros Argyriou¶, Antonia Karamatskou¶, Nikolaos Papadakis¶, Emmanouil Kalotychos‖, Nikolaos Chatzivasileiadis‖, Dimosthenis Masouros*, George Theodoridis†, Dimitrios Soudris*
*National Technical University of Athens, Greece †University of Patras, Greece
‡R&D Department, Space Hellas S.A., Greece §NCSR "Demokritos" Institute of Informatics and Telecommunications, Greece
¶Infili Technologies S.A., Greece ‖Ubitech Ltd., Digital Security & Trusted Computing Group, Greece
*{ipapalambrou, dmasouros, dsoudris}@microlab.ntua.gr, †aleftheriotis@ac.upatras.gr, theodor@ece.upatras.gr,
‡{agaros, ggar}@space.gr, §{maria.christopoulou, xilouris}@iit.demokritos.gr,
¶{largyriou, akaramatskou, npapadakis}@infili.com, ‖{mkalotychos, nchatzivasileiadis}@ubitech.eu

Abstract—**Next generation 6G networks are designed to meet the requirements of modern applications, including the need for higher bandwidth and ultra-low latency services. While these networks show significant potential to fulfill these evolving connectivity needs, they also bring new challenges, particularly in the area of security. Meanwhile, ensuring the privacy is paramount in 6G network development, demanding robust solutions following "privacy-by-design" principles. To address these challenges, PRIVATEER project strengthens existing security mechanisms, introducing privacy-centric enablers tailored for 6G networks. This work, evaluates key enablers within PRIVATEER, focusing on the development and acceleration of AI-driven anomaly detection models, as well as attestation mechanisms for both hardware accelerators and containerized applications.**

Index Terms—**6G, Security, Privacy, AI, Hardware Acceleration**

I. Introduction

The development of beyond-5G (B5G) and upcoming 6G networks marks a pivotal shift in mobile communications, promising to reduce latency, enhance bandwidth, and improve overall performance [1]. The planned evolution towards 6G aims to enable transformative technologies, e.g. augmented reality, massive Internet of Things (IoT) and AI-driven applications, by offering faster, more reliable and ultra-responsive network experiences [2]. This shift not only plans to enhance connectivity and speed but needs to address emerging security and privacy challenges arising from immersive use cases.

PRIVATEER project[1] addresses the security and privacy challenges of 5G and envisioned 6G networks through four key areas [3]: i) Decentralized Security Analytics, ii) Infrastructure and Service Attestation to ensure integrity across a multi-actor environment (including Service Providers, Mobile Network Operators, Infrastructure Providers, and End Users), iii) Privacy-Aware Orchestration, and iv) Privacy-Friendly Cyber Threat Intelligence (CTI) Sharing.

Given the complex nature of 6G networks, the adoption of AI is one of the most promising solutions to support advanced network management as well as sophisticated security mechanisms [4]. However, due to high computational requirements, general-purpose processors (CPUs) alone are insufficient for deployment. This challenge underscores the need for a heterogeneous computing continuum - integrating specialized hardware accelerators to meet the low-latency and energy-efficiency requirements of 6G services. Among these, Field Programmable Gate Arrays (FPGAs) distinguish as a flexible option, providing low-latency, energy-efficient performance well-suited to 6G's needs [5]. However, the complex structure of 6G networks heightens security risks that existing mechanisms may not address [2]. Threats like malware updates, hardware trojans, and DDoS attacks demand tailored solutions to ensure network integrity and data protection.

This paper highlights key developments from the first phase of the PRIVATEER project, crucial for securing 6G services, particularly in securely deploying data analytic functions at the edge. Its contributions are as follows:

- **Anomaly detection AI models** for detecting Distributed Denial-of-Service (DDoS) attacks in the network.
- **Hardware Acceleration of AI models** aiming for both low latency and energy efficient execution of data-analytics applications in the edge.
- **Secure configuration of hardware accelerators** for ensuring their secure deployment in the edge.
- **Attestation for virtualized infrastructures** for establishing trustworthiness for the containerized applications.

This work has been partially funded by the PRIVATEER project. PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme 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 European Union or SNS JU. Neither the European Union nor the granting authority can be held responsible for them.

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

978-3-9826741-0-0/DATE25/© 2025 EDAA

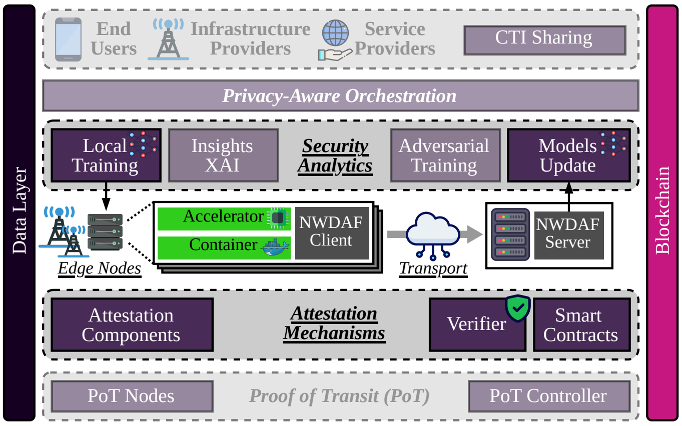


Fig. 1: PRIVATEER's high-level architecture.

II. PRIVATEER's Vision & Overview

PRIVATEER Horizon 2020 research and innovation programme, initiated on February 2023, with an expected duration of 3 years. The abstract architecture of PRIVATEER's framework, as analyzed in [3] and illustrated in Fig. 1, aims to develop innovative security enablers *following a privacy-by-design approach*, in alignment with EU standards, including GDPR. PRIVATEER introduces innovative methodologies to ensure privacy preservation across all stakeholders, encompassing End Users, Infrastructure Providers/Neutral Hosts, and Service Providers. The security enablers include the following: *i) Decentralized Robust Security Analytics:* The existing security analytics are enhanced using AI, for detection and classification of network threats. from traffic data and logs. To improve privacy, it adopts decentralized federated learning, supported by adversarial training and anonymization techniques [6].
ii) Privacy-aware Slicing and Orchestration: PRIVATEER integrates privacy awareness and user intent, while securing the service path. The framework prioritizes creating trusted network topologies by incorporating Proof-of-Transit (PoT) services and implementing privacy-focused orchestration mechanisms based on individual user needs.
iii) Distributed Attestation: Various mechanisms for distributed privacy-preserving attestation, identification and threat sharing are introduced. This includes tools for distributed verification through digital trusted wallets and verifiable credentials, as well as components necessary for remote attestation of the 6G services and the heterogeneous hardware infrastructure.
iv) Cyber Threat Intelligence (CTI) Sharing: CTI sharing enables privacy-preserving secure exchange of threat intelligence.

In the final stage of the project, the enablers will be evaluated across five use cases in two distinct environments: Intelligent Transport Systems (ITS) and Smart Cities, demonstrating their effectiveness in representative, real-world scenarios.

This paper provides a deep-dive analysis of PRIVATEER's hardware-accelerated data analytics engine and attestation mechanisms, which enable the deployment of secure monitoring across heterogeneous distributed edge computing environments. The security enablers developed are open-source and available through PRIVATEER's GitHub repository[2].

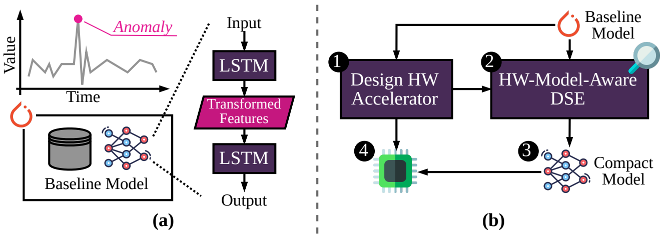


Fig. 2: **(a)** LSTM-AE development. **(b)** FPGA acceleration.

III. PRIVATEER's Security Enablers

A. AI-Driven Hardware Accelerated Security Analytics

With the rapid increase in connected devices within 6G networks, the ability to efficiently detect attacks is essential for maintaining reliable and secure network performance. Detecting anomalies in network traffic is particularly important for identifying threats like DDoS attacks, which, particularly in the 6G ecosystem, pose significant security risks for various critical technologies, such as Network Function Virtualization (NFV) and Software-Defined Wide-Area Networks (SD-WAN) [7]. To address these risks, PRIVATEER has developed AI-based security analytics, leveraging data from the Network Data Analytics Function (NWDAF). NWDAFs are distributed across the network continuum and are responsible for continuously monitoring network traffic, providing insights into network data production and consumption. On top of that, to support real-time threat detection, often required within a few milliseconds [8], PRIVATEER leverages FPGA hardware accelerators to provide efficient and high-performing threat detection.

1) LSTM Autoencoder for Anomaly Detection: PRIVATEER utilizes a Long Short-Term Memory Autoencoder (LSTM-AE) architecture to identify anomalies on streaming data coming from the NWDAF. This hybrid architecture is well-suited for detecting anomalies in sequential data [9], as it learns typical patterns and identifies deviations based on reconstruction error. For anomalous data, the reconstruction error is usually significantly higher, enabling their effective detection.

To fine-tune the LSTM-AE for optimal performance, PRIVATEER employs a systematic hyperparameter-tuning approach using Grid Search. This method involves defining a comprehensive search space and systematically evaluating the model's performance across all possible combinations of hyperparameter values. This Grid Search identified a regularized overcomplete LSTM-AE, which we refer to as *Baseline* model.

2) Acceleration of Data Analytics on FPGAs: PRIVATEER leverages FPGAs to facilitate the deployment of energy-efficient, low-latency AI-based data analytics applications at the edge. FPGAs are well-suited for such tasks due to their parallel-processing capabilities, which allow for significant acceleration of computationally intensive operations.

The process of hardware acceleration of PRIVATEER's AI models, illustrated in Fig. 1b, begins with the design and opti-

[2] https://github.com/privateer-project

mization of the hardware accelerator. In Step ❶, PRIVATEER's *Baseline* model serves as the foundation, where design choices for key model components (e.g., LSTM layers) are translated into architectural specifications suited for FPGA deployment. The FPGA design includes specific considerations to accommodate the structure and requirements of the LSTM model.

In Step ❷, a Hardware-Model-Aware Design Space Exploration (DSE) is conducted. This stage integrates both hardware design and model characteristics, guiding the DSE process to identify an optimal configuration that balances the performance requirements of the AI model with the capabilities and limitations of the target FPGA platform. By combining hardware-awareness and model-awareness, this DSE process not only maximizes model performance for its intended anomaly detection task but also adjusts the model's structure to fully capitalize on the specialized hardware design developed in Step ❶, achieving a highly efficient and compact design.

The DSE in Step ❷ results in a refined version of the *Baseline* model—referred to as the *Compact* model ❸. The DSE ensures that the *Compact* model achieves the best possible performance trade-offs, balancing minimal accuracy degradation with significant gains in energy efficiency and processing speed. Finally, Step ❹ involves integrating the identified *Compact* model ❸ with the hardware design developed in Step ❶, to realise a complete FPGA-based inference accelerator.

B. Secure Services in Heterogeneous Edge Systems

As B5G technologies progress, new functionalities introduce fresh challenges, highlighting the need for adaptive security measures. Robust security is critical not only for services but also for the infrastructure that supports them, including virtualized services, Virtual Network Functions (VNFs), and a heterogeneous edge infrastructure. These systems are susceptible to various attacks, such as reverse engineering, malicious code injection, hardware trojans, as well as physical attacks in multi-tenant scenarios [10]. To address these risks, PRIVATEER employs remote attestation protocols in conjunction with dedicated hardware (e.g. encryption modules, Trusted Execution Environments (TEEs)), to enable secure service deployment across the edge, covering both FPGAs and containerized applications. This enables a system to prove its trustworthiness to a remote verifier by responding to a challenge with security evidence, which the verifier validates against some reference values. Hence, following Zero Trust principles -where no entity is inherently trusted and all must continuously demonstrate their trustworthiness- we ensure secure service deployment across the edge. Additionally, for collecting any security evidence for service deployment, a decentralized secure storage mechanism is employed, i.e., the Blockchain.

1) Secure configuration of FPGAs: For edge nodes featuring FPGA-based accelerators, a custom hardware/software solution is presented to ensure secure configuration, comprised of:
Edge Node: The computing platform with the FPGA accelerator, that apart from hosting the hardware accelerated application (i.e., the bitstream) of the *Application Provider*, it contains supplementary modules responsible for verifying the integrity and authenticity of all individual components. The *attestation service* serves as the backbone of the system, handling the collection of any security evidence using hardware and software components, as well as exchanging those data with an external attestation server.

TABLE I: Accuracy Metrics for different AI models

Model	Accuracy	Precision	Recall	F1 Score
Baseline	0.9982	1.0000	0.9822	0.9910
Compact	0.9936	1.0000	0.9416	0.9699

Attestation Server: Acts as an external authority that coordinates with all involved parties, for verifying the integrity of all components and deploy them securely in the target node.

When deploying a hardware-accelerated application to the edge, the process begins with an offline phase where the application provider encrypts the application's bitstream and transfers it to the edge node. Meanwhile, the attestation server gathers reference values, including cryptographic checksums and digital signatures. Afterwards, in the online phase the integrity and authenticity of the *attestation service* on the edge node and the *application's bitstream* is ensured. After successful verification, the application's bitstream is decrypted and loaded onto the FPGA. Furthermore, after each attestation process is finalized, the results are forwarded to the Blockchain, to be stored in a decentralized location.

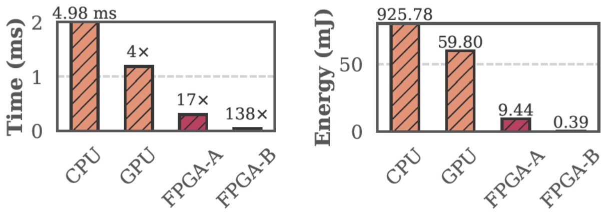
2) Secure Containerized Applications: For addressing the vulnerabilities of the containerized applications, TEEs are leveraged to ensure secure and reliable operation. TEEs are secure areas within a device's processor that provide isolated execution of code and data, shielding sensitive information from the rest of the system. To achieve robust security for sensitive applications, PRIVATEER leverages Intel Software Guard Extensions (Intel SGX) [11], as its TEE solution. Additionally, PRIVATEER leverages the TEE for extracting (verifiable) evidence; thus performing attestation tasks, ensuring the integrity and authenticity of the code running within an enclave. A core component is proposed, i.e., the *Attestation Agent*, that is responsible for monitoring and verifying the *static* and the *runtime* properties of the containerized application and the virtualised infrastructure. The output of the *Attestation Agent* is a proof of correctness, which does not reveal the exact evidence, providing privacy-preservation. The extracted attestation evidence, similar with those collected from the edge nodes with FPGAs, is stored in PRIVATEER's Blockchain.

IV. Evaluation of Security Enablers

A. AI-Driven Hardware Accelerated Security Analytics

1) Development of AI models: To evaluate the accuracy of PRIVATEER's AI models, we utilize the NCSRD-DS-5GDDoS dataset [12]. Each series in this dataset consists of various metrics related to 5G radio and core networks, capturing the performance and behaviour of network components during normal operation and sporadic DDoS attacks.

The DSE mentioned in Section III-A2, identified a regularized overcomplete autoencoder, containing two LSTM layers in the encoder, two LSTM layers in the decoder, and processing input sequences of 120 timesteps, which we refer as *Baseline*



(a) Latency

(b) Energy

Fig. 3: Experimental Results for FPGA acceleration

model. Table I demonstrates the performance metrics of the *Baseline* model and its high effectiveness in anomaly detection. Recall, or the true positive rate, stands at 0.9822, signifying that the model successfully captures 98.22% of all actual anomalies. The F1 Score, which balances precision and recall, is at a robust 0.9910, further underscoring the model's reliability.

2) Acceleration of Data Analytics on FPGAs: As described in Section III-A2 and depicted in Step ❷ of Fig. 2b PRIVATEER employs a Hardware-Model-Aware DSE. The resulting model, which we refer as *Compact* model, is a regularized overcomplete LSTM-AE that processes inputs of 8 timesteps, containing one LSTM layer in the encoder and another LSTM layer coupled with a linear layer in the decoder.

To evaluate the effectiveness of PRIVATEER's FPGA-accelerated implementation for anomaly detection, we conducted a comparative evaluation focusing on inference latency and energy efficiency across different hardware platforms. Specifically, we evaluated 4 setups: the *Baseline* model deployed on an Intel Xeon Gold 6530 @2.10 GHz (`CPU`) and on a Nvidia V100 (`GPU`), and the *Compact* model deployed on two diverse FPGA-enabled edge nodes, i.e., `FPGA-A`, which consists of an Alveo U280 FPGA, and `FPGA-B`, which is based on the Multiprocessor System-on-a-Chip (MPSoC) ZCU104.

Fig. 3 illustrates the average inference latency and the average energy per inference consumption comparison of each implementation, across 1000 inferences. The `FPGA-B` implementation demonstrated an average latency of 0.036 ms, achieving substantial speedups compared to the rest of the setups. The large difference in latency between `FPGA-A` and `FPGA-B` can be explained by the increased overheads in data transfers that occur in the ALVEO U280. Moreover, `FPGA-B` reduced energy consumption dramatically, requiring 2374×, 153.33×, and 24× less energy per inference than the `CPU`, `GPU`, and `FPGA-A` implementations respectively.

Finally, we assessed the trade-off between model compactness and detection performance. Table I compares the *Baseline* and *Compact* models, demonstrating that the *Compact* model exhibits minimal degradation in key performance metrics—less than 4% across accuracy, precision, recall, and F1 score. This minor reduction in detection accuracy indicates that the *Compact* model remains highly effective for anomaly detection.

B. Edge Service Deployment in Heterogeneous Environments

1) Secure Service Deployment: The methodologies for the integrity verification of deployed services are evaluated with their execution time. For the FPGA-enabled edge nodes, as in Section IV-A2 we have the two distinct FPGAs, `FPGA-A` and `FPGA-B`. For evaluating the attestation latency of containerized applications, we follow a similar approach to [13], which applies a zero-knowledge methodology. It targets a Raspberry Pi 4B equipped with a Trusted Platform Module (TPM), that is responsible for securely calculating attestation evidence. In all platforms the attestation process takes less than 5sec., having therefore minimal overhead to the application deployment.

V. Conclusion & Future Steps

PRIVATEER project aims to enhance the security enablers of 5G networks by following a privacy-by-design approach. In this paper, we evaluate several of PRIVATEER's methodologies developed in the first phase of the project, with a focus on developing hardware-accelerated AI models for anomaly detection in 6G networks. In the second phase, detection will expand to cover more 6G network attacks. Security evidence from services will support a comprehensive privacy mechanism, while a privacy-aware orchestrator will ensure secure and private service deployment and management.

References

[1] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies," *IEEE access*, vol. 9, pp. 67512–67547, 2020.

[2] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[3] D. Masouros, D. Soudris, G. Gardikis, V. Katsarou, M. Christopoulou, G. Xilouris, H. Ramón, A. Pastor, F. Scaglione, C. Petrollini, *et al.*, "Towards privacy-first security enablers for 6g networks: the privateer approach," in *International Conference on Embedded Computer Systems*, pp. 379–391, Springer, 2023.

[4] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6g: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.

[5] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hätönen, "6g architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173508–173520, 2020.

[6] M. Cunha, G. Duarte, R. Andrade, R. Mendes, and J. P. Vilela, "Privkit: A toolkit of privacy-preserving mechanisms for heterogeneous data types," in *Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy*, pp. 319–324, 2024.

[7] S. B. Prathiba, G. Raja, S. Anbalagan, K. Arikumar, S. Gurumoorthy, and K. Dev, "A hybrid deep sensor anomaly detection for autonomous vehicles in 6g-v2x environment," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1246–1255, 2022.

[8] M. A. Ferrag, O. Friha, B. Kantarci, N. Tihanyi, L. Cordeiro, M. Debbah, D. Hamouda, M. Al-Hawawreh, and K.-K. R. Choo, "Edge learning for 6g-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses," *IEEE Communications Surveys & Tutorials*, 2023.

[9] M. Said Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Network anomaly detection using lstm based autoencoder," in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pp. 37–45, 2020.

[10] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010–1038, 2020.

[11] V. Costan, "Intel sgx explained," *IACR Cryptol, EPrint Arch*, 2016.

[12] N. C. of Scientific Research "Demokritos" and S. H. (Greece), "NCSRD-DS-5GDDoS: 5G Radio and Core metrics containing sporadic DDoS attacks," Oct. 2024. https://doi.org/10.5281/zenodo.13900057.

[13] H. B. Debes and T. Giannetsos, "Zekro: Zero-knowledge proof of integrity conformance," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–10, 2022.