The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 08 2025
PAGE NO. 100-104

FPGA Acceleration for Security and Performance in Multi-Tenant Clouds with Hardware-Assured IP Protection

Dr. Alexander M. Reynolds
Department of Computer Science, University of Melbourne, Australia

Received: 01 August 2025; **Accepted:** 15 August 2025; **Published:** 31 August 2025

Abstract: The rapid proliferation of cloud computing services has necessitated an urgent focus on ensuring both performance efficiency and robust security in multi-tenant environments. In particular, the adoption of Field-Programmable Gate Arrays (FPGAs) in cloud infrastructures presents a promising avenue for accelerating computation-intensive workloads while simultaneously addressing critical security concerns associated with untrusted intellectual property (IP) cores. This study synthesizes contemporary research in FPGA-enabled cloud architectures, zero-trust frameworks for multi-tenant platforms, and hardware protection techniques for system-on-chip (SoC) designs to establish a cohesive perspective on securing cloud acceleration. We explore obfuscation strategies, statistical hardware Trojan detection, and voltage-based attack mitigation in FPGA environments. The research further examines encryption methodologies, including hybrid and elliptic curve-based algorithms, tailored to preserving data privacy in shared cloud infrastructures. By integrating hardware-centric security measures with advanced cryptographic techniques and cloud-native acceleration strategies, the paper proposes a multi-layered paradigm for enhancing resilience, performance, and trustworthiness in next-generation cloud services. The findings elucidate theoretical and practical implications, highlighting both the opportunities for deploying FPGAs at scale in public clouds and the complex security challenges that arise from multi-tenancy, shared resources, and potentially untrusted hardware modules. The study concludes by outlining future research trajectories, emphasizing adaptive security frameworks, dynamic resource isolation, and cross-layer verification methodologies as essential components of secure cloud acceleration.

Keywords: FPGA acceleration, cloud security, multi-tenant environments, hardware IP protection, zero trust, elliptic curve cryptography, system-on-chip security

INTRODUCTION

Cloud computing has fundamentally transformed the landscape of information technology by enabling elastic, on-demand access to shared computational resources, thereby catalyzing innovation across industry and academia (Hariharan, 2025). Multi-tenant cloud environments, wherein multiple clients share hardware, software, and network infrastructures, offer unparalleled scalability and cost efficiency. However, the inherent sharing of resources introduces a complex attack surface. Security breaches, including data leakage, side-channel attacks, and malicious hardware insertion, threaten the integrity, confidentiality, and availability of cloud services. While software-level security controls provide essential mitigation, they are insufficient in addressing vulnerabilities originating from hardware-level attacks, particularly when third-party IPs are integrated into system-on-chip designs (Basak et al., 2017).

The introduction of FPGA acceleration into cloud platforms represents a transformative paradigm. FPGAs provide reconfigurable hardware capable of executing parallel computation tasks at substantially higher speeds than general-purpose processors, thus offering significant performance benefits for workloads such as deep learning, big data analytics, and high-frequency financial modeling (Bobda et al., 2022; Caulfield et al., 2016). OpenStack and other virtualization frameworks have demonstrated feasibility for booting FPGA resources in virtualized environments, effectively democratizing access to hardware acceleration across tenants (Byma et al., 2014; Chen et al., 2014). Despite these advances, the integration of FPGA accelerators in multi-tenant clouds exacerbates security risks, including voltage and side-channel attacks, which can be exploited by

neighboring tenants to extract sensitive computation patterns (Boutros et al., 2020).

Simultaneously, the proliferation of third-party IP cores in SoC designs has led to concerns over untrusted modules introducing hardware Trojans or embedded malicious logic. Conventional software-level protections are inadequate for detecting these threats, necessitating advanced methodologies such as obfuscation-based design strategies (Chakraborty & Bhunia, 2009), statistical detection mechanisms (Chakraborty et al., 2009), and IP watermarking techniques (Chapman & Durrani, 2000; Basak et al., 2017). These approaches aim to safeguard the functional and structural integrity of IPs while maintaining design flexibility and performance.

In addition to hardware-centric security, data confidentiality in cloud platforms remains a persistent concern. Advanced encryption strategies, including hybrid and fully homomorphic cryptography coupled with elliptic curve schemes, have emerged as viable solutions for preserving privacy in cloud storage and computation (Goyal & Kant, 2018; Kanna & Vasudevan, 2019; Subramanian & Tamilselvan, 2020). Integrating these cryptographic solutions with hardware-enforced protections creates a comprehensive defense framework that spans both software and hardware layers.

Despite significant research progress, a literature gap persists in harmonizing FPGA acceleration, hardware IP protection, and cryptographic security within a unified multi-tenant cloud framework. Current studies often address these domains in isolation, leaving unresolved challenges related to dynamic resource allocation, cross-tenant threat detection, and performance-security trade-offs. This research endeavors to fill these gaps by synthesizing hardware and software security methodologies, evaluating their practical implications for FPGA-accelerated cloud platforms, and proposing a multi-layered, zero-trust-inspired framework for secure computation in shared environments.

METHODOLOGY

This study adopts a multi-faceted methodological approach, integrating a comprehensive review of state-of-the-art FPGA cloud architectures, hardware security mechanisms, and cryptographic techniques with theoretical analysis and system-level modeling. The methodology encompasses the following components:

First, we conduct an extensive review of FPGA-based cloud acceleration platforms, including both proprietary initiatives such as Microsoft's Catapult project (Chiou, 2017) and open-source frameworks enabling FPGA virtualization (Byma et al., 2014; Chen et al., 2014b). Emphasis is placed on understanding the architectural design of FPGA clusters, interconnect topologies, and resource scheduling strategies, as these factors directly influence both performance and security outcomes. We analyze trade-offs associated with shared FPGA deployment, particularly in multi-tenant scenarios where isolation mechanisms may impact computational throughput.

Second, the research evaluates security assurance methodologies for SoC designs integrating untrusted IPs. Techniques such as HARPOON, which employs obfuscation to prevent reverse engineering and IP theft (Chakraborty & Bhunia, 2009), and MERO, a statistical approach for hardware Trojan detection (Chakraborty et al., 2009), are examined for their applicability in cloud-deployed FPGA environments. Voltage and side-channel attacks against multi-tenant FPGAs, including 'neighbors from hell' scenarios, are studied in detail to identify vulnerabilities that may be exploited by co-located tenants (Boutros et al., 2020). Consideration is given to both design-time and run-time mitigation strategies, evaluating the efficacy of countermeasures such as power regulation, signal masking, and runtime monitoring.

Third, data privacy measures are incorporated through an analysis of advanced encryption algorithms, focusing on hybrid schemes combining symmetric and asymmetric cryptography, as well as elliptic curve-based solutions (Goyal & Kant, 2018; Kanna & Vasudevan, 2019; Alowolodu et al., 2013). The methodology assesses how these cryptographic schemes can be efficiently implemented on FPGA platforms to ensure minimal performance overhead while maximizing confidentiality, particularly for workloads involving sensitive healthcare or financial datasets.

Fourth, the study employs a descriptive systems modeling approach to simulate multi-tenant cloud environments with FPGA accelerators. Resource allocation policies, isolation strategies, and encryption overheads are modeled to provide a comprehensive view of performance-security trade-offs. This theoretical modeling is augmented by literature-based performance metrics from existing FPGA cloud deployments (Bobda et al., 2022; Caulfield et al., 2016), providing empirical grounding for the analysis.

Finally, a conceptual zero-trust framework is integrated throughout the methodology. Each hardware and software component is treated as potentially untrusted, and security mechanisms are evaluated under the assumption that attackers may

have both software and physical access to shared resources (Hariharan, 2025). This perspective informs both the architectural design principles and the security evaluation criteria, ensuring a holistic approach to safeguarding multi-tenant cloud operations.

RESULTS

The analysis indicates that FPGA acceleration in cloud environments can deliver significant computational performance improvements across diverse workloads, including deep learning inference, cryptographic operations, and high-performance data analytics (Caulfield et al., 2016; Bobda et al., 2022). By leveraging parallelism inherent in FPGA architectures, tasks traditionally limited by CPU-based bottlenecks can achieve substantial latency reductions, improving end-user responsiveness in multi-tenant platforms.

However, the findings also underscore that multi-tenancy introduces complex security challenges. Voltage-based side-channel attacks demonstrate the capacity for cross-tenant leakage of sensitive computational data, confirming prior findings in 'neighbors from hell' studies (Boutros et al., 2020). Statistical detection mechanisms such as MERO exhibit high efficacy in identifying anomalous hardware behavior indicative of Trojans (Chakraborty et al., 2009), though implementation complexity and runtime overheads remain non-trivial. Obfuscation-based IP protection methodologies (Chakraborty & Bhunia, 2009) are shown to provide robust defenses against reverse engineering, but they require careful consideration of design performance trade-offs.

From a cryptographic standpoint, hybrid and elliptic curve-based encryption techniques successfully secure data in transit and at rest, mitigating risks associated with co-located tenants in shared cloud infrastructure (Goyal & Kant, 2018; Kanna & Vasudevan, 2019). Implementing these encryption mechanisms on FPGA platforms allows for high-throughput, low-latency processing, ensuring that data confidentiality is maintained without compromising performance. Nonetheless, encryption introduces additional resource utilization, necessitating careful balancing between security guarantees and computational efficiency.

The synthesis of these findings reveals that a multi-layered security paradigm—combining hardware-level protections, software-based cryptography, and zero-trust architectural principles—can effectively mitigate the majority of vulnerabilities inherent to FPGA-accelerated multi-tenant clouds. The analysis highlights the critical importance of continuous monitoring, adaptive resource isolation, and integration of security measures at both the design and operational stages.

DISCUSSION

The results suggest profound theoretical and practical implications for cloud service providers and hardware designers. The integration of FPGA acceleration with hardware IP protection establishes a framework in which performance and security are not mutually exclusive but mutually reinforcing. Obfuscation techniques, when coupled with statistical Trojan detection, can preemptively safeguard against intellectual property theft and malicious modification, offering assurances that traditional software-based security measures cannot provide (Basak et al., 2017; Chakraborty & Bhunia, 2009).

Despite these advances, challenges persist. Voltage-based attacks illustrate that even sophisticated hardware protections are not fully impervious to side-channel exploitation in shared FPGA environments (Boutros et al., 2020). Future research must explore dynamic mitigation strategies, such as adaptive voltage regulation, fine-grained tenant isolation, and real-time anomaly detection, to address emerging attack vectors. Furthermore, balancing performance optimization with security enforcement remains an intricate task, particularly when deploying cryptographic workloads on resource-constrained FPGA clusters. The overhead introduced by encryption and monitoring must be carefully managed to preserve the latency advantages offered by hardware acceleration.

The zero-trust paradigm offers a robust conceptual framework, yet its operationalization in cloud-based FPGA infrastructures requires additional exploration. Continuous verification of both hardware and software components, tenant behavior analysis, and policy-driven resource allocation are essential for achieving end-to-end security assurance (Hariharan, 2025). Moreover, the integration of emerging cryptographic techniques, such as fully homomorphic encryption, may provide future avenues for performing computation on encrypted data without exposing sensitive information, though practical implementation at scale remains challenging (Kanna & Vasudevan, 2019).

From a broader perspective, the convergence of hardware security, cryptographic safeguards, and cloud-native acceleration strategies reflects a shift toward holistic cybersecurity in next-generation cloud services. The theoretical contribution of this research lies in demonstrating the synergies among these domains, emphasizing that a layered,

integrated approach is necessary to protect against multi-dimensional threats. Practically, the findings inform cloud service architects about resource management strategies, hardware selection criteria, and security enforcement mechanisms necessary for resilient, high-performance multi-tenant platforms.

CONCLUSION

This study provides a comprehensive analysis of FPGA-enabled cloud acceleration, hardware IP protection, and cryptographic security within multi-tenant environments. By synthesizing contemporary research, the paper establishes that high-performance computation and robust security are achievable through the integration of obfuscation-based hardware protections, statistical Trojan detection, voltage-attack mitigation strategies, and advanced encryption techniques. The adoption of a zero-trust framework ensures that each layer of the system is continuously verified, enhancing the resilience of shared cloud infrastructures.

Future research should focus on refining dynamic resource isolation techniques, optimizing encryption for high-throughput FPGA deployment, and exploring adaptive threat detection mechanisms capable of responding to evolving attack vectors. By advancing these areas, cloud providers can create multi-tenant platforms that not only maximize computational performance but also uphold stringent security and privacy standards, ultimately fostering trust in next-generation cloud ecosystems.

REFERENCES

1. Abhishek Basak, Swarup Bhunia, Thomas Tkacik, and Sandip Ray. 2017. Security assurance for system-on-chip designs with untrusted IPs. IEEE Transactions on Information Forensics and Security 12, 7 (July 2017), 1515–1528. DOI: https://doi.org/10.1109/TIFS.2017.2658544
2. Hariharan, R. 2025. Zero trust security in multi-tenant cloud environments. Journal of Information Systems Engineering and Management, 10.
3. Christophe Bobda, Joel Mandebi Mbongue, Paul Chow, Mohammad Ewais, Naif Tarafdar, Juan Camilo Vega, Ken Eguro, Dirk Koch, Suranga Handagala, Miriam Leeser, et al. 2022. The future of FPGA acceleration in datacenters and the cloud. ACM Transactions on Reconfigurable Technology and Systems 15, 3 (2 2022), 1–42. DOI: https://doi.org/10.1145/3506713
4. Andrew Boutros, Mathew Hall, Nicolas Papernot, and Vaughn Betz. 2020. Neighbors from hell: Voltage attacks against deep learning accelerators on multi-tenant FPGAs. In 2020 Proceedings of the International Conference of Field-Programmable Technology (ICFPT), 103–111.
5. Stuart Byma, J. Gregory Steffan, Hadi Bannazadeh, Alberto Leon-Garcia, and Paul Chow. 2014. FPGAs in the cloud: Booting virtualized hardware accelerators with OpenStack. In Proceedings of the IEEE 22nd International Symposium on Field-Programmable Custom Computing Machines (FCCM ’14), 109–116. DOI: https://doi.org/10.1109/FCCM.2014.42
6. Adrian M. Caulfield, Eric S. Chung, Andrew Putnam, Hari Angepat, Jeremy Fowers, Michael Haselman, Stephen Heil, Matt Humphrey, Puneet Kaur, Joo-Young Kim, et al. 2016. A cloud-scale acceleration architecture. In Proceedings of the 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO ’16), 1–13. DOI: https://doi.org/10.1109/MICRO.2016.7783710
7. Rajat Subhra Chakraborty and Swarup Bhunia. 2009. HARPOON: An obfuscation-based SoC design methodology for hardware protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 28, 10 (2009), 1493–1502. DOI: https://doi.org/10.1109/TCAD.2009.2028166
8. Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia. 2009. MERO: A statistical approach for hardware Trojan detection. In Proceedings of the 11th International Workshop Lausanne on Cryptographic Hardware and Embedded Systems (CHES ’09). Springer, 396–410.
9. Roy Chapman and Tariq S. Durrani. 2000. IP protection of DSP algorithms for system on chip implementation. IEEE Transactions on Signal Processing 48, 3 (2000), 854–861. DOI: https://doi.org/10.1109/78.824679
10. Fei Chen, Yi Shan, Yu Zhang, Yu Wang, Hubertus Franke, Xiaotao Chang, and Kun Wang. 2014. Enabling FPGAs in the cloud. In CF ’14: Proceedings of the 11th ACM Conference on Computing Frontiers, Article 3, 1–10. DOI: https://doi.org/10.1145/2597917.2597929
11. Derek Chiou. 2017. The Microsoft catapult project. In Proceedings of the IEEE International Symposium on Workload Characterization (IISWC ’17), 124–124. DOI: https://doi.org/10.1109/IISWC.2017.8167769
12. Goyal, V., Kant, C. 2018. An effective hybrid encryption algorithm for ensuring cloud data

security. Big Data Analytics, Singapore, pp. 195–210

13. Kanna, G.P., Vasudevan, V. 2019. A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data. Cluster Comput., 22(4), pp. 9561–9569

14. Subramanian, E.K., Tamilselvan, L. 2020. Elliptic curve Diffie–Hellman cryptosystem in big data cloud security. Cluster Comput., pp. 1–11

15. Alowolodu, O.D., Alese, B.K., Adetunmbi, A.O., et al. 2013. Elliptic curve cryptography for securing cloud computing applications. Int. J. Comput. Appl., 66(23), pp. 10–17

16. Wang, G-G. 2018. Moth search algorithm: a bio-inspired metaheuristic algorithm for global optimization problems. Memetic Comput., 10(2), pp. 151–164

17. Bh, P., Chandravathi, D., Roja, P.P. 2010. Encoding and decoding of a message in the implementation of elliptic curve cryptography using Koblitz's method. Int. J. Comput. Sci. Eng., 2(5), pp. 1904–1907

18. Shilpa, Lalitha, Prakash, A., & Rao, S. 2009. BFHI in a tertiary care hospital: Does being Baby friendly affect lactation success? The Indian Journal of Pediatrics, 76, 655–657

19. Singh, V. K., Mishra, A., Gupta, K. K., Misra, R., & Patel, M. L. 2015. Reduction of microalbuminuria in type-2 diabetes mellitus with angiotensin-converting enzyme inhibitor alone and with cilnidipine. Indian Journal of Nephrology, 25(6), 334–339

20. Gopinath, S., Giambarberi, L., Patil, S., & Chamberlain, R. S. 2016. Characteristics and survival of patients with eccrine carcinoma: a cohort study. Journal of the American Academy of Dermatology, 75(1), 215–217

21. Lin, L. I., & Hao, L. I. 2024. The efficacy of niraparib in pediatric recurrent PFA‑ type ependymoma. Chinese Journal