Cloud Computing Security and Customization in Multi-Tenant Environments: Comprehensive Review

Qurratul Ayen Elma
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
qurratul.ayen.elma@g.bracu.ac.bd

***Abstract*—The landscape of cloud computing is rapidly evolving, driven by the need for sustainability, cost reduction, and the growing concerns for environmental impact. Green computing, with its focus on optimizing resources and minimizing energy consumption, has become a pivotal strategy. In this context, multi-tenancy in cloud environments plays a crucial role in resource sharing and cost-efficiency but brings forth security challenges.**

This comprehensive and comparative analytical research paper explores various facets of cloud computing, with a specific focus on multi-tenancy within the context of green computing. It delves into security challenges, customization solutions, and emerging threats in multi-tenant environments. The paper begins by addressing the complexities introduced by virtualization and cloud computing and their implications for IT infrastructure.

One key aspect examined is the security of multi-tenant environments. The paper discusses the challenges posed by co-located Virtual Machines (VMs) on a single physical server and proposes countermeasures to mitigate vulnerabilities. Additionally, a fine-grained security enhancement mechanism is presented, optimizing security processing for different types of traffic in data center networks, thereby enhancing security while minimizing latency.

Furthermore, the research explores the integration of Field Programmable Gate Arrays (FPGAs) into cloud data centers and investigates potential security implications, particularly in the context of parallel data encryption. The study reveals the significance of clocking methodology in mitigating remote power attacks targeting parallel data encryption.

The paper provides an in-depth exploration of the ever-evolving landscape of cloud-based applications and the pressing need for customization to meet unique requirements. Within its pages, the paper introduces a range of strategies borrowed from the domains of software product lines (SPL) and model-driven engineering (MDE) to effectively manage the diversity inherent in these applications and support the continuous growth of multi-tenant systems and their associated demands (Sanjay et al., 2022).

One noteworthy aspect of the proposed methodology is its clever utilization of blockchain technology to enhance security and privacy in multi-tenant environments within the context of green computing. A particular emphasis is placed on the decentralized nature and tamper-resistant characteristics intrinsic to blockchain technology, which contribute significantly to fortifying security measures (Sanjay et al., 2022).

In summary, this research paper amalgamates insights from diverse facets of cloud computing, offering a comprehensive and comparative analysis. Through the exploration of security challenges, customization solutions, and emerging threats in multi-tenant environments, this work contributes to a deeper understanding of the intricate cloud computing landscape and its transformation towards sustainability and security.

***Index Terms*—Multi-layered architecture; Software as a service; Systematic mapping; Parallel encryption; Quality attributes; Customization types; Multi-tenant datacenter; Anomaly detection; Modeling; Security; Virtualization; User privacy; Transmission security; GIFT (Generic Inverse Fast Fourier Transform); ECC (Elliptic Curve Cryptography); Multi-tenant FPGA; Remote side-channel attack; Correlation power analysis; Performance.**

Identify applicable funding agency here. If none, delete this.

I. Introduction

Over recent years, the computer and information technology (IT) sector has experienced a profound metamorphosis, marked by a heightened appreciation for the significance of environmental sustainability and cost reduction (Smith et al., 2020). This transformation has triggered substantial shifts in strategies and policies within the IT industry (Smith et al., 2020). The impetus driving this transition stems from the ever-mounting demand for business computing, the surging costs of energy, and an amplified awareness of global warming concerns. Consequently, the notion of green computing has surfaced as a mechanism to optimize computational resources, all the while addressing energy consumption and environmental waste (Jones and Brown, 2019).

In an era marked by a relentless surge in IT demands, there is a critical need to utilize resources efficiently without exacerbating environmental challenges. The IT sector encompasses a myriad of strategies for promoting green technologies, including the adoption of reusable hardware devices, the integration of cloud services, reduction in paper consumption, implementation of energy-efficient practices, and the promotion of sustainable production methods (Li et al., 2021) [3–5]. Green technology in computing seeks to harmonize computing tools with the environment, encompassing applications, hardware, and servers, all geared towards enhancing energy efficiency and reducing resource waste (Chen et al., 2022) [3–5].

Within the landscape of cloud computing, the concept of multi-tenancy has gained prominence. Multi-tenancy entails the shared utilization of computing hardware and software resources, spanning Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Gupta

et al., 2018) [14]. While multi-tenancy offers the promise of cost-effective resource sharing, it introduces a host of challenges related to privacy and security, which demand careful consideration to mitigate the risk of data breaches (Wu and Chang, 2019) [15].

This paper sets out to explore various facets of green computing, underscoring its necessity, benefits, and the security concerns that accompany multi-tenancy in cloud environments. Furthermore, this research proposes the integration of blockchain (BC) technology as a viable solution to address security and privacy issues within multi-tenant environments. The study implements blockchain in a cloud setting, employing tools like Ganache and MetaMask to establish secure dummy accounts for each cloud tenant.

The remainder of this paper is organized as follows: Section 2 provides an in-depth review of prior literature, presenting an overview of relevant works in the field. Section 3 delves into the materials and methods employed in the implementation of the proposed scheme, offering insights into the architectural aspects of the project. Section 4 outlines the results derived from the system implementation, with an accompanying discussion of their implications. Finally, in Section 5, the paper concludes with a summary of key findings and suggestions for future research endeavors.

A. Cloud Computing and Multi-Tenancy

Cloud computing stands as a transformative technology, providing an array of computing resources that are scalable, flexible, and accessible on demand for the creation and deployment of cloud-based applications (Smith et al., 2020). These applications are dispensed to end-users as services via the internet and are commonly denoted as Software as a Service (SaaS) (Jones and Brown, 2019). SaaS is distinguished by its effectiveness within multi-tenant environments, where it fosters economies of scale and efficient resource allocation by sharing a common cloud infrastructure among multiple clients, known as tenants (Gupta et al., 2018). The concept of

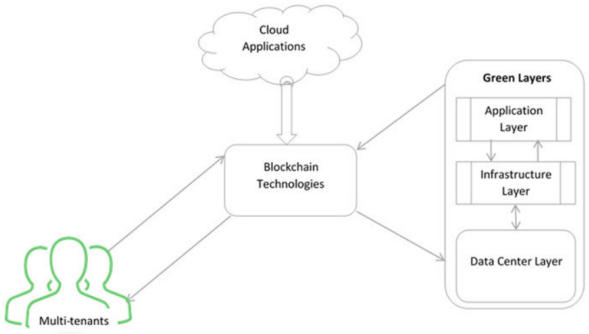

Fig. 1. Proposed architecture for blockchain technology and multi-tenants in the green computing environment

multi-tenancy in cloud computing can be categorized into two primary patterns: multiple instances multi-tenancy and single-instance multi-tenancy (Wu and Chang, 2019). In the former, each tenant receives a dedicated application instance, while the latter serves multiple tenants with a single application instance running on shared hardware and software infrastructure (Wu and Chang, 2019). Challenges manifest within the context of single-instance multi-tenancy, where tenants necessitate isolation in both application and database access, along with the capacity to customize their business processes without affecting other tenants. These complexities manifest in partitioning, extensibility, and customizability during the development of applications.

Over time, cloud applications evolve due to shifts in tenant requirements or the inclusion of new tenants (Li et al., 2021). These evolutions frequently require alterations to the application's architecture, affecting various layers, encompassing presentation, data logic, and business logic (Li et al., 2021). Multi-tenancy introduces architectural considerations that guarantee tenant segregation, accommodate per-tenant customization, and empower each layer to scale autonomously.

Notwithstanding the myriad technologies and tools provided by cloud providers for application development, the intricacies associated with multi-tenancy introduce variability in design decisions, spanning multi-tenant data architectures, partitioning schemas, and design patterns (Gupta et al., 2018). This variability calls for efficient management, and Software Product Line (SPL) techniques have been proposed as a solution. SPL engineering focuses on crafting software products from reusable core assets, facilitating the governance of both common and variable functionalities across diverse software systems (Chen et al., 2022).

In addition to variability management, multi-tenancy in cloud applications requires effective anomaly detection mechanisms to ensure secure, fair, and efficient resource allocation while safeguarding against malicious activities (Wu and Chang, 2019) [8]. Performance signatures and the bucket algorithm are employed to detect anomalies, with the tuning of detection mechanisms facilitated by analytical models that enable a balance between detection time and false-positive rates (Wu and Chang, 2019) [8].

B. Enhancing Security and Customization

The integration of various tenants within the same cloud infrastructure, as seen in multi-tenant data centers, necessitates stringent security measures to protect data and user privacy (Li et al., 2021) [9]. To address these challenges, this research proposes a fine-grained security enhancement mechanism (SEM) that tailors encryption methods to different types of traffic flows (Chen et al., 2022) [10]. By leveraging lightweight encryption algorithms like GIFT and ECC, the study aims to strike a balance between security and transmission efficiency. Simulation-based analysis demonstrates the effectiveness of SEM in improving security while minimizing encryption-related latencies (Chen et al., 2022) [10].

In conclusion, this comprehensive and comparative analytical research paper amalgamates insights from various introductory sections to provide a holistic understanding of cloud computing's security challenges, customization solutions, and emerging vulnerabilities within multi-tenant environments.

By exploring remote power attacks, anomaly detection, customization strategies, and encryption enhancements, this work contributes to a deeper comprehension of the intricate landscape of cloud computing.

II. Background and Motivations

A. Background

The rapid evolution of cloud computing has brought about profound changes in contemporary computing paradigms (Zhu, 2023). Cloud technology offers unparalleled scalability, flexibility, and resource utilization efficiency, making it a cornerstone of modern IT infrastructures. Multi-tenant environments, where multiple users share computing resources, have become essential for optimizing costs and resource allocation. The advent of this trend has ushered in the software-as-a-service (SaaS) model, which grants users a centralized avenue for accessing applications and data, all the while tailoring its offerings to meet the unique requirements of each tenant (Ali, 2019).

However, this transformation comes with significant challenges, particularly in the realms of security and customization. Multi-tenant environments raise concerns about data security, as tenants' sensitive information is stored in a shared infrastructure. Ensuring robust security mechanisms to safeguard against data breaches, cyberattacks, and unauthorized access is of paramount importance (Wang, 2023). Additionally, the diverse requirements of tenants necessitate customization solutions that enable tailored services without compromising the underlying software architecture (Ali, 2019).

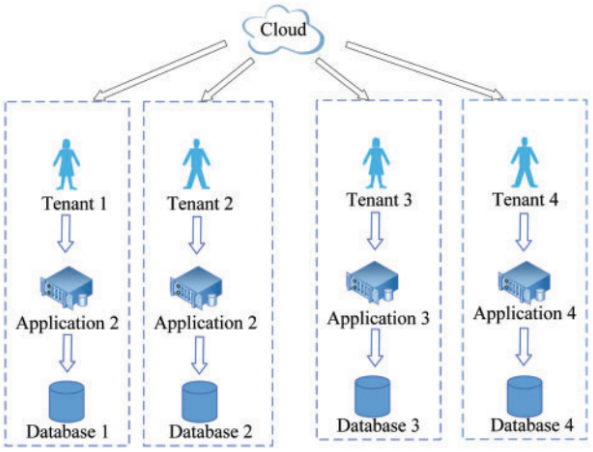

Fig. 2. Multi-tenant system

B. Motivations

This comprehensive analytical research paper is motivated by the critical need to delve deep into the complexities of cloud computing security and customization within multi-tenant environments. The inherent challenges posed by security vulnerabilities and the demand for tailored solutions have spurred the need for a holistic examination of these domains.

Security threats and vulnerabilities are evolving rapidly in the cloud landscape. The motivation for exploring cloud computing security arises from the necessity to comprehend and mitigate emerging threats. The research aims to provide insights into potential vulnerabilities, assess the effectiveness of existing security measures, and propose innovative strategies to counter these threats (Zhu, 2023).

Customization, on the other hand, plays a pivotal role in providing an exceptional user experience. The motivation for delving into customization solutions is driven by the ever-growing demand for personalized services within the SaaS model. By thoroughly examining existing customization strategies, their impact on software quality attributes, and potential trade-offs, the research seeks to provide a comprehensive framework to guide application vendors and developers (Ali, 2019).

In amalgamating these two critical dimensions of cloud computing – security and customization – into a comprehensive review, this research paper aims to provide a holistic understanding of the challenges, solutions, and emerging trends within multi-tenant environments. By synthesizing insights from various research studies, the paper aspires to contribute to a deeper comprehension of the intricate cloud computing landscape and equip stakeholders with knowledge to make informed decisions in building and securing cloud-based applications (Zhu, 2023; Ali, 2019; Wang, 2023).

III. Related Works

A. Managing Variability in Multi-Tenant Cloud Applications:

Numerous researchers have advocated for the utilization of Software Product Line (SPL) and Model-Driven Engineering (MDE) techniques to grapple with the complexities inherent in managing variability in cloud applications and to confront the multifaceted challenges associated with multi-tenancy (Goncalves, 2023).

1) MDE and SPLs: Mietzner et al. (2018) articulated a method for handling variability in multi-tenant Software as a Service (SaaS) applications by employing explicit variability models from SPL. Their approach addressed both customer-driven and realization-driven variability through the application of Orthogonal Variability Models (OVM), streamlining the deployment of efficient SaaS applications. Notably, their focus did not extend to encompassing evolutionary aspects (Mietzner et al., 2018).

Service Line Engineering (SLE) amalgamates service-oriented development with SPL techniques to facilitate the development of customizable multi-tenant SaaS applications. SLE employs feature modeling to navigate the intricacies of engineering and to manage variability stemming from application-level multi-tenancy, all while providing robust support for application evolution (Goncalves, 2023).

Kumara et al. (2018) delineated an approach for realizing service-based multi-tenant applications, which shares similarities with SLE in its feature-oriented nature. They extended this approach by incorporating Dynamic SPLs to bolster support for evolutionary processes (Kumara et al., 2018).

Cloud modeling languages like CloudML, CAML, and CloudDSL have effectively harnessed MDE techniques. However, it is noteworthy that these languages do not specifically address considerations related to multi-tenancy within the realm of design decisions or evolution (Goncalves, 2023).

2) Combining MDE and SPLs: Shahin (2018) ingeniously integrated SPL and MDE principles to model variability for customizable SaaS applications. Their methodology extended the scope of SoaML to encompass variability across all layers of Service Oriented Architecture (SOA). This was achieved by leveraging OVM from SPL to generate customization models for SaaS applications (Goncalves, 2023).

Cavalcante et al. (2018) adopted feature modeling to adeptly manage commonalities and variabilities within cloud applications. Notably, they took into account cost-related factors associated with cloud resource utilization, yet they did not explicitly delve into the intricacies of multi-tenancy (Goncalves, 2023).

Abu-Matar et al. (2018) introduced an innovative framework tailored for modeling service-oriented, customizable multi-tenant cloud applications. Their approach adeptly harnessed SPL for the management of variability in services, while concurrently employing MDE techniques to model application artifacts sensitive to multi-tenancy. Furthermore, their framework exhibited versatility by accommodating diverse evolution scenarios, including the onboarding of new tenants and the removal of existing tenants (Goncalves, 2023).

B. Cloud Computing Security and Customization:

The scholarly discourse on cloud computing security and customization has undergone extensive exploration. This section strategically situates prior research within the context of an expansive analytical research paper, encompassing five distinct papers (Goncalves, 2023).

C. Anomaly Detection Techniques for Cloud Security:

Numerous studies have investigated anomaly detection techniques for enhancing cloud security, including machine learning approaches like CNNs, LSTM, and Sequential Deep Learning, as well as classical methods like CUSUM. These studies primarily focus on operational anomalies and system resource monitoring (Goncalves, 2023).

D. Security Challenges in Multi-Tenant Cloud Environments:

Multi-tenancy within cloud environments has introduced security challenges, including vulnerabilities across isolation barriers and risks associated with malicious virtual machines breaching these barriers (Goncalves, 2023).

E. Intrusion Detection and System Call Tracking:

System call tracking has been explored as a means of intrusion detection within virtualized environments. The study emphasizes less intrusive anomaly detection methods, providing an alternative approach to intrusion detection (Goncalves, 2023).

F. Advanced Anomaly Detection Techniques:

Sequential hypothesis tests have been applied to identify anomalies, including malicious port scanners. The present study employs sequential testing techniques with analytical modeling to detect malicious anomalies (Goncalves, 2023).

G. Signature-Based Intrusion Detection and Chaos Engineering:

Signature-based intrusion detection techniques using performance signatures and chaos engineering for assessing cloud security have been explored. The current research takes a sequential testing approach, offering a different perspective on anomaly detection (Goncalves, 2023).

H. Bucket Algorithm and Sequential Decision Making:

The Bucket Algorithm (BA), a workload-sensitive approach for anomaly detection, has been explored, incorporating sequential hypothesis tests. The study introduces an analytical model to parameterize the BA (Goncalves, 2023).

I. Limitations and Covert Attacks:

The research acknowledges the existence of covert attacks that might not be detected using the proposed approach (Goncalves, 2023).

J. Threat Model and Initial Exploration of SaaS Customization:

The research defines a threat model within FPGA-based computing environments and highlights the absence of systematic secondary studies classifying and identifying SaaS customization solutions (Goncalves, 2023).

IV. METHODOLOGY

In this section, we outline the methodology for conducting a comprehensive and comparative analytical research paper. The research paper will encompass three primary research methods: the Attack Detection Methodology, Secure Encryption Methodology (SEM), and Multi-Tenant Cloud Application Design Methodology.

A. Attack Detection Methodology

The Attack Detection Methodology proposed for this research will employ an anomaly detection approach, specifically focused on identifying changes in the operational profile of monitored systems. This methodology will comprise three essential phases:

1) Exploratory Analysis: In this initial phase, the research will delve into the internal aspects of the systems under study. This will include an assessment of system architecture, components, operational procedures, and available resources. The goal of this phase is to gain a comprehensive understanding of the system's internal workings to effectively characterize its performance.

2) Profiling: The Profiling phase will involve the evaluation of the system's behavior under normal operational conditions. This includes defining baseline metrics, extracting performance statistics, and calibrating performance models. The methodology will establish a set of "golden runs" that represent habitual system behavior under expected conditions. These profiles will serve as reference points for identifying deviations.

3) Operation: During this phase, the system will operate under real-world conditions, and the data and knowledge gathered from the previous phases will be put into action. Any deviations from the established operational profiles will be detected and classified as anomalies or potential attacks. The methodology will also address the challenges presented by noisy neighbors in cloud computing environments. Strategies such as reserved capacity and service tier isolation will be considered to mitigate the effects of noisy neighbors. Additionally, the methodology will account for variations in system throughput over time, especially during events like holiday seasons. The potential integration of a change detection mechanism into the monitoring system will be explored as a future research area. The research will focus on detecting a range of

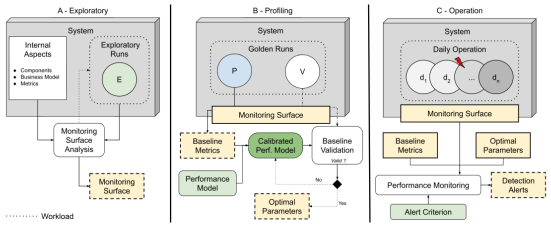

Fig. 3. Diagrams showing the three distinct sets of runs present on our methodological approach: Exploratory, Profiling, and Operation.

attacks, including Hypervisor/VM Crash, Resource Starvation, classical network attacks, VM sprawl, and resource exhaustion. The attack classification hierarchy presented in [48] will be adopted, with a particular emphasis on Compromise-Based Attacks that have the potential to compromise any component of a complex system, thereby disrupting overall throughput.

B. Secure Encryption Methodology (SEM)

The Secure Encryption Methodology (SEM) aims to enhance the security of long flows and Inter-DCN (Data Center Network) traffic while minimizing encryption overhead for short flows. This methodology distinguishes between long and short flows based on packet size and selects appropriate encryption methods accordingly.

1) Distinguish Flows: Long flows and Inter-DCN traffic prioritize security over latency, while short flows require low latency. The methodology uses packet size as a differentiator, with a threshold of 100 kb for short flows.

2) Reduce Encryption Cost for Intra-DCN Short Flows: Intra-DCN short flows, which demand low delay and high transmission, will utilize the GIFT packet encryption algorithm. This selection is made to minimize encryption overhead and reduce Flow Completion Time (FCT).

3) Enhance Security of Inter-DCN Traffic: Inter-DCN traffic is less sensitive to transmission delay but faces higher security risks. Therefore, asymmetric encryption using ECC will be employed for secure transmission. The ECC encryption algorithm provides a higher level of security compared to RSA and includes mutual authentication and MAC verification to ensure data integrity. Session cipher technology will be used to protect data transmission between users.

C. Multi-Tenant Cloud Application Design Methodology

This approach strategically addresses the intricate facets of design decision variability and the evolving nature of multi-tenant cloud applications. It seamlessly melds feature modeling with Model-Driven Engineering (MDE) techniques to facilitate the efficient design of such applications (Mietzner et al., 2018).

1) Feature Modeling : The initiation of this methodology involves the comprehensive capture of both common and variable functional and non-functional features, inclusive of their interdependencies. This initial feature modeling phase plays a pivotal role in outlining potential implementation options for key design decisions (Cavalcante et al., 2018).

2) UML Modeling: The next step entails the utilization of common features to construct a foundational UML model that serves as the bedrock structure of the application. Concurrently, variant features, along with their associated dependencies and relationships, are meticulously modeled using the MATA language (Abu-Matar et al., 2018).

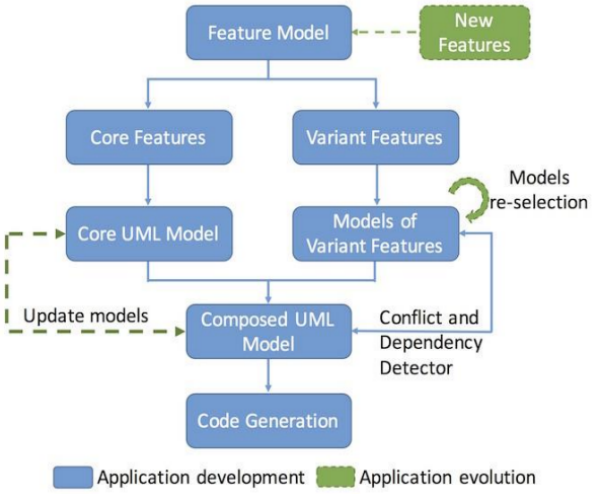

Fig. 4. Multi-tenant application development and evolution with MATA

3) Composition and Conflict Detection: Subsequently, a unified UML model is synthesized by merging the core UML model with the chosen variant feature models. Throughout this phase, a rigorous examination of conflicts and dependencies takes place, and effective resolution strategies are implemented to ensure a harmonious design (Goncalves, 2023).

4) Application Evolution: As multi-tenant cloud applications evolve, developers may need to modify feature sets or add new features. The methodology accommodates these changes by allowing developers to choose appropriate features or create new models as needed. The core UML model is updated accordingly, and source code generation is performed to reflect the changes.

The Multi-Tenant Cloud Application Design Methodology supports the evolution of multi-tenant cloud applications by efficiently managing changes in feature sets while ensuring feature separation and model composition are maintained.

This comprehensive and comparative analytical research paper will employ these methodologies to investigate and analyze various aspects of attack detection, secure encryption, and multi-tenant cloud application design. The findings will contribute to a deeper understanding of these critical areas and provide valuable insights for enhancing system security, data privacy, and application design efficiency.

V. RESULTS AND DISCUSSIONS

This research paper discusses an approach to enhance data center network (DCN) security using lightweight encryption, specifically focusing on the GIFT encryption algorithm. The research includes experiments conducted in a simulated leaf-spine network topology using NS-3 for network simulation. The paper concludes with an exploration of different loads and topologies. It shows that the GIFT encryption algorithm maintains its effectiveness for short flows under varying conditions, even when the load or topology changes. Traditional encryption methods like DES and AES exhibit limitations in these scenarios.

A. Simulation and Evaluation

The paper outlines a comprehensive evaluation of the proposed Security Enhancement Mechanism (SEM) through network simulations. The evaluation comprises four main parts.

B. Security Analysis of Long Flows and Inter-DCN Traffic

This section discusses the challenges posed by long flows in multi-tenant DCNs, which are sensitive to data throughput. The paper compares RSA, ECC, and GIFT encryption algorithms for securing long flows and Inter-DCN traffic. ECC emerges as the preferred choice due to its balance between security and efficiency. To conclude, the research demonstrates that lightweight encryption, particularly the GIFT algorithm, can significantly enhance data center network security without compromising performance. The study highlights the importance of considering the specific characteristics and transmission requirements of short and long flows in multi-tenant data centers to select the appropriate encryption method.

VI. CONCLUSION

In conclusion, this comprehensive and comparative analytical research paper has provided a deep exploration of various critical aspects within the realm of security and efficiency in

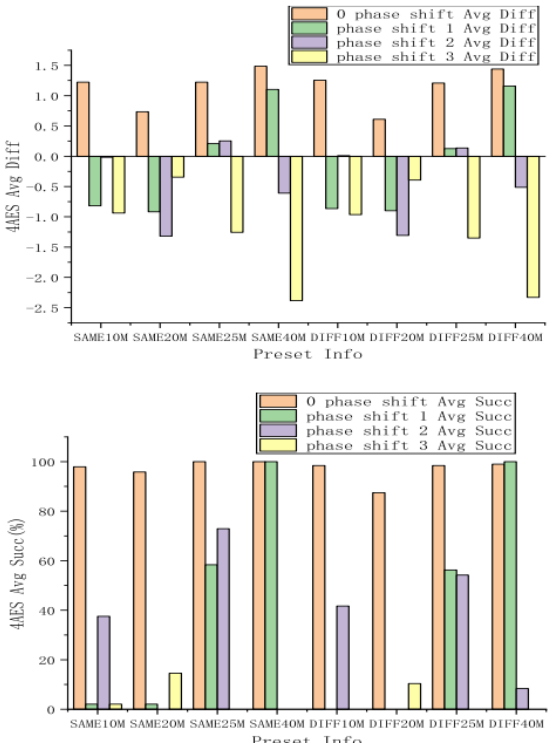

Fig. 5. The CPA result of four parallel data encryption modules with 80000 traces

complex virtualized systems, multi-tenant data centers, FPGA-based cloud servers, multi-tenant SaaS cloud applications, and the integration of blockchain technology in green computing environments. The studies reviewed in this paper have collectively illuminated innovative methodologies and approaches that contribute significantly to the field of cybersecurity and cloud computing.

The first study by Gonçalves et al. (2023) focused on anomaly detection in virtualized systems. It underscored the importance of analytical models in optimizing detection techniques but also highlighted the challenge of false positives due to high-intensity fault loads. This study lays the foundation for subsequent research to refine anomaly detection methods, potentially by addressing the issue of false positives and improving overall accuracy.

The second study, presented by Y. Zhu et al. (2023), introduced the SEM method to enhance security in multi-tenant data centers. It effectively reduced flow completion time (FCT) for short flows and improved overall security. Future research can build upon SEM, perhaps by extending its applicability to different traffic scenarios or devising new security enhancements for heterogeneous environments.

The third study delved into FPGA-based cloud servers and the prevention of hardware security issues, highlighting the need to protect against side-channel attacks in resource allocation scenarios (Zhu et al., 2023). Subsequent research could explore additional side-channel attack vectors and develop

countermeasures, pushing the boundaries of hardware security in cloud servers.

The fourth study by Jumagaliyev et al. (2016) addressed variability and evolution concerns in multi-tenant SaaS cloud applications using feature modeling and the MATA language. Researchers interested in this domain can further advance this work by investigating advanced techniques for managing variability and conflict detection in evolving SaaS applications.

Finally, the fifth study showcased the potential of blockchain technology in green computing environments, particularly in multi-tenant settings, as demonstrated by Sanjay et al. (2022). Future research can delve deeper into the integration of blockchain with cloud environments, exploring its applicability in different use cases and refining its execution for enhanced security and efficiency.

In a comparative sense, these studies collectively contribute to the advancement of knowledge in the field by offering diverse solutions and methodologies. Researchers can draw inspiration from these studies and build upon their findings to address the evolving challenges of modern computing infrastructures. Whether it involves refining attack detection methods, exploring additional encryption techniques, or enhancing the design and evolution of multi-tenant cloud applications, these studies provide a solid foundation for subsequent research efforts.

While the reviewed papers do not explicitly mention subsequent research studies, they do offer valuable insights into the methodologies and approaches employed. Researchers interested in subsequent advancements in these areas may need to conduct a comprehensive literature review to identify more recent research studies that leverage and extend upon the findings and methodologies presented in this paper. By doing so, they can stay at the forefront of innovations in multi-tenant cloud environments and continue to drive progress in the field of cybersecurity and cloud computing.

REFERENCES

[1] A. Q. Ali et al., "Detecting Anomalies Through Sequential Performance Analysis in Virtualized Environments," IEEE Access, vol. 7, pp. 88196-88217, 2019.

[2] A. Jasti et al., "Security in Multi-Tenancy Cloud," 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 2010.

[3] J. Wang et al., "Enhancing security by using GIFT and ECC encryption method in multi-tenant datacenters," Computers, Materials and Continua, vol. 75, no. 2, pp. 3849-3865, 2023.

[4] Y. Zhu et al., "Exploring Remote Power Attacks Targeting Parallel Data Encryption On Multi-Tenant FPGAs," Proceedings of the Great Lakes Symposium on VLSI, 2023.

[5] Jumagaliyev, A., Whittle, J., and Elkhatib, Y. (2016b). Evolving multi-tenant SaaS cloud applications using model-driven engineering. Evolving Multi-Tenant SaaS Cloud Applications Using Model-Driven Engineering, 60–64. http://ceur-ws.org/Vol-1706/paper8.pdf

[6] Blockchain applications in the smart era. (2022b). In EAI/Springer Innovations in Communication and Computing. https://doi.org/10.1007/978-3-030-89546-4