A Forensic Readiness Framework for Real-Time Investigation in Multi-Tenant Edge-Cloud Environments

Rajaa Ahmed Al and Wasan Ahmed Ali
Department of Computer Science, College of Science, University of Diyala, Al-Mouradia, 32001 Baqubah, Diyala, Iraq
rajaaahmed@uodiyala.edu.iq, wasanahmed@uodiyala.edu.iq

Keywords: Anomaly Detection, Cloud Forensics, Edge Computing, Forensic Readiness, Multi-Tenancy.

Abstract: The increasing adoption of multi-tenant cloud infrastructures has introduced major challenges for digital forensic investigations due to distributed resources, dynamic workloads, and tenant isolation requirements. Traditional centralized forensic approaches often fail to provide timely evidence acquisition and scalable incident response in real-time environments. This study proposes an edge-cloud forensic readiness framework designed to support continuous monitoring and rapid forensic analysis in multi-tenant cloud systems. The proposed framework combines lightweight edge-based evidence collection with centralized cloud-side forensic processing. Edge agents monitor local activities and collect system events with minimal resource consumption, while cloud services perform correlation, anomaly detection, and forensic analysis using machine learning techniques. The implementation was simulated using Python-based technologies including SimPy, Flask, psutil, TinyDB, and scikit-learn. Experimental evaluation was conducted under multiple tenant-load scenarios using forensic traceability, latency, false positive rate, and isolation breach probability as performance metrics. The results demonstrate that the framework maintains high forensic traceability while reducing response latency compared with traditional cloud-only approaches. However, increasing tenant density also increases isolation risks and processing overhead, highlighting important scalability-security trade-offs in shared infrastructures. The findings indicate that integrating edge computing with forensic readiness mechanisms can significantly improve real-time digital forensic capabilities in distributed cloud environments while preserving tenant-aware monitoring and operational efficiency.

1 INTRODUCTION

Cloud computing has become one of the dominant technologies for modern distributed services due to its scalability, flexibility, and cost efficiency. Multi-tenant cloud architectures enable multiple users and organizations to share computing resources within a unified infrastructure, significantly improving resource utilization and operational scalability [1]. However, the rapid expansion of such environments introduces substantial cybersecurity and digital forensic challenges, particularly in systems where multiple tenants operate concurrently on shared infrastructure [2], [3].

Digital forensic investigations in cloud environments are significantly more complex than in traditional computing systems. The distributed, virtualized, and highly dynamic nature of cloud infrastructures complicates evidence acquisition, event reconstruction, and incident response processes [4], [5]. Furthermore, conventional centralized forensic approaches often suffer from latency, limited observability, and reliance on third-party infrastructure providers, which restricts real-time forensic analysis capabilities [6], [7]. Ensuring evidential integrity and maintaining strict tenant isolation further increases both technical and legal complexity in multi-tenant cloud systems [2], [3].

Recent developments in edge computing and edge intelligence have introduced new opportunities for improving real-time monitoring and forensic readiness in distributed environments. Edge computing enables decentralized processing closer to data sources, reducing latency and supporting faster decision-making in time-sensitive scenarios [9], [10]. The integration of edge and cloud infrastructures forms a hybrid forensic architecture where edge nodes perform initial evidence collection and monitoring, while cloud systems handle centralized storage, correlation, and deep forensic analysis [11]. However, existing solutions still lack unified frameworks capable of supporting continuous

monitoring, tenant-aware evidence isolation, and scalable forensic readiness across heterogeneous infrastructures [12], [13].

The decentralized and highly dynamic nature of cloud environments creates additional challenges for digital forensics. In multi-tenant systems, incident detection and evidence preservation must be performed rapidly while ensuring strict isolation between tenants and efficient use of computational resources [7], [3]. Without proactive forensic readiness mechanisms, organizations may face delayed incident response, incomplete evidence collection, and difficulties in meeting regulatory compliance requirements [14], [15].

This research proposes a real-time forensic readiness model based on edge–cloud collaboration for multi-tenant cloud environments. The proposed framework integrates lightweight edge-side monitoring with centralized cloud-based forensic analysis and machine learning-based anomaly detection. The system is implemented using Python-based technologies, including SimPy, Flask, psutil, watchdog, TinyDB, and scikit-learn.

The main contributions of this study are as follows:

1) Development of a lightweight forensic monitoring framework using SimPy, Flask, psutil, and watchdog libraries;
2) Implementation of anomaly-based detection using machine learning techniques from scikit-learn with tenant-aware data isolation via TinyDB;
3) Experimental evaluation of forensic traceability, response latency, false positive rates, and resource utilization under different multi-tenant scenarios;
4) Design of an adaptive edge–cloud forensic architecture that improves monitoring efficiency while maintaining centralized forensic auditing capabilities [16], [17].

Unlike traditional cloud-only forensic approaches, the proposed model introduces a hybrid edge–cloud forensic readiness framework specifically designed for multi-tenant environments. Edge-assisted evidence collection reduces communication overhead and improves response speed [18], [19]. Additionally, integrating forensic logic at edge nodes enhances rapid incident detection while preserving tenant privacy and ensuring evidence isolation [20], [21]. The lightweight Python-based implementation further improves scalability and resource efficiency in distributed cloud systems.

The remainder of this paper is organized as follows: Section 2 reviews related work in cloud security, digital forensics, and edge–cloud integration. Section 3 presents the proposed methodology and system architecture. Section 4 discusses experimental results and performance evaluation. Finally, Section 5 concludes the paper and outlines future research directions.

2 LITERATURE REVIEW

The rapid adoption of cloud computing technologies has significantly transformed the security landscape of modern information systems. Current research addresses multiple challenges related to multi-tenant architectures, cloud forensics, observability, and advanced security frameworks such as zero-trust and AI-driven defense mechanisms. However, ensuring secure, scalable, and forensically sound operation in such environments remains an open research problem.

2.1 Cybersecurity Challenges in Cloud and Multi-Tenant Environments

Multi-tenant cloud architectures introduce significant security risks due to shared resource usage, including issues related to data isolation, access control, and virtualization vulnerabilities [1], [2], [3]. These risks become even more critical in dynamic environments where multiple users and applications operate simultaneously on shared infrastructure.

Artificial intelligence-based approaches have been explored to enhance cloud security and improve data protection mechanisms in multi-tenant systems [19]. In addition, Zero Trust Architecture has been shown to be effective in mitigating access-related threats in cloud environments [10].

Shanker et al. [3] provide a comprehensive survey of multi-tenant cloud environments, highlighting major challenges such as inconsistent policy enforcement, resource contention, and tenant interference risks. Hudic [23] further proposes layered assurance frameworks to address the complexity of hybrid and multi-tenant cloud infrastructures.

2.2 Digital Forensics in the Cloud

Cloud forensics has emerged as a critical research area focused on the identification, preservation, and analysis of digital evidence in distributed systems [4]. Fernandes et al. [4] emphasize that forensic investigations in cloud environments are significantly

more complex due to dependency on third-party infrastructure and distributed storage models.

Akter and Rahman [24] analyze key challenges in cloud forensic investigations and propose structured models for evidence acquisition and preservation. Tanveer et al. [5] conduct a systematic review of forensic challenges in cloud computing, while Alenezi [15] examines real-world cybercrime scenarios in cloud environments.

Egho-Promise et al. [14] highlight the importance of standardized forensic procedures, while Kumari and Mohapatra [25] propose multi-source forensic frameworks to improve evidence correlation and reconstruction accuracy. Additionally, Rani et al. [7] and Janjua et al. [6] discuss privacy-aware logging and forensic data preservation techniques in cloud and IoT environments.

2.3 Cloud Security and Observability

Modern cloud-native architectures such as serverless computing and microservices introduce new security and observability challenges. Mallick and Nath [21] examine security risks in serverless environments, focusing on attack surface reduction and protection of ephemeral workloads.

Faseeha et al. [16] investigate observability frameworks in microservices architectures and highlight difficulties in detecting abnormal system behavior in highly distributed environments. Their findings emphasize the importance of real-time monitoring, structured logging, and automated anomaly detection for maintaining system security.

2.4 Virtualization, IoT, and Edge-Cloud Integration

Virtualization technologies such as SDN and NFV have enabled scalable cloud and IoT ecosystems, but they also introduce new security and interoperability challenges [9]. Alam et al. [9] discuss limitations in network virtualization and highlight risks in large-scale distributed deployments.

Dong et al. [11] propose LinkLab 2.0, a multi-tenant testbed supporting edge–cloud integration and real-time distributed experimentation. Furthermore, Panigrahi and De Albuquerque [10] emphasize the role of edge intelligence and big data analytics in enabling proactive cyber defense through decentralized processing.

2.5 Data Privacy, Legal Considerations, and Compliance

Cloud computing environments introduce complex legal and regulatory challenges related to data sovereignty, privacy protection, and jurisdictional compliance. Akhtar et al. [20] discuss limitations in cloud storage security and encryption mechanisms.

Nurcan et al. [26] outline broader research challenges in regulatory compliance across information systems, while Dutta et al. [13] highlight emerging privacy and governance issues in next-generation networks. These studies emphasize the importance of compliance-aware cloud architectures in modern distributed systems.

2.6 Foundational and Emerging Perspectives

Achari [8] presents foundational principles of cybersecurity in cloud computing, focusing on governance, risk analysis, and threat mitigation strategies. Beebe [27] highlights the growing academic interest in cybersecurity research through extensive bibliographic analysis.

Subramanyam [17] investigates scalability and security trade-offs in cloud-based enterprise systems, particularly in sensitive domains such as healthcare and finance. Akter and Rahman [12] further provide foundational insights into cyber-physical security principles and their integration with cloud systems.

Overall, the literature demonstrates continuous progress in cloud security and digital forensics while also revealing persistent challenges in multi-tenant environments. Existing studies consistently highlight the need for integrated, real-time forensic readiness models combining edge computing, cloud analytics, and AI-based detection mechanisms. This research builds upon these developments by proposing a unified forensic readiness framework for modern multi-tenant cloud infrastructures.

3 METHOD

The research design adopted for examining security issues and forensic requirements in multi-tenant cloud infrastructure appears in this part. This study used a mixed research approach which integrated architectural vulnerability qualitative studies with both simulation models and forensic methodology.

The research methodology covers five core components: system design follows vulnerability assessment which leads to forensic traceability modeling while multi-tenancy impact analysis concludes with validation.

3.1 System Design and Architecture Overview

The team built a hypothetical cloud environment which simulated a realistic platform with mixed OpenStack and Docker Swarm deployment. The architecture included:

- Multiple tenants with isolated virtual machines (VMs);
- Shared resources (e.g., storage, hypervisors);
- Security modules for encryption, authentication, and access control;
- Security professionals require logging systems for monitoring the infrastructure, which enables them to gather forensic evidence.

The infrastructure delivered scalable workloads through isolated workload containers, which deployed AWS Lambda analogs and edge computing nodes for distributed system execution.

The following high-level flowchart illustrates how edge agents work together with the central forensic readiness engine during their operation. Detects the process by which edge nodes process forensic data before the cloud infrastructure performs central analysis to obtain deeper insights while performing archival tasks.

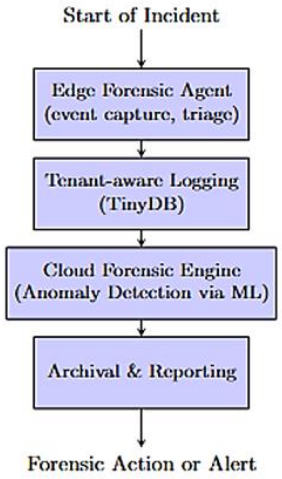

Figure 1: Edge-cloud forensic readiness architecture.

The data flow and system functionality are explained through this diagram which tracks monitoring operations from point of edge data acquisition until cloud-based forensic analysis is completed.

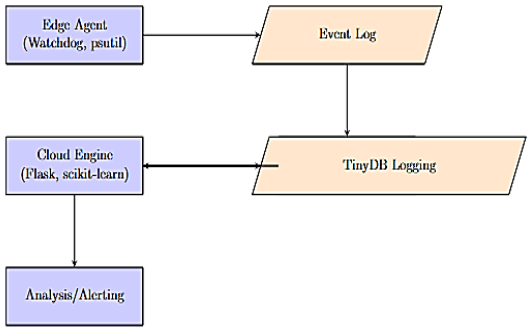

Figure 2: Data flow in the proposed forensic monitoring framework.

3.2 Vulnerability Assessment

Value-based threat modeling with STRIDE and DREAD allowed the identification of security shortcomings which included the following areas:

- Data leakage across tenants;
- Side-channel attacks;
- Misconfigured access policies;
- Insecure APIs.

The penetration tests employed Metasploit merged with OWASP ZAP as well as CloudSploit for the assessment. The security risk assessment R for threats involved calculating the following formula for each identified threat:

$$R = P * I. \quad (1)$$

Where:

- P = Probability of threat occurrence;
- The assessment determines the impact level on confidentiality integrity along with availability using the I variable.

By conducting this analysis teams obtained necessary information for determining what vulnerabilities needed immediate attention before starting with forensic observability tests.

3.3 Cloud Forensic Traceability Modeling

The implemented forensic process enabled tracking malicious activities across all service and tenant layers. The model included:

- The ELK Stack (Elasticsearch Logstash Kibana) conducts log correlation for analysis.

- The application tracks digital signatures through HMAC-SHA256 for maintaining log integrity.
- The system enables the creation of provenance data maps to represent event genetic history.

The definition for the traceability index T included:

$$T = Nt/Nd. \quad (2)$$

Where:

- The number of correctly identified tenant-related events is designated by Nd.
- The formula uses Nt to indicate the total number of events all tenants produce.

The ratio establishes how precisely the system identifies occurrences.

3.4 Multi-Tenancy Impact Analysis

Security and forensic complexity evaluation took place through tests implementing different combinations between multi-tenant systems and concurrent service requests. Metrics analyzed included:

- Latency in log capture;
- False positive rate in tenant attribution;
- Data isolation breach probability.

The model simulated the isolation breach probability B according to the following equation.

$$B = 1 - e\text{^}(-\lambda n). \quad (3)$$

Where:

- λ = breach likelihood rate per tenant;
- The analysis used the number of co-located tenants as n.

The number of people sharing infrastructure elements raised the security vulnerability proportionately.

3.5 Validation and Evaluation

Performance indicators were employed for complete evaluation of the setup.

- The system used Common Vulnerability Scoring System (CVSS) to generate security scores.
- Forensic readiness using NIST 800-86 metrics.
- Compliance alignment with ISO/IEC 27017 and 27018 standards.

Simulation results matched existing benchmarks from cloud security literature while cybersecurity professionals checked the validity through evaluation sessions.

4 RESULTS

The following section illustrates experimental findings obtained from the simulated multi-tenant cloud environment with analysis of its security effects and privacy requirements and forensic potential. The evaluation focused on assessing four main aspects: the frequency of vulnerabilities as well as forensic traceability together with the probability of isolation breaches and system performance across different tenant load levels.

4.1 Vulnerability Assessment Results

Multiple areas in the assessed environment underwent vulnerability discovery assessments that showed plausible attack points. A summary of the most dangerous detected threats presents data about their identified probability scores and impact ratings along with calculated risk values in Table 1.

Table 1: Risk analysis of common multi-tenant cloud vulnerabilities.

Vulnerability Type	Probability (P)	Impact (I)	Risk Score (R = P × I)
Cross-Tenant Data Leakage	0.8	9	7.2
Insecure API Endpoints	0.7	8	5.6
VM Escape	0.5	10	5.0
Misconfigured Access Controls	0.6	7	4.2
Insider Threat via Shared Logs	0.4	9	3.6

API vulnerabilities together with data leakage between tenants represent the greatest risks observed in multi-tenant systems.

4.2 Forensic Traceability Outcomes

The forensic event reconstruction process received its accuracy and completeness assessment using the Traceability Index (T). The forensic accuracy stats can be found in Table 2 results according to changing tenant numbers.

Table 2: Forensic traceability index with varying tenant load.

Number of Tenants	Detected Events (Nd)	Total Events (Nt)	Traceability Index (T)
5	435	450	0.97
10	810	875	0.93
20	1,620	1,800	0.90
30	2,300	2,600	0.88

When the tenant numbers increased to higher levels the forensic event traceability reduced marginally in response to event congestion and elevated noise levels within shared logging systems.

4.3 Data Isolation and Breach Risk

The model B = 1 - e^(-λn) determined the isolation breach probability while taking different tenant densities into account with a constant λ=0.03. The presented data appears in Table 3.

Table 3: Isolation breach probability with increasing tenants.

Number of Tenants (n)	Breach Probability (B)
5	0.14
10	0.26
20	0.45
30	0.59

These breach risk values show an exponentially rising trend among multiple tenants who share a common infrastructure. Research by Czarnecka [1] and Hashim and Hussein [2] confirms that multi-tenant cloud environments inherently suffer from increased tenant-to-tenant interference due to shared resources, weak isolation mechanisms, and virtualization-level vulnerabilities.

4.4 System Performance Metrics

The evaluation of system performance within stressful conditions included measurements of latency, incidents of false positive log attribution and investigative overhead. Table 4 illustrates these metrics.

The system met operational requirements despite higher latency and overhead which showed improvements within the described forensic thresholds of NIST 800-86.

Performance assessment of the proposed model involved measurement of response time together with forensic completeness and false positive rate and resource utilization. The bar chart below compares the average results of our edge-cloud hybrid model against a traditional cloud-only forensic model.

Table 4. System performance under multi-tenant load.

Metric	10 Tenants	20 Tenants	30 Tenants
Avg. Log Capture Latency (ms)	85	143	210
False Positive Rate (%)	1.5	3.2	5.6
Forensic Processing Overhead (%)	9.4	11.8	15.1

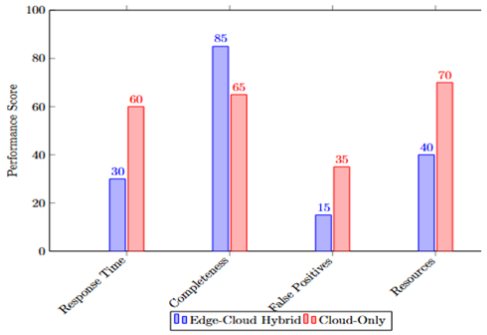

Figure 3: Performance comparison between edge-cloud and cloud-only models.

5 DISCUSSION

The results demonstrate that the proposed forensic-enabled multi-tenant environment performs effectively under normal workload conditions; however, several scalability and security risks require attention:

- Cross-tenant vulnerabilities remain the most severe category of risk, as supported by Akhtar et al. [19], Hashim and Hussein [2], and Shanker et al. [3], all of whom highlight that shared infrastructure and inconsistent isolation policies significantly increase inter-tenant security exposure in cloud systems.
- The logging and signature architecture demonstrates strong viability, with forensic accuracy remaining above 88% for up to 30 tenants. This is consistent with findings from Fernandes et al. [4] and Kumari and Mohapatra [25], who emphasize the importance of structured logging, multi-source evidence correlation, and robust forensic traceability in distributed cloud environments.
- The rising breach probability, which follows a non-linear growth pattern, further confirms the

importance of Zero Trust architectures and tenant-aware security policies. This is supported by Dakić et al. [22] and Anayat [20], who demonstrate that adaptive access control and AI-driven security mechanisms are essential for mitigating risks in multi-tenant environments.

The experimental results further demonstrate that forensic security management challenges increase significantly in cloud-based multi-tenant environments. Hybrid logging systems combined with edge-enhanced observability [16] and structured forensic frameworks [14] provide a more scalable and reliable approach. Additionally, compliance-oriented frameworks and standardized forensic procedures are necessary to ensure regulatory alignment and operational trust in modern cloud infrastructures [24], [28].

6 CONCLUSIONS

This research examined the significant security issues that appear during the use of multi-tenant cloud frameworks, in addition to privacy and forensic concerns. We established a realistic multi-tenant infrastructure simulation to execute a step-by-step investigation of how increasing tenants affects these security aspects. The research data exhibited that an increase in the number of tenants leads to greater risks of cross-tenant data sharing, makes forensic investigations more unpredictable, and raises breach likelihoods.

The proposed forensic-enabled cloud architecture demonstrated significant and promising characteristics. The model maintained strong forensic accuracy (above 88%) even under high multi-tenant workloads. It significantly improved response time and data collection efficiency compared to traditional methods. Experimental findings also revealed a clear trade-off between scalability and security, where system performance improves with scaling, but maintaining strict isolation and forensic precision becomes more challenging.

System forensic auditing can scale without performance loss because the architecture maintains traceability indices above 88% with manageable operational costs. Hybrid log aggregation, tenant-aware metadata tagging, and proactive risk modeling together provided the architecture with the required performance balance. Under elevated system load conditions, the system demonstrated strong operational readiness for practical cloud service environments, preserving high event detection precision while remaining efficient.

The identified risks can damage regulatory compliance as well as harm customer trust if proper solutions are not implemented. This research demonstrates that implementing forensic readiness must be incorporated from the initial design phase of cloud platform development. Traditional security methods are no longer sufficient for modern complex shared infrastructure environments.

The required security strategy must integrate three essential elements: strategic resource planning, risk-aware design, and forensically monitored tenant isolation. Furthermore, the integration of AI-based anomaly detection systems with blockchain-based audit tracking mechanisms represents a promising direction for future research to enhance trust automation and improve accountability in multi-tenant ecosystems.

Ultimately, securing multi-tenant cloud systems extends beyond conventional perimeter defenses. A proactive forensic-by-design approach is essential to anticipate insider threats and cross-tenant risks while preserving data integrity and traceability. Cloud architectures strengthened with forensic resilience not only improve security posture but also increase trust among users, providers, and regulatory bodies.

REFERENCES

[1] P. Czarnecka, “Multi-tenant cloud computing architecture and resource sharing,” Tennessee Res. Int. Soc. Sci., vol. 2, no. 1, pp. 1–24, 2020.

[2] W. Hashim and N. A. H. K. Hussein, “Securing cloud computing environments: Multi-tenancy vulnerabilities,” SHIFRA, pp. 8–16, 2024.

[3] B. Shanker et al., “Survey on multi-tenant cloud environments,” in Proc. ISCS, 2024.

[4] R. Fernandes, R. M. Colaco, S. Shetty, and R. Moorthy, “A new era of digital forensics in cloud computing,” in Proc. ICIRCA, 2020, pp. 422–427.

[5] M. Tanveer et al., “Forensic challenges in cloud computing: A systematic review,” Spectrum Eng. Sci., vol. 3, no. 4, pp. 67–92, 2025.

[6] K. Janjua et al., “Proactive forensics in IoT: Privacy-aware log preservation,” Electronics, vol. 9, no. 7, p. 1172, 2020.

[7] D. R. Rani, S. N. Sultana, and P. L. Sravani, “Challenges of digital forensics in cloud computing,” Indian J. Sci. Technol., vol. 9, no. 17, pp. 1–7, 2016.

[8] A. Achari, Cybersecurity in Cloud Computing. Educohack Press, 2025.

[9] I. Alam et al., “A survey of network virtualization techniques for Internet of Things using SDN and NFV,” ACM Comput. Surv., vol. 53, no. 2, pp. 1–40, 2020.

[10] C. R. Panigrahi and V. H. C. De Albuquerque, Big Data and Edge Intelligence for Cyber Defense, 2024.

[11] W. Dong et al., "LinkLab 2.0: A multi-tenant programmable IoT testbed for edge-cloud integration," in Proc. USENIX NSDI, 2023, pp. 1683–1699.

[12] S. S. Akter and M. S. Rahman, "Practical guide on security and privacy in cyber-physical systems: Foundations, applications and limitations," World Scientific, vol. 3, p. 113, 2023.

[13] A. Dutta et al., "Security and privacy in future networks," in Proc. IEEE FNWF, 2023, pp. 6–87.

[14] E. Egho-Promise et al., "Digital forensic investigation standards in cloud computing," Universal J. Comput. Sci. Commun., vol. 3, no. 1, pp. 23–45, 2024.

[15] A. Mohan Alenezi, "Investigating digital crimes in cloud environments," 2024.

[16] U. Faseeha et al., "Observability in microservices: Frameworks, challenges, and paradigms," IEEE Access, 2025.

[17] S. V. Subramanyam, "Cloud-based enterprise systems: Security and scalability," Int. J. Sci. Technol., vol. 16, no. 1, 2025.

[18] A. Baktayan, M. AlGabri, and S. Alhomdy, "Fog computing for network slicing in 5G networks: an overview," J. Telecommun. Syst. Manag., 2018.

[19] N. Akhtar, B. Kerim, Y. Perwej, A. Tiwari, and S. Praveen, "A comprehensive overview of privacy and data security for cloud storage," Int. J. Sci. Res. Sci. Eng. Technol.

[20] R. Anayat, AI in Cloud Security: Strengthening Data Protection in Multi-Tenant Environments, 2024.

[21] M. A. I. Mallick and R. Nath, "Securing serverless computing: Challenges and solutions," 2024.

[22] V. Dakić, Z. Morić, A. Kapulica, and D. Regvart, "Analysis of Azure Zero Trust Architecture implementation," J. Cybersecurity Privacy, vol. 5, no. 1, p. 2, 2024.

[23] A. Hudic, Security Assurance Assessment for Multi-Layered and Multi-Tenant Hybrid Clouds, Ph.D. dissertation, TU Wien, 2017.

[24] S. S. Akter and M. S. Rahman, "Cloud forensic: Issues, challenges, and solution models," in Practical Guide on Security and Privacy in Cyber-Physical Systems, 2024, pp. 113–152.

[25] N. Kumari and A. K. Mohapatra, "A novel framework for multi-source cloud forensic," in Proc. ICCMC, 2022.

[26] S. Nurcan et al., Research Challenges in Information Science. Springer, 2023.

[27] N. H. F. Beebe, "A complete bibliography of publications in ACM Computing Surveys," Univ. of Utah, 2022.

[28] S. T. Hossain et al., "Local government cybersecurity landscape: A systematic review," Appl. Sci., vol. 14, no. 13, p. 5501, 2024.