Review

Not peer-reviewed version

Multi-Tenancy Security in IoT-Cloud Systems: Challenges, Mitigations, and Future Directions

Bader Alobaywi *, Mohammed G. Almutairi, Frederick T. Sheldon *

Posted Date: 4 December 2025

doi: 10.20944/preprints202512.0463.v1

Keywords: multi-tenancy; cloud; cloud security; IoT-cloud integration; multi-tenant cloud security; IoT-cloud isolation

 doi:10.20944/preprints202512.0463.v1

Review

Multi-Tenancy Security in IoT-Cloud Systems: Challenges, Mitigations, and Future Directions

Bader Alobaywi [1,2,*], Mohammed G. Almutairi [1,2] and Frederick T. Sheldon [1,*]

[1] Department of Computer Science, College of Engineering, University of Idaho, Moscow, ID 83844, USA

[2] College of Computer Science and Engineering, University of Hafr Al Batin, Hafar Al Batin 39923, Saudi Arabia

* Correspondence: (alob8017@vandals.uidaho.edu) & (sheldon@uidaho.edu)

Abstract

The rapid convergence of the Internet of Things (IoT) and cloud computing has intensified reliance on multi-tenancy, a model that enables resource sharing to enhance scalability and reduce costs. However, this shared infrastructure introduces significant security vulnerabilities, particularly at the intersection of IoT's resource-constrained devices and the cloud shared environment. While existing literature has addressed IoT or cloud security separately, a significant research gap exists in analyzing the specific risks of multi-tenancy in these integrated systems. This review synthesizes recent research on mitigation techniques to address security and privacy challenges in multi-tenant IoT-cloud environments. We provide a comprehensive classification of threats, including inter-tenant data leakage, side-channel vulnerabilities, and privilege escalation. Our analysis reveals a persistent security-performance trade-off that limits the widespread adoption of robust defenses in resource-constrained IoT environments. Current mitigation techniques, including access control models and AI-driven detection systems, incur significant computational overhead. This makes them impractical for numerous IoT applications with constrained processing and energy resources. This review analyzes the limitations of existing approaches and identifies key architectural gaps. In this paper, we present a roadmap of emerging solutions to resolve this security-performance trade-off. This work emphasizes the integration of Zero Trust Architectures (ZTA) for continuous verification, adaptive AI for real-time threat detection, blockchain for immutable audit trails, and the adoption of Post-Quantum Cryptography (PQC) as essential strategies to secure the next generation of multi-tenant IoT-cloud infrastructures.

Keywords: multi-tenancy; cloud; cloud security; IoT-cloud integration; multi-tenant cloud security; IoT-cloud isolation

1. Introduction

The integration of the Internet of Things (IoT) and cloud computing has become a fundamental part of modern digital infrastructure, enabling exceptional scalability and resource sharing. This integration allows billions of distributed devices to offload computation and storage to powerful cloud backends. Also, it creates an infrastructure capable of supporting mission-critical applications in healthcare, transportation, smart cities, and industrial automation. At the core of this combination is multi-tenancy, an architectural model that allows multiple tenants (users or organizations) to operate within shared, virtualized environments. Thus, multi-tenancy significantly improves resource efficiency and reduces operational cost, making it essential for large-scale IoT deployments. The economic momentum behind this architecture is substantial. The global multi-tenant data center market was valued at approximately USD 56.10 billion in 2024 and is projected to reach USD 189.59 billion by 2034. This growth confirms that multi-tenancy is a foundational post for modern digital infrastructure [1]. However, this shared operational environment presents new security and privacy risks that do not exist in isolated or single-tenant systems. Prior work highlights weaknesses in access

 doi:10.20944/preprints202512.0463.v1

control configurations, data separation, and resource isolation across IoT-cloud systems [2,3]. These issues are due to the limited processing power, small memory footprints, and strict latency requirements. That makes traditional security mechanisms difficult to deploy at scale.

While several surveys have addressed general IoT security or broader cloud vulnerabilities [4], a significant gap exists in the literature. Existing reviews typically analyze IoT and cloud domains in isolation, overlooking how their integration fundamentally changes the threat landscape. The interaction between IoT's constrained devices and the cloud's complex multi-tenant infrastructure poses a unique risk. For example, cross-Virtual-Machine attacks, leaks, side channels, and inter-tenant privilege escalation are not sufficiently captured when these environments are studied separately. The lack of current studies leaves a clear research gap with practical implications for industry and academia.

This paper reviews the security challenges of multi-tenancy in integrated IoT-cloud environments. We provide a comprehensive classification of threats, including cross-tenant data leakage, misconfigured identity boundaries, side-channel exploitation, and noisy-neighbor resource contention. Our analysis emphasizes that the core challenge across current research is the continuous performance of a security trade-off. This means the strongest defense mechanisms impose significant computational overhead (e.g., 12% in documented cases), which many IoT deployments cannot take due to energy, memory, and latency limitations.

To address this gap, the review synthesizes the state of mitigation strategies, starting from enhanced access control models and virtualization safeguards to AI-driven anomaly detection and federated threat intelligence. Also, it critically evaluates their practical suitability for IoT environments. Additionally, we further highlight emerging trends that represent promising future directions, including Zero Trust Architecture, adaptive AI-driven analytics, blockchain-based auditing, and the rapid adoption of lightweight Post-Quantum Cryptography (PQC) for long-term resilience.

This review is guided by the following research questions, which frame the scope and provide a roadmap for the analysis:

1. What are the main multi-tenancy security threats in IoT-Cloud systems?
2. What mitigation techniques have been proposed, and how do they perform?
3. Which emerging technologies show promise for enabling secure, scalable, and future-proof multi-tenant IoT-cloud deployments?

Collectively, these contributions position this review as one of the early efforts to examine multi-tenancy security within IoT-cloud systems. Also, it provides a view of the key threats, current defenses, existing architectural gaps, and emerging technologies shaping future solutions.

2. Architecture Foundations of IoT-Cloud Integration

2.1. Internet of Things and Cloud Integration

The emergence of the Internet of Things (IoT) and Cloud integration has become a fundamental enabler of the next generation of intelligent, interconnected systems. This integration has introduced a new conceptual framework, the Cloud of Things [5]. IoT features an extensive number of heterogeneous devices, encompassing sensors, actuators, smart appliances, and industrial controllers that produce data streams. However, these devices are frequently constrained by limited processing capabilities, restricted storage capacity, and energy consumption considerations, thereby complicating the execution of complex tasks such as large-scale analytics, artificial intelligence inference, and long-term data management at the device level.

Cloud computing alleviates these constraints by providing virtually infinite storage capacity, robust computational resources, and elastic scalability, enabling IoT applications to expand or contract in accordance with demand [6]. Such integration allows IoT devices to transmit substantial workloads to cloud resources, thereby facilitating real-time data analysis, predictive insights, and decision-making processes that would otherwise be difficult to achieve locally. In addition to

 doi:10.20944/preprints202512.0463.v1

computational support, cloud services offer vital features like worldwide access, service coordination, and uniform interfaces, enabling interoperability among various IoT platforms [7]. This interoperability is essential in a wide range of fields, such as smart cities, healthcare, and industrial automation, where the IoT-cloud model enables seamless data collection from multiple devices, facilitating integrated services on centralized platforms for monitoring, diagnostics, and optimization.

2.2. IoT-Cloud Systems Architecture

The integration of IoT and cloud computing establishes a layered, service-oriented architecture intended to manage extensive data streams, provide real-time analytics, and support scalable applications. This architecture leverages the ubiquitous connectivity of IoT devices and the computational and storage capabilities of cloud technology to deliver intelligent and adaptable solutions. The IoT-Cloud system consists of five main layers: the perception (or physical) layer, the network layer, the edge/fog layer, the cloud layer, and the application layer, as shown in Figure 1. Each layer performs distinct, interdependent functions to ensure effective communication, resource allocation, and service delivery.

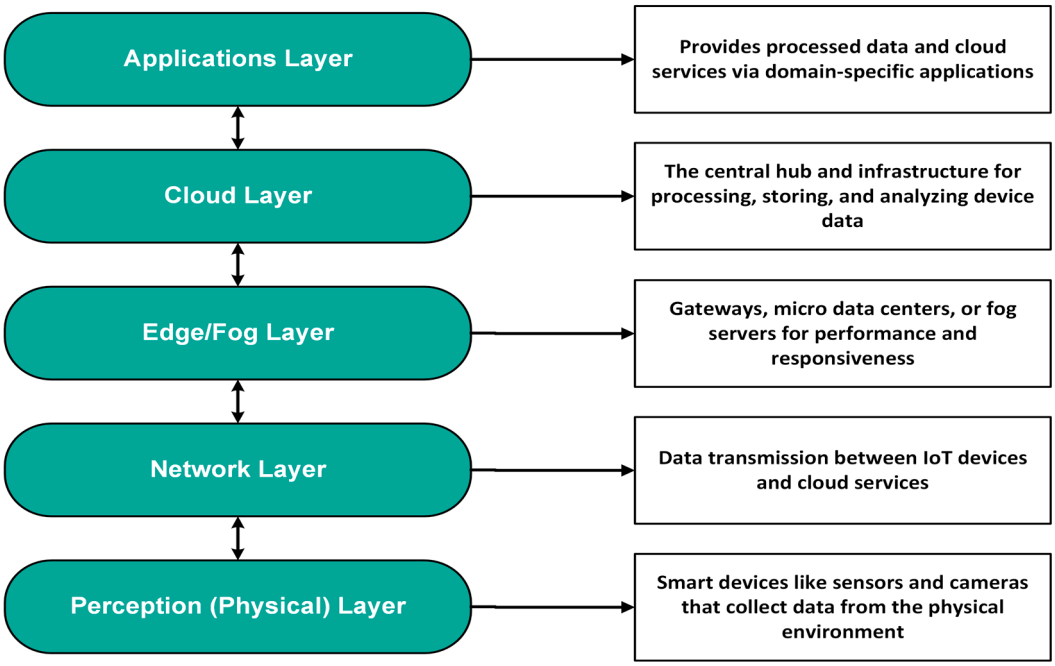

Figure 1. IoT-Cloud Architecture.

2.2.1. Perception (Physical) Layer

The perception layer forms the foundation of the IoT-Cloud architecture, comprising various smart devices like sensors, actuators, RFID tags, cameras, and wearable technologies that collect data from the physical environment. These devices are responsible for detecting parameters such as temperature, humidity, motion, or location, and converting them into digital signals. IoT devices with limited processing capabilities depend heavily on external processing and storage resources provided by higher layers in the architecture. Security at this layer is crucial, as devices are often physically accessible and vulnerable to tampering, spoofing, or data injection attacks [8].

2.2.2. Network Layer

The network layer ensures reliable, efficient data transmission between IoT devices and cloud services, using technologies like Wi-Fi, Bluetooth, Zigbee, 4G/5G, LoRaWAN, and NB-IoT [9]. This layer serves as a bridge, transporting the enormous data volumes generated at the perception layer

 doi:10.20944/preprints202512.0463.v1

to processing entities. Network management protocols, Quality of Service (QoS) mechanisms, and data encryption techniques are essential for ensuring the availability, reliability, and confidentiality of transmitted data.

Security remains a paramount concern within the network layer because it manages sensitive data and is vulnerable to various attacks [10]. As this layer is tasked with transmitting sensitive information between end-user devices and central processing hubs, it is particularly susceptible to a range of security threats. These include man-in-the-middle attacks, in which an adversary intercepts or alters communications, as well as denial-of-service (DoS) attacks that restrict data flow. This problem is aggravated by the massive proliferation and diversity of smart devices within IoT systems, which has significantly broadened the overall attack surface of IoT networks [10].

2.2.3. Edge/Fog Layer

Situated between the network and the cloud, the edge or fog layer improves the architecture's performance and responsiveness. This layer introduces intermediate computing nodes, such as gateways, micro data centers, or fog servers, that perform local data aggregation, filtering, and analytics before sending relevant information to the cloud. By processing data closer to the source, the edge/fog layer reduces latency, conserves bandwidth, and enables real-time decision-making, which is vital for time-sensitive IoT applications like autonomous vehicles and industrial automation [11]. Additionally, fog computing promotes privacy preservation by storing sensitive data locally when appropriate [12].

2.2.4. Cloud Layer

The cloud layer acts as the central hub and data repository within any IoT ecosystem, providing the essential infrastructure for processing, storing, and analyzing device-generated data. It provides elastic, scalable resources through virtualization and multi-tenancy, enabling multiple users or organizations to share the same physical infrastructure while maintaining logical isolation. Cloud computing can be deployed in public, private, or hybrid models depending on the desired control, cost, and security requirements. In the context of multi-tenancy, this layer must enforce strong isolation and security policies to prevent data leakage or unauthorized access among tenants. Presented herein is an analysis of the principal units of the cloud layer.

2.2.4.1. Cloud System Components

The cloud system is composed of several critical components that collaborate to provide cloud services. Therefore, understanding these units is essential for effective management and utilization of cloud resources.

- **Compute Resources:** Contemporary cloud infrastructures utilize a wide variety of computing resources to supply the processing power needed for modern applications and services. These core elements include virtualized servers like Amazon Elastic Compute Cloud (Amazon EC2) that operate independently on physical hardware; containers, offering lightweight and efficient virtualization at the OS level; and serverless computing, also known as Function as a Service (FaaS), that enables cost-effective, highly scalable applications without infrastructure management worries [13,14]. The combination of these paradigms has resulted in innovative solutions like serverless containers, such as AWS Fargate and the SCAR framework, which build on microservice architectures to make managing complex applications easier for users without system-level expertise [15,16]. However, the growing adoption of container-based virtualization has highlighted significant challenges in maintaining adequate isolation and security. This has led to the active development of innovative container runtimes and specialized security solutions aimed at mitigating these risks [13].
- **Storage:** Cloud storage solutions are fundamental to IoT architectures, as they must ingest and persistently store massive volumes of data at varying velocities and varieties. These solutions

 doi:10.20944/preprints202512.0463.v1

can be generally classified into three categories: object storage, including Amazon S3 and Azure Blob Storage, which are highly scalable and cost-efficient for unstructured data such as images, videos, and log files; block storage, providing high-performance virtual disks (volumes) for computing instances; and file storage, intended for shared access [17].

- **Networking:** Cloud networking components are integral to managing communication between cloud resources and external networks, enabling data ingress from IoT gateways. Key components include Virtual Private Clouds (VPCs), a fundamental aspect of this architecture that provides logically isolated virtual networks within a public cloud infrastructure [18]. Moreover, load balancers evenly allocate incoming traffic among multiple virtual machine instances to ensure high availability, reliability, and optimal performance, preventing the overloading or underutilization of networking nodes [19]. Content Delivery Networks (CDNs) mitigate latency by distributing content across geographically dispersed edge locations. Furthermore, these CDNs may be virtualized by utilizing cloud infrastructure, employing shared virtual machines within an Infrastructure as a Service (IaaS) model. This approach delivers tailored content-delivery services that dynamically scale resources to accommodate evolving demands while maintaining compliance with service-level agreements [20].
- **Management and Monitoring:** Cloud resource management and security rely on three primary categories of tools and services: monitoring, management, and automation. Monitoring tools such as Azure Monitor, Google Cloud Operations Suite, and AWS CloudWatch enable ongoing tracking of resource usage, system performance, and operational health. Management tools enable system administrators to efficiently provision, configure, and monitor cloud resources, often including features for policy enforcement and lifecycle management. Automation tools, including Azure Resource Manager, facilitate the deployment, scaling, and orchestration of resources via predefined templates and scripts. Collectively, these tools establish the technological foundation for advancing next-generation internet applications, expanding smart infrastructure markets, and optimizing business operations within cloud computing ecosystems [21].
- **Cloud Security:** Ensuring robust security is a paramount concern in cloud computing, necessitating a multifaceted approach to safeguard sensitive data and applications. At a fundamental level, security is established through both contractual agreements and technical controls. Service Level Agreements (SLAs) function as formal contracts to align data protection expectations between users and cloud service providers. Simultaneously, it is imperative to establish robust technical protections for data storage, transmission, and authorization [22]. These strategies usually involve encrypting data at rest and in transit, implementing protected authentication methods, enforcing strict access controls, employing data loss prevention techniques, and conducting regular security audits to ensure confidentiality, integrity, and availability [23].

More sophisticated strategies have also been suggested to improve this security stance. One specific approach combines Secure Sockets Layer (SSL) to encrypt data in transit, Message Authentication Codes (MACs) to ensure data integrity, and a data segmentation method. This segmentation involves splitting the data into parts, reducing the risk that a single compromise affects the entire dataset [24]. Additionally, a novel architectural approach, the two-tier WAY (Who Are You?) framework has been developed. This framework employs a virtual machine (VM) monitoring system to assess user trust and applies security strategies at multiple levels—network, infrastructure, and data storage to address the unique challenges posed by different cloud platforms [25].

2.2.4.2. Cloud Service Models

Infrastructure as a Service (IaaS) is a cloud computing paradigm that provides virtualized computing resources, including virtual machines, storage, and networking, over the internet. Operating as a utility-like service, IaaS offers a scalable platform for data storage and networking, enabling users to access servers and storage facilities on demand [26].

 doi:10.20944/preprints202512.0463.v1

Platform as a Service (PaaS) delivers an online platform for application development, providing hardware and software tools such as frameworks, databases, and middleware. This model allows developers to build, deploy, and manage applications without the complexity of maintaining the underlying infrastructure. PaaS offers a comprehensive development environment with Application Programming Interfaces (APIs) that enable the creation of custom applications and obviate the requirement for local hardware and software configuration [27].

Software as a Service (SaaS) provides fully functional software applications to users via the internet. In this model, end-users access ready-to-use software, such as email services, CRM systems, and collaboration tools, directly through a web browser. This approach eliminates the need for local installation and maintenance, with services typically offered on a subscription or as-you-go model [27].

2.2.4.3. Cloud Deployment Models

Public Cloud is owned and operated by a third-party cloud service provider, such as Amazon Web Services, Microsoft Azure, or Google Cloud. This type of cloud delivers computing resources over the internet and operates on a multi-tenant model, offering immense scalability, pay-as-you-go pricing, and a broad portfolio of services. For many IoT applications, the public cloud is predominantly chosen for its cost-effective entry point and elastic scaling, which address unpredictable, high-volume data loads from millions of devices.

Private Cloud comprises computing resources dedicated solely to a single business or organization. It may be situated within the client's data center or managed by an external service provider. This model provides the highest levels of control, security, and privacy, making it an optimal choice for IoT applications in sensitive sectors such as healthcare or critical infrastructure.

Hybrid Cloud integrates a private cloud with one or more public cloud services, facilitating the sharing of data and applications across these environments. This model offers organizations greater flexibility by enabling them to leverage the scalability of the public cloud for non-sensitive data processing and analytics, while retaining sensitive IoT data or low-latency control applications within their private cloud. This strategic approach is becoming increasingly prevalent in mature IoT deployments that require a careful balance among cost, performance, and compliance [28].

Community Cloud is a collaborative cloud deployment model in which infrastructure is exclusively allocated to a designated community of organizations sharing common interests. These interests commonly pertain to security, privacy, or regulatory compliance, which are prevalent in sectors such as government, healthcare, and finance. The community cloud functions as an intermediary between public and private clouds, integrating the cost-sharing benefits of a multi-tenant arrangement with enhanced security and privacy features inherent in dedicated infrastructure.

2.2.5. Application Layer

The application layer provides processed data and cloud services to end users via domain-specific applications. This layer encompasses a wide range of sectors, including smart cities, healthcare, transportation, industrial control, agriculture, and energy management. Moreover, this layer facilitates efficient communication between IoT devices and cloud services via various protocols such as MQTT, CoAP, XMPP, and AMQP [28,29]. Applications at this layer depend on APIs and service interfaces to facilitate interaction with the underlying infrastructure. APIs offer functionalities such as data visualization, decision support, and automated control [30].

Security is a primary consideration at the application layer, as it directly interfaces with end users and is often responsible for processing sensitive data. To ensure the delivery of a trustworthy service, key mechanisms at this level include access control, user authentication, and data integrity verification [31]. The primary security concerns at this stage pertain to users' data privacy and the applications they utilize, as outlined below[32].

 doi:10.20944/preprints202512.0463.v1

- **Access Control Attack**: Access control prevents unauthorized users from accessing IoT data, ensuring it remains restricted to legitimate users. However, if that access is compromised, the entire IoT system is at risk.
- **Malicious Code Injection Attacks:** An attacker injects malicious code or scripts from an unknown source into the system, hacking authorized user data and stealing or manipulating important user information.
- **Sniffing Attacks:** An attacker can monitor network traffic using sniffer applications, which can reveal confidential user data.

Overall, the IoT-Cloud architecture establishes a robust ecosystem that converts raw sensor data into actionable insights via seamless integration of physical devices with virtualized cloud services. Nevertheless, this closely integrated architecture presents numerous challenges, including latency management, data privacy, interoperability, and particularly security issues in multi-tenant environments, a subject that continues to be a primary focus of ongoing IoT-Cloud research.

2.3. Multi-Tenancy Cloud Systems

Multi-tenancy is a fundamental architectural principle in cloud computing, facilitating a single software instance and its underlying infrastructure to serve multiple distinct user groups, referred to as tenants. This model constitutes the foundational element of the "as-a-Service" economy (SaaS, PaaS, IaaS), providing substantial economies of scale, enhanced resource optimization, and diminished operational expenses through the sharing of computing, storage, and networking resources [33]. Implementing multi-tenancy in IoT ecosystems poses a complex, multi-layered challenge. An IoT-Cloud platform is required to manage multi-tenancy not only at the levels of cloud applications and databases, but also to enforce it throughout the entire data lifecycle, encompassing device connectivity, messaging, data processing, and storage.

Multi-tenant sharing of compute, storage, and networking resources creates additional attack surfaces not found in single-tenant setups: co-residency (whether physical or logical), shared hypervisors and kernel instances, common management APIs, and multi-tenant storage architectures can all serve as points for cross-tenant interference or data leaks when isolation fails. These risks are well documented in cloud security literature and remain a core part of threat models for tenant isolation[34]. There are three main models of multitenancy in IoT-Cloud systems [35]:

1. **Single Database:** Each tenant has a dedicated application and database instance.
2. **Shared Database, Isolated Schema:** A single database instance is utilized; however, each tenant maintains a separate schema.
3. **Shared Database, Shared Schema:** All tenants utilize the same database schema, with mechanisms implemented to distinguish their data.

2.3.1. Mechanisms of Tenant Isolation

The convergence of IoT and cloud computing has heightened the significance of multi-tenancy security issues, introducing additional complexities in managing shared infrastructure and heterogeneous devices. In IoT-Cloud architectures, large numbers of interconnected, diverse devices simultaneously connect to shared cloud resources for data storage, analytics, and orchestration services. This extensive interconnection substantially enlarges the attack surface and complicates tenant isolation. The primary objective of such environments is to ensure strict logical isolation among tenants across the entire platform stack, such that the data, devices, and configurations of one tenant remain inaccessible and invisible to all others.

Effective multi-tenancy in IoT-Cloud environments requires isolation mechanisms spanning several layers of the system architecture. These layers collectively define how tenants are separated at the physical, logical, and application levels to preserve confidentiality, integrity, and availability.

2.3.1.1. Device and Connectivity Isolation

 doi:10.20944/preprints202512.0463.v1

At the foundational layer, device and connectivity isolation ensure that each IoT device is securely provisioned and authenticated to its specific tenant. Communication protocols, such as Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Constrained Application Protocol (CoAP), must be configured to prevent cross-tenant data visibility and interference. This is typically achieved by implementing tenant-specific namespaces and access control lists (ACLs) at the message broker level, preventing unauthorized tenants from publishing or subscribing to another tenant's data streams. Additionally, secure onboarding procedures, unique device credentials, and mutual authentication mechanisms are critical to maintaining isolation at the device layer.

2.3.1.2. Network Isolation

Network isolation is a critical security control in multi-tenant architectures, designed to segregate tenant traffic and resources to prevent cross-tenant data leakage, interference, and unauthorized access. The primary objective is to establish secure boundaries that protect tenant confidentiality and integrity while maintaining performance and regulatory compliance. These strategies are broadly classified into two main categories: physical and logical isolation [36].

1. Physical Isolation

Physical isolation represents the strongest, most straightforward form of network segregation. This approach involves dedicating distinct, separate physical network hardware—such as switches, routers, or entire private data centers to each tenant. By eliminating shared resources, it effectively removes the attack surface for network-level cross-tenant interference. However, this model's high cost, operational rigidity, and inefficient resource utilization (low scalability) make it economically unviable for most of the public cloud and large-scale IoT applications, reserving it for environments with extreme compliance and security requirements.

2. Logical Isolation

Consequently, logical isolation has become the predominant model in cloud and IoT-Cloud systems. This approach leverages software-defined constructs to partition a shared physical infrastructure, balancing isolation, cost-effectiveness, and scalability [37]. The mechanisms for logical isolation exist on a spectrum from coarse-grained network segmentation to fine-grained, workload-centric controls.

- Virtual LANs (VLANs) are logical clusters of network devices separated from devices on other VLANs, regardless of shared physical infrastructure. Each tenant is assigned a unique VLAN, providing network traffic isolation. VLANs are scalable, adaptable, and economical, although managing them becomes more complex as the tenant count grows.
- Virtual Private Networks (VPNs): A VPN establishes a secure, encrypted tunnel for a tenant's data transmission over a shared network. Each tenant is allocated a distinct private virtual network within the shared infrastructure, ensuring all traffic is encrypted and isolated from other tenants. This mechanism offers robust security and privacy for tenant communications; however, it may also introduce latency and pose scalability challenges if not properly managed.
- Software-Defined Networking (SDN) facilitates dynamic and programmable control of network traffic. Through the utilization of SDN, tenants are able to isolate their network traffic via software configurations that establish virtualized networks on a shared physical infrastructure. SDN is characterized by its high flexibility and scalability; however, it necessitates sophisticated software-defined network infrastructure and management.
- Network policies and micro-segmentation: Micro-segmentation is a network security strategy that partitions a network into discrete, isolated segments. This methodology facilitates the granular isolation of tenants' networks and applications by enforcing policies engineered to govern traffic flow and mandate separation. Implementation is commonly achieved via technologies such as network firewalls, access control lists (ACLs), and policy-driven routing. While this approach affords highly fine-grained control over network access, it introduces

 doi:10.20944/preprints202512.0463.v1

significant management complexity, particularly within large-scale, multi-tenant architectures [36].

2.3.1.3. Resource Isolation

Resource isolation in multi-tenant systems ensures that the computational, storage, and network resources allocated to one tenant remain independent of those allocated to others. Its primary goal is to prevent any tenant's workload from degrading the performance, security, or availability of shared infrastructure while maintaining efficient utilization and scalability.

In IoT-cloud environments, resource isolation is implemented across multiple layers, including hardware, virtualization, containerization, and applications. Virtual machines (VMs) and containers (e.g., Docker, Kubernetes) are commonly used to separate tenant workloads, ensuring that a fault or compromise in one environment does not impact others.

To guarantee fair access and prevent resource contention, systems typically enforce per-tenant quotas on CPU, memory, storage, and network bandwidth. These limits are managed through virtualization controls frameworks to achieve balanced performance and predictable service quality across tenants.

Effective resource isolation not only mitigates "noisy neighbor" effects but also strengthens overall multi-tenancy security by reducing the risk of denial-of-service (DoS) conditions, side-channel exploitation, and privilege escalation across shared cloud and IoT infrastructures [36].

2.3.1.4. Data Isolation

Data isolation is fundamental to multi-tenancy security, as IoT-cloud systems generate and store substantial volumes of time-series telemetry, metadata, and analytics results in shared databases. Logical separation of tenant data within these repositories is essential to prevent data leakage or inference attacks. Different database isolation models address this need, including separate databases per tenant, distinct schemas for each tenant, or a shared schema. The selection of an appropriate model is typically guided by scalability, performance, and regulatory compliance considerations [38].

2.3.1.5. Application Isolation

At the software level, application isolation ensures that tenants' user interfaces, business logic, and rule engine configurations are securely partitioned. One technique is employed in such isolation, whereby each tenant should operate within a distinctly separate runtime environment, supported by tenant-aware Role-Based Access Control (RBAC) systems. This ensures that users and APIs are scoped strictly to the resources owned by their respective tenants. Application-layer isolation is particularly important in IoT-Cloud environments, where shared analytics engines and visualization dashboards might otherwise enable inadvertent or malicious cross-tenant data exposure [39].

2.3.1.6. Management and Governance Isolation

Beyond data and application separation, management and governance isolation involves enforcing clear boundaries in system administration, configuration policies, and monitoring activities. Multi-tenant platforms must ensure that operational tools, logs, and telemetry are tenant-specific to avoid indirect information leakage. Furthermore, proper segregation of administrative privileges across tenants is necessary to prevent lateral privilege escalation within shared environments [36].

3. Critical Analysis of Multi-Tenancy Security

The integration of IoT and cloud computing has inspired a growing number of studies examining data privacy, virtualization security, and cross-domain trust management. Nevertheless, research addressing multi-tenancy, a defining feature of modern cloud infrastructures within IoT-Cloud contexts, remains fragmented. Despite progress across these domains, studies rarely examine

 doi:10.20944/preprints202512.0463.v1

multi-tenancy within IoT-cloud environments as a unified security challenge. This section analyzes these findings collectively to surface unresolved gaps in isolation, performance, and architecture.

Multi-tenancy architectures naturally increase the attack surface because multiple tenants operate within shared virtualized environments. These issues are summarized in the threat model shown in Figure 2, which highlights how shared virtualized resources expose tenants to cross-tenant attacks. Studies have shown that such shared infrastructures expand security risks, particularly regarding data confidentiality, access control, and resource isolation. [2,3] emphasized that multi-tenant deployments expose serious vulnerabilities, as shared physical resources enable malicious tenants to compromise or access confidential data. In addition to these risks, the distributed and heterogeneous nature of IoT systems renders tenant isolation an ongoing challenge.

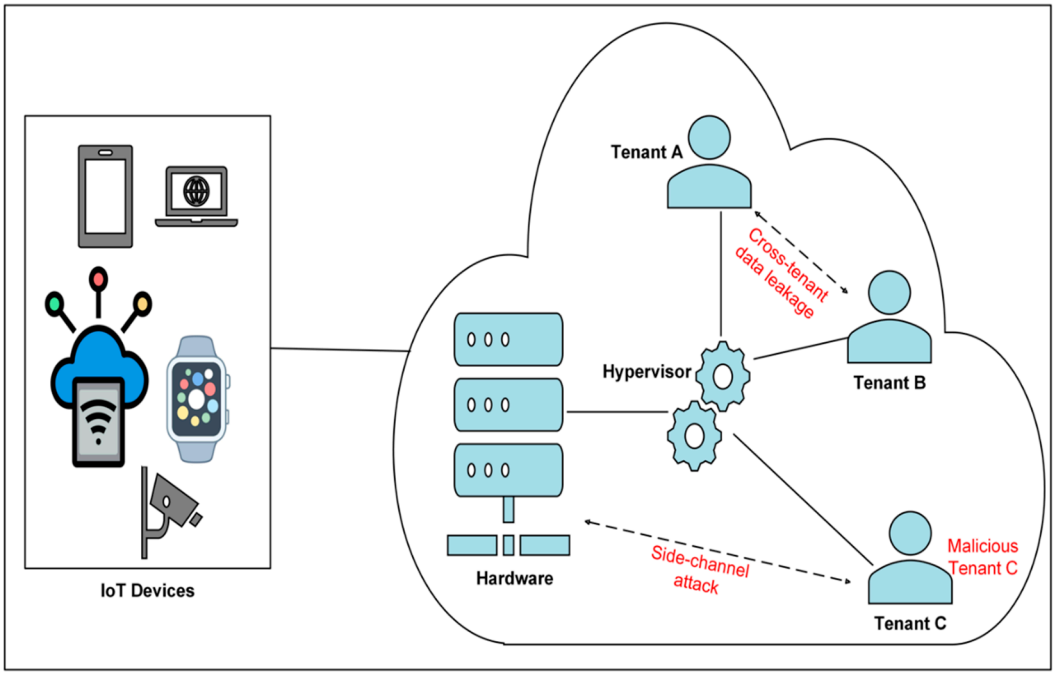

Figure 2. Threat Model of a Multi-Tenant IoT and Cloud Environment.

3.1. Classification of Multi-Tenancy Security Risks

Building on the risks outlined in Figure 2, recent research classifies multi-tenancy threats into several dominant categories. Cross-tenant data leakage remains one of the most critical threats in shared IoT-cloud platforms [40]. These leaks often come from improper isolation of virtualized resources, insecure APIs, or poor access configurations. Wahidah Hashim et al. reported that weak permission models and misconfigured authorization mechanisms are frequent sources of tenant-level data exposure [2]. Ritesh Kumar et al. further demonstrated that insufficient isolation between virtual machines or containers can enable cross-tenant inference attacks and unauthorized side-channel movement within the infrastructure [39].

In addition to these logical threats, several studies highlight the potential for physical and timing-based attacks. Side-channel vulnerabilities, denial-of-service (DoS) incidents, and API-level exploitation have been repeatedly observed in multi-tenant environments. Empirical evidence suggests that while enhanced encryption and access control can lower successful attack rates to approximately 5%, these defenses typically put a performance overhead of about 12% [2]. These trade-offs between security and efficiency are especially problematic in IoT workloads that require low latency and minimal resource consumption. Table 1 summarizes key studies that illustrate these risks and highlight limitations in current mitigation strategies.

Table 1. Summary of Existing Studies on Multi-Tenancy Security.

 doi:10.20944/preprints202512.0463.v1

Author(s)	Focus / Approach	Key Contribution	Remarks
Hashim et al., 2024 [2]	Tenant isolation & access control	Enhanced encryption reduced attacks ~5%	12% overhead; limited scalability
Surianarayanan et al., 2023 [3]	Data confidentiality	Exposed leakage risks in shared setups	No mitigation modeling
Panguraj et al., 2025 [40]	Resource sharing	Identified inter-tenant leakage paths	No integrated isolation model
Kumar et al., 2020[39]	VM isolation	Simulated weak boundaries	Lacked IoT performance context
Kyriakidou et al., 2024 [41]	ABAC + Verifiable credentials	Tenant-level privacy authentication	Added computation overhead
Yadav et al., 2025 [42]	Zero Trust analytics	Continuous access validation	Not tested at scale
Pandit et al., 2025 [43]	AI anomaly detection	97.3% accuracy for tenant attacks	Training bias; scalability issue
Neto et al., 2022 [44]	Federated DDoS detection	84.2% accuracy; privacy preserved	Energy overhead
Almutairi et al., 2025 [4]	AI & PQC survey	Highlighted framework gaps	No unified integration
Malikireddy et al., 2024 [45]	Elasticity testing	Found inadequate dynamic security	No adaptive model proposed
Hariharan et al., 2025 [46]	Zero Trust	Continuous verification model	Conceptual; no IoT validation
Sebestyen et al., 2025 [47]	Blockchain audit	Immutable audit trails	Scalability constraints

3.2. Existing Mitigation Techniques

Early approaches for securing multi-tenant cloud environments were primarily driven by major cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. These platforms introduced foundational mechanisms including strong virtualization boundaries (e.g., AWS Nitro hypervisor isolation), tenant-scoped Identity and Access Management (IAM), Virtual Private Cloud (VPC) segmentation, hardware-assisted encryption, and continuous compliance monitoring. While these industrial solutions offer robust baseline protections, they are generally optimized for traditional cloud workloads rather than the resource-constrained and latency-sensitive characteristics inherent to IoT ecosystems [48].

Researchers have proposed multiple defense mechanisms to address these issues. For example, Kyriakidou explored Attribute-Based Access Control (ABAC) with verifiable credentials as a privacy-preserving authentication method that implements stronger tenant-specific identity verification [49]. Also, Multi-layered security frameworks grounded in Zero Trust principles have become popular, focusing on continuous validation and access control. These architectures integrate behavioral analytics to monitor user activity and detect abnormal patterns in real time.

Artificial intelligence and machine learning are increasingly used to enhance detection capabilities. Atharv Pandit demonstrated a machine learning-based anomaly detection system that achieved 97.3% accuracy in identifying malicious tenant behavior[43]. Similarly, Neto proposed a federated learning model for collaborative DDoS detection, achieving 84.2% classification accuracy while maintaining data privacy across tenants [44]. Although these methods significantly improve security, they still incur substantial computational and communication overheads, reaching up to 12% in some cases [2]. This creates a critical design dilemma: balancing proactive defense with the lightweight performance requirements of IoT systems.

 doi:10.20944/preprints202512.0463.v1

4. Discussion

Despite significant progress in identifying and mitigating specific threats, current research continues to face several unresolved challenges. As highlighted in Table 2, previous methods have provided broad surveys of IoT and Cloud security [4] or general cloud vulnerabilities [3]. However, a systematic review focused specifically on the multi-tenancy challenges at their intersection has been missing. This review fills that gap by providing a mapping of tenant-specific risks (e.g., inter-tenant leakage, isolation failures) and evaluating mitigations within the specific context of IoT-cloud performance constraints.

4.1. Fragmentation of Security Architectures

This analysis reveals a clear lack of standardized and end-to-end security architectures for multi-tenant IoT and cloud ecosystems. That leads to fragmented implementations across platforms, which means each IoT or cloud platform applies its own version of a solution [4]. Resource isolation, a foundational requirement, remains insufficient. This leaves room for unauthorized data access or privilege escalation [40]. This lack of holistic frameworks is most clear in the unresolved trade-off between security robustness and system performance.

4.2. The Security-Performance Trade-Off

The most ongoing challenge revealed by this review is the unresolved conflict between establishing robust security and maintaining the lightweight performance required by IoT systems. While traditional defenses such as heavy encryption and comprehensive access controls are effective in standard server environments, they impose unacceptable costs on IoT infrastructures. Empirical evidence demonstrates that while these mechanisms can reduce successful attacks, they incur a computational and communication overhead of approximately 12% [2]. This overhead stems from the high resource demands of standard protocols. For instance, a standard AES-128 implementation requires approximately 3.6KB of Flash memory and consumes an average of 1.24μJ/bit for encryption operations[50]. Also, it acts as a critical barrier for low-latency IoT applications, forcing architects to choose between performance and protection. This creates a security-constraint feedback loop. Cost constraints force the use of limited hardware, limiting the deployment of robust security and increasing vulnerability. This cycle fundamentally limits the scalability of secure multi-tenant systems unless specialized hardware acceleration is adopted.

4.3. Lack of Dynamic Adaptability

Current security testing frameworks and static defense mechanisms often fail to accommodate the rapid flexibility and dynamic provisioning of modern cloud environments [45]. Multi-tenant workloads spin up and down into containers in seconds; however, traditional static policies cannot adapt quickly enough to this pace. This creates a vulnerability gap in which short-lived malicious containers can operate undetected until static rules are updated. This limitation underscores the urgent need for adaptive AI-driven monitoring that can detect anomalies in real-time without relying on manual policy updates

4.4. Long-Term Cryptographic Vulnerabilities

Finally, most existing multi-tenant security frameworks fail to account for the "harvest now, decrypt later" threat posed by quantum computing. Most current research relies on classical encryption standards (RSA, ECC), leaving long-lifespan IoT data vulnerable to future decryption [51]. There is a special lack of integration of lightweight Post-Quantum Cryptography (PQC) into multi-tenant architectures, creating a resilience gap for data that requires long-term confidentiality

Table 2. Comparison Between Previous Works and the Current Review.

 doi:10.20944/preprints202512.0463.v1

Aspect	Previous Works	This Review
Scope	Prior studies analyzed IoT or cloud security separately, lacking focus on shared tenancy [2] [40].	Provides an integrated review of IoT-Cloud multi-tenancy security.
Target Environment	Most works addressed single-tenant or hybrid edge models [39] [49].	Focuses on multi-tenant resource sharing and isolation.
Depth of Threat Analysis	Broader surveys covered generic cloud threats with limited tenant-specific risks [4] [3].	Categorizes tenant-level threats: data leakage, privilege escalation, and cross-VM attacks.
Mitigation Techniques	Emphasized traditional encryption and access control [42] [45].	Introduces adaptive models integrating ZTA, AI-driven detection, blockchain, and PQC.
Evaluation Focus	Prior work offered qualitative insights only [44] [43].	Provides comparative evaluation based on scalability, latency, and isolation effectiveness.
Gap Analysis	Often lacked systematic categorization [46].	Delivers structured taxonomy of unresolved issues and testable metrics.
Post-Quantum Readiness	PQC rarely examined [2] [51].	Positions PQC as a critical enabler for quantum-resilient multi-tenant communication.
Contribution Type	Mostly descriptive surveys [4] [3].	Provides comparative synthesis and a roadmap for future research directions.

5. Emerging Trends and Future Directions

To address these gaps, the literature is clearly moving toward more adaptive, intelligent, and holistic models. We identify four major trends that aim to resolve the central conflict between security and performance:

5.1. Zero Trust Architectures (ZTA)

In response to the persistent isolation gap in multi-tenant environments, Zero Trust Architecture (ZTA) is emerging as a foundational security paradigm. Rooted in the "never trust, always verify" principle, ZTA treats every entity, user, device, or workload as untrusted until verified [46]. Unlike traditional perimeter-based models that assume trust within a tenant network boundary, ZTA enforces continuous authentication, authorization, and context validation for every access request, regardless of origin or prior trust state.

In multi-tenant clouds, this model directly mitigates cross-tenant threats, lateral movement, and privilege escalation, which often stem from shared infrastructure and weak logical boundaries. Through mechanisms such as micro-segmentation, identity-centric access control, and real-time trust scoring, ZTA provides dynamic workload-level isolation rather than relying solely on static virtualization controls. Recent studies emphasize that ZTA strengthens security by unifying identity management, access policies, and telemetry across tenants. That minimizes policy drift and unauthorized data exposure [52].

However, adoption remains constrained by implementation of complexity, tool fragmentation, and performance overhead in large-scale or resource-constrained settings. Continuous verification introduces latency, and enforcing consistent policies across heterogeneous tenants and hybrid clouds remains a challenge. Therefore, current literature calls for lightweight ZTA models that integrate automated trust evaluation, adaptive policy enforcement, and privacy-preserving monitoring to maintain both scalability and compliance in multi-tenant deployments.

 doi:10.20944/preprints202512.0463.v1

5.2. AI-Driven Threat Detection

To balance the trade-off between strong security and system performance, current research is moving toward AI-enabled, adaptive threat detection rather than static, resource-intensive defenses. As demonstrated by Pandit et al., machine-learning-based intrusion systems can analyze telemetry, user behavior, and inter-tenant traffic in real time to identify anomalies indicative of malicious activity[43]. Such intelligence is essential for distinguishing legitimate workload behavior from cross-tenant threats in multi-tenant environments, where tenants share both infrastructure and control planes. For example, Saxena et al. proposed a VM threat prediction model that identifies attack vectors specific to shared virtualization layers[41]. Collectively, these advances position AI as a core enabler of intelligent, real-time security orchestration across distributed tenants.

5.3. Blockchain Integration

To address the lack of standardized trust and verifiable auditing in multi-tenant architectures, blockchain technology has gained traction as a mechanism for decentralized audit trails. Hannelore Sebestyen et al. highlighted that blockchain provides transaction records accessible to all tenants and service providers[47]. This is to ensure transparency and integrity in shared environments. This decentralized trust model mitigates insider threats and access violations.

Blockchain integration enhances accountability, supports cross-tenant compliance verification, and simplifies forensic analysis following security incidents. Its adoption is still constrained by latency, storage overhead, and scalability challenges, especially when integrated into high-throughput cloud layers. Current research is shifting toward lightweight, permissioned blockchains and hybrid on-chain/off-chain models that maintain audit integrity without forcing computational costs on tenants [47].

5.4. Lightweight Post-Quantum Cryptography (PQC)

To address the long-term cryptographic resilience gap, PQC has emerged as a forward-looking approach. With quantum computing advancing rapidly, traditional schemes such as RSA and ECC face an ultimate risk. PQC ensures the long-term confidentiality and integrity of tenant data, particularly in IoT and cloud ecosystems [2].

Recent studies emphasize the importance of lightweight PQC schemes that balance computation and bandwidth constraints typical of IoT edge deployments [51]. Additional analyses by Peng et al. further highlight the necessity of PQC to mitigate cross-tenant data breaches once classical encryption is broken. Collectively, PQC transitions multi-tenant infrastructures toward quantum-resilient architectures that sustain long-term data privacy [53].

However, the implementation of PQC introduces new risks. PQC algorithms often require larger key sizes and complex operations, which can make devices more exposed to physical side-channel attacks (SCA). Therefore, future architectures must focus on hardware-accelerated PQC to mitigate this side-channel leakage.

These trends collectively indicate a move toward intelligent, distributed, and future-proof security models. Therefore, the next generation of multi-tenant security must incorporate ZTA's trust minimization, AI awareness, blockchain's auditability, and PQC's encryption into a cohesive framework. This should balance performance and isolation across shared infrastructure. The following table formalizes this integration roadmap.

Table 3. Roadmap for Advanced Multi-Tenancy IoT-Cloud Security Mitigation.

Emerging Solution	Core Function	Primary Multi-Tenancy Benefit	Key IoT Implementation Challenge
Zero Trust Architecture (ZTA)	Continuous Authentication & Authorization	Granular Access Control, Minimized	Lack of Visibility, Overhead of Continuous

 doi:10.20944/preprints202512.0463.v1

		"Blast Radius" of Tenant Compromise	Monitoring, Legacy System Integration
Blockchain	Decentralized & Immutable Ledger	Tamper-Proof Audit Trails, Non-Repudiation for Compliance and Forensics	Scalability, High Latency/Throughput, Computational Cost of Consensus
Post-Quantum Cryptography (PQC)	Quantum-Resistant Encryption	Future-Proofing Long-Term Data Confidentiality and Integrity	Increased Memory/Processing Footprint, Resistance to Side-Channel Attacks
Adaptive AI Security	Real-Time Anomaly Detection and Intrusion Prevention	Proactive, Automated Threat Identification and Mitigation	Vulnerability to Adversarial Attacks (Poisoning, Evasion), High Computational Demand

6. Conclusion

This paper provides a review of the security and privacy challenges in multi-tenant IoT-cloud environments. The analysis has mapped the primary threats, including cross-tenant data leakage, insecure APIs, and side-channel vulnerabilities, and evaluated the current landscape of mitigation techniques from access control models to AI-driven detection.

Our central finding is the identification of a critical and unresolved conflict between security robustness and system performance. The high computational and latency overheads of many current solutions make them unsuitable for lightweight resource-constrained IoT devices. This gap highlights the insufficiency of existing approaches and the urgent need for more adaptive and lightweight security frameworks. Future research is moving towards promising solutions to address this trade-off. The integration of Zero Trust principles for continuous verification, the use of adaptive AI for real-time threat detection, the use of blockchain for decentralized, immutable audit trails, and the urgent adoption of post-quantum cryptography represent the most effective paths forward. These trends indicate a necessary paradigm shift toward intelligent, decentralized, auditable, and quantum-resistant security models capable of securing the next generation of multi-tenant IoT-cloud infrastructures. Future work must focus on unified, lightweight security architectures that address tenant isolation without compromising IoT performance.

Acknowledgments: During the preparation of this manuscript/study, the author(s) used Gemini 3 (Google) for the purposes of language editing. The authors have reviewed and edited the output and taken full responsibility for the content of this publication.

Author Contributions: Conceptualization, B.A.; methodology, B.A.; validation, B.A. and M.A.; formal analysis, B.A and M.A.; investigation, B.A and M.A.; resources, B.A.; data curation, F.T.S.; writing original draft preparation, B.A.; writing review and editing, B.A, F.T.S and M.A.; visualization, B.A.; supervision, F.T.S.; project administration, F.T.S.; funding acquisition, B.A. and F.T.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

 doi:10.20944/preprints202512.0463.v1

IoT	Internet of Things	**MQTT**	Message Queuing Telemetry Transport
PQC	Post-Quantum Cryptography	**SaaS**	Software as a Service
ZTA	Zero Trust Architectures	**IaaS**	Infrastructure as a Service
CoAP	Constrained Application Protocol	**AMQP**	Advanced Message Queuing Protocol
LPWANs	Low-Power Wide Area Networks	**ACLs**	Access Control Lists
SSL	Secure Sockets Layer	**Amazon EC2**	Amazon Elastic Compute Cloud
RBAC	Role-Based Access Control	**PaaS**	Platform as a Service
VM	virtual machine	**SDN**	Software-Defined Networking
QoS	Quality of Service	**VPN**	Virtual Private Networks
VPCs	Virtual Private Clouds	**VLAN**	Virtual Local Area Network
ABAC	Attribute-Based Access Control	**DoS**	Denial-of-Service
APIs	Application Programming Interfaces	**SCA**	side-channel attacks

References

1. Zoting, S.S., Aditi. *Multi-Tenant Data Centers Market Size, Share and Trends 2025 to 2034*. 2025; Available from: https://www.precedenceresearch.com/multi-tenant-data-centers-market.
2. Hashim, W. and N.A.-H.K. Hussein, *Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures.* SHIFRA, 2024.
3. Surianarayanan, C. and P.R. Chelliah, *Integration of the Internet of Things and Cloud: Security Challenges and Solutions – A Review.* International Journal of Cloud Applications and Computing (IJCAC), 2023. **13**(1).
4. Almutairi, M., et al., *IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions.* Electronics 2025, Vol. 14, Page 1394, 2025-03-30. **14**(7).
5. Kuchuk, H. and E. Malokhvii, *INTEGRATION OF IOT WITH CLOUD, FOG, AND EDGE COMPUTING: A REVIEW.* Advanced Information Systems, 2024/06/04. **8**(2).
6. Botta, A., et al., *Integration of Cloud computing and Internet of Things: A survey.* Future Generation Computer Systems, 2016/03/01. **56**.
7. Gubbi, J., et al., *Internet of Things (IoT): A vision, architectural elements, and future directions.* Future Generation Computer Systems, 2013/09/01. **29**(7).
8. Mrabet, H., et al., *A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis.* Sensors 2020, Vol. 20, Page 3625, 2020-06-28. **20**(13).
9. Bello, O., S. Zeadally, and M. Badra, *Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT).* Ad Hoc Networks, 2017/03/15. **57**.
10. Sharif;, B.H.W.E.M.S., *The Internet of Things Security Issues and Countermeasures in Network Layer: A Systematic Literature Review.* 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 2022.
11. Dallaf, A.A.A., *Edge Computing in IoT Networks: Enhancing Efficiency, Reducing Latency, and Improving Scalability.* International Journal of Advanced Network, Monitoring and Controls, 2025/06/13. **10**(1).
12. Sarwar, K., et al., *Efficient privacy-preserving data replication in fog-enabled IoT.* Future Generation Computer Systems, 2022/03/01. **128**.
13. Mavridis, I. and H. Karatza, *Orchestrated sandboxed containers, unikernels, and virtual machines for isolation-enhanced multitenant workloads and serverless computing in cloud.* Concurrency and Computation: Practice and Experience, 2023/05/15. **35**(11).
14. Emeakaroha, T.L.P.R.A.L.V., *A Preliminary Review of Enterprise Serverless Cloud Computing (Function-as-a-Service) Platforms.* 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2017.

 doi:10.20944/preprints202512.0463.v1

15. Jain, P., et al., *Performance Analysis of Various Server Hosting Techniques.* Procedia Computer Science, 2020/01/01. **173**.
16. Toader, E.v.E.J.G.S.E.A.B.L.V.L., *The SPEC-RG Reference Architecture for FaaS: From Microservices and Containers to Serverless Platforms.* IEEE Internet Computing, 2019. **23**(6).
17. Armoogum, S. and P. Khonje, *Healthcare Data Storage Options Using Cloud.* Internet of Things, 2021.
18. Hu, Z., et al., *FDRA: Fully Distributed Routing Architecture for Private Virtual Netwo.* Parallel Architectures, Algorithms and Programming, 2021.
19. Moharana, S.S., R.D. Ramesh, and D. Powar, *Analysis of load balancers in cloud computing.* International Journal of Computer Science and Engineering, 2013. **2**(2): p. 101-108.
20. Um, T.-W., et al., *Dynamic Resource Allocation and Scheduling for Cloud-Based Virtual Content Delivery Networks.* ETRI Journal, 2014/04/01. **36**(2).
21. Facca, T.Z.A.P.F.A.J.G.F.L.F., *FIWARE Lab: Managing Resources and Services in a Cloud Federation Supporting Future Internet Applications.* 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014.
22. Zeng, X.Z.H.-t.D.J.-q.C.Y.L.L.-j., *Ensure Data Security in Cloud Storage.* 2011 International Conference on Network Computing and Information Security, 2011.
23. Waghchaude, K., *A Review on Cloud Computing Security Issues, Applicable Solutions and Implementation.* Int. J. Sci. Res. Eng. Manag, 2024. **8**: p. 1-3.
24. Sood, S.K., *A combined approach to ensure data security in cloud computing.* Journal of Network and Computer Applications, 2012/11/01. **35**(6).
25. Pal, S., et al., *A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security.* 2011/08/20.
26. Joel Gibson, R.R., Darren Eveleigh, Qing Tan, *Benefits and challenges of three cloud computing service models.* 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012.
27. Lagana, C.D.N.A.F.G.F.A.G.A.G.D., *IoT-HC: A Novel IoT Architecture for the Hybrid Cloud.* 2019 28th International Conference on Computer Communication and Networks (ICCCN), 2019.
28. Muneer Bani Yassein, M.Q.S., Dua' Al-zoubi, *Application layer protocols for the Internet of Things: A survey.* 2016 International Conference on Engineering & MIS (ICEMIS), 2016.
29. Elmedany, S.A.W., *Security threats of application programming interface (API's) in internet of things (IoT) communications.* 2021.
30. Jannatul Ferdows, S.T.M., A.S.M. Delowar Hossain, Abdullah Al Mamun Shamim, G.M. Rasiqul Islam Rasiq, *A Comprehensive Study of IoT Application Layer Security Management.* 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020.
31. Kaur, K., et al., *Frontiers | Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies.* Frontiers in Computer Science, 2024/06/26. **6**.
32. Khan, Y., et al., *Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications.* Electronics 2023, Vol. 12, Page 88, 2022-12-26. **12**(1).
33. Banerjee, S. and S.K. Parisa, *Secure Multi-Tenancy in Cloud Computing: Challenges and Solutions.* 2025(Vol. 17 No. 17 (2025): TRIoT).
34. Sharma, R.K., *Multi-Tenant Architectures in Modern Cloud Computing: A Technical Deep Dive.* International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025/01/03. **11**(1).
35. Njeguš, A., *Intelligent Software Systems for Multi-Tenant Cloud Environments: Challenges and Solutions.* Sinteza 2025 - International Scientific Conference on Information Technology, Computer Science, and Data Science, 2025.
36. Paktiti, M. *Tenant isolation in multi-tenant systems: What you need to know*. 2025; Available from: https://workos.com/blog/tenant-isolation-in-multi-tenant-systems.
37. Factor, M., et al., *Secure Logical Isolation for Multi-tenancy in cloud storage.* IEEE Conference on Mass Storage Systems and Technologies, 2013.
38. M, T.B., *Enhancing Data Security under Multi-Tenancy within Open Stack.* International Journal of Advanced Trends in Computer Science and Engineering, 2020.

 doi:10.20944/preprints202512.0463.v1

39. Kumar, R., *Multi-Tenant SaaS Architectures: Design Principles and Security Considerations.* Journal of Software Engineering and Simulation, 2020. **Volume 6 ~ Issue 5 (2020) pp: 28-41**.
40. Panguraj, A.R.R., *Systematic Approach to Security Testing in Multi-Tenant Cloud Systems.* International Journal of Multidisciplinary Research and Growth Evaluation, 2025. **06**(1).
41. Saxena, D., et al., *An AI-Driven VM Threat Prediction Model for Multi-Risks Analysis-Based Cloud Cybersecurity.* 2023/08/18.
42. Yadav, S., *Enhancing Security in Multi-Tenant Cloud Environments: Threat Detection, Prevention, and Data Breach Mitigation.* Journal of Information Systems Engineering and Management, 2025/03/18. **10**(22s).
43. Pandit, A. and R. Pandit, *Side-Channel Attacks in Multi-Tenant Cloud Environments: Prevention & Mitigation.* International Journal of Innovations in Science, Engineering And Management, 2025/04/30.
44. Ghorbani, E.C.P.N.S.D.A.A., *Collaborative DDoS Detection in Distributed Multi-Tenant IoT using Federated Learning.* 2022 19th Annual International Conference on Privacy, Security & Trust (PST), 2022.
45. Malikireddy, S.K.R., *Securing Multi-Tenant Cloud Environments with Graph-Based Models* 2024.
46. Hariharan, R., *Zero Trust Security in Multi-Tenant Cloud Environments.* Journal of Information Systems Engineering and Management, 2025/04/30. **10**(45s).
47. Sebestyen, H., et al., *A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories.* Computers 2025, Vol. 14, Page 61, 2025-02-11. **14**(2).
48. Dauda, A., et al., *A Survey on IoT Application Architectures.* Sensors 2024, Vol. 24,, 2024-08-17. **24**(16).
49. Kyriakidou, C.D.P., A.M. Pittaras,I. Fotiou, N. Thomas, Y. Polyzos, G., *Attribute-Based Access Control Utilizing Verifiable Credentials for Multi-Tenant IoT Systems.* 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), 2024. **800**.
50. Awasthi, A. and https://independent.academia.edu/AmitAwasthi46, *Quantum-Resistant Security for IoT Systems Challenges and Implementation Strategies.* International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025/01/01.
51. Mahdi, L.H. and A. A. Abdullah, *Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography.* Engineering, Technology & Applied Science Research, 2025. **15**(2): p. 21812-21821.
52. Oladimeji, G., *A Critical Analysis of Foundations, Challenges and Directions for Zero Trust Security in Cloud Environments.* 2024/11/09.
53. Peng, Y., et al., *An Improved Co-Resident Attack Defense Strategy Based on Multi-Level Tenant Classification in Public Cloud Platforms.* Electronics 2024, Vol. 13, Page 3273, 2024-08-18. **13**(16).