Article

Cybersecurity Challenges in Cloud-Based ICT Systems

Emmanuel Idowu *

Posted Date: 21 April 2025

doi: 10.20944/preprints202504.1651.v1

Keywords: Cloud Security; Cybersecurity Challenges; ICT Systems; Zero Trust Architecture; DevSecOps; Data Breach; Encryption; Quantum Computing; Identity and Access Management; AI in Cybersecurity

Article

Cybersecurity Challenges in Cloud-Based ICT Systems

Emmanuel Idowu

B.Sc. Computer science, Ladoke Akintola University of Technology

Abstract: As cloud computing continues to transform the landscape of information and communication technologies (ICT), it also introduces a complex array of cybersecurity challenges that threaten data integrity, confidentiality, and availability. This paper provides a comprehensive analysis of the evolving threat landscape in cloud-based ICT systems, identifying critical vulnerabilities such as data breaches, misconfigurations, inadequate identity and access controls, and insider threats. Emerging risks from AI-driven attacks, quantum computing, and complex multi-cloud environments are also explored. Through detailed case studies, the paper illustrates real-world incidents and their consequences. It further evaluates contemporary strategies including Zero Trust Architecture, encryption practices, DevSecOps, and AI-powered threat detection. By aligning these solutions with international standards and organizational objectives, the paper presents actionable recommendations for enhancing cloud security resilience. The findings underscore the importance of adopting a holistic, proactive, and adaptive approach to cybersecurity in the cloud era.

Keywords: cloud security; cybersecurity challenges; ICT systems; zero trust architecture; DevSecOps; data breach; encryption; quantum computing; identity and access management; AI in cybersecurity

1. Introduction

1.1. Background of Cloud-Based ICT Systems

Cloud computing has become a foundational component of modern Information and Communication Technology (ICT) systems. It enables organizations to store, process, and manage data over the internet using virtualized resources. Cloud-based ICT systems offer flexibility, scalability, cost-efficiency, and ease of access, making them essential across various sectors such as healthcare, education, finance, and government services.

1.2. Importance of Cybersecurity in Cloud Environments

As organizations increasingly rely on cloud infrastructure, ensuring the security of data and services becomes critical. Cloud environments introduce unique security concerns due to their distributed nature, shared responsibility models, and third-party dependencies. The increasing volume and complexity of cyber threats—ranging from data breaches and DDoS attacks to advanced persistent threats (APTs)—require robust cybersecurity frameworks.

1.3. Purpose and Scope of the Study

This study aims to explore the major cybersecurity challenges that threaten cloud-based ICT systems and evaluate the effectiveness of current mitigation strategies. The paper also seeks to identify emerging threats and propose innovative approaches to strengthen cloud security.

1.4. Research Questions

1. What are the most prevalent cybersecurity threats in cloud-based ICT systems?
2. How do cloud architectures contribute to specific security vulnerabilities?
3. What are the most effective strategies and technologies currently used to address these challenges?
4. What emerging trends and threats are likely to shape the future of cloud cybersecurity?

1.5. Structure of the Paper

The paper is organized as follows:

1. **Introduction** – provides context and outlines the study's focus.
2. **Literature Review** – examines previous research on cloud cybersecurity.
3. **Methodology** – outlines research design and data collection approaches.
4. **Cybersecurity Challenges** – analyzes current threats.
5. **Emerging Threats** – explores future vulnerabilities.
6. **Strategies and Solutions** – evaluates mitigation techniques.
7. **Case Studies** – provides real-world insights.
8. **Discussion** – reflects on findings and implications.
9. **Conclusion and Recommendations** – summarizes and suggests next steps.

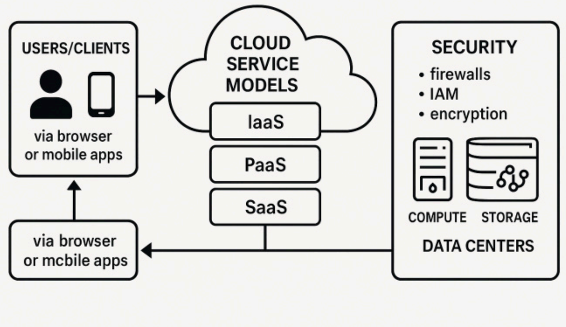
Diagram 1.1: Basic Architecture of a Cloud-Based ICT System

2. Literature Review

2.1. Overview of Cloud Computing Models (IaaS, PaaS, SaaS)

Cloud services are generally delivered through three primary models:

- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet. Users manage operating systems and applications but rely on the provider for hardware and networking infrastructure.
- **Platform as a Service (PaaS):** Offers a platform allowing customers to develop, run, and manage applications without dealing with underlying infrastructure.
- **Software as a Service (SaaS):** Delivers software applications via the internet, with the provider handling everything from infrastructure to data management.

Each model has different **security implications** and **responsibility boundaries** between provider and customer.

Table 2.1: Comparison of Cloud Service Models and Their Security Concerns.

Model	Description	Customer Responsibility	Security Concerns
IaaS	Virtual machines, storage, and networking	OS, applications, data	Misconfigurations, insecure VM instances

PaaS	App development and deployment platform	Application logic, data	Application-level vulnerabilities
SaaS	Complete software solutions	User access, data handling	Data leakage, identity theft

Diagram 1.1: Basic Architecture of a Cloud-Based ICT System.

2.2. Security Architecture in Cloud-Based ICT Systems

Cloud security architecture typically includes a layered approach involving:

- **Network Security** (e.g., firewalls, VPNs)
- **Data Security** (e.g., encryption, tokenization)
- **Identity & Access Management (IAM)**
- **Monitoring & Logging Tools**

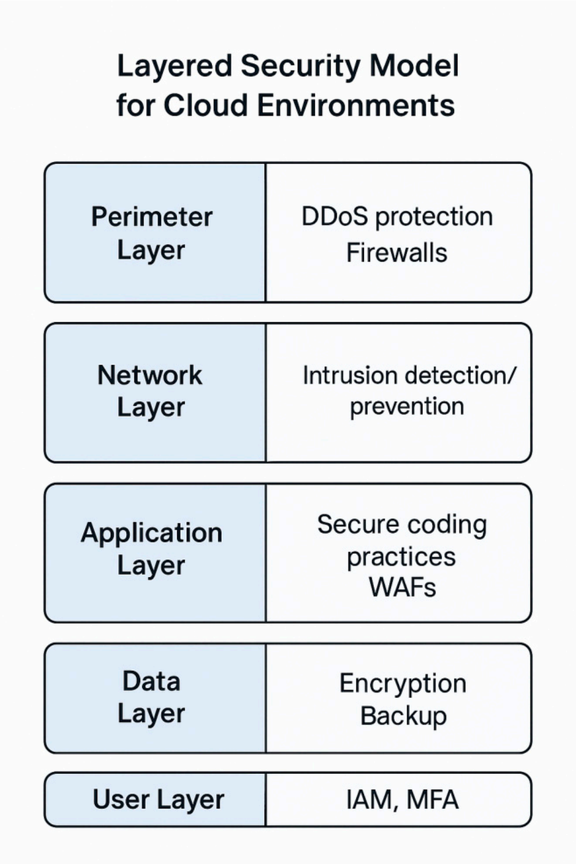

Diagram 2.2: Layered Security Model for Application Layer: Secure coding practices, WAFs

---

2.3. Previous Studies on Cloud Cybersecurity Challenges

A broad body of research identifies key risks in cloud systems.

- *Subashini and Kavitha (2011)* emphasized the lack of strong SLAs (Service-Level Agreements) as a threat to security assurance.
- *Zissis and Lekkas (2012)* explored the implications of cloud multitenancy and virtualization for data integrity and confidentiality.
- *Hashizume et al. (2013)* created a taxonomy of cloud vulnerabilities, noting that APIs and insider threats are major concerns.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2025 doi:10.20944/preprints202504.1651.v1

2.4. Gaps in Existing Research

While existing literature outlines threats and solutions, gaps remain in areas such as:

1. Security challenges in hybrid/multi-cloud environments.
2. Automation and AI-based defense mechanisms.
3. The role of regulatory compliance in cross-border cloud services.
4. Integration of IoT and edge devices into cloud ecosystems.

3. Methodology

3.1. Research Design

This study adopts a **qualitative research design** to explore cybersecurity challenges in cloud-based ICT systems. The research combines:

- **Descriptive analysis** of current threats and vulnerabilities.
- **Exploratory case studies** of cloud security incidents.
- **Comparative analysis** of security frameworks and practices.

The focus is on gathering rich, detailed data from various secondary sources such as journal articles, technical reports, white papers, and cybersecurity advisories.

3.2. Data Collection Methods

The research relies on **secondary data collection** methods, including:

1. **Literature survey** of academic databases (IEEE, ACM, ScienceDirect, Springer).
2. **Industry reports** from organizations like NIST, ENISA, CSA, and Gartner.
3. **Case studies** of past cloud-related security breaches.
4. **Framework documentation** from major providers (e.g., AWS, Azure, Google Cloud).

Table 3. 1: Summary of Methods Used in Previous Research.

Author(s)	Method Used	Focus Area	Limitation
Subashini & Kavitha (2011)	Literature Review	SaaS security issues	Lacked case analysis
Hashizume et al. (2013)	Threat Taxonomy	General cloud vulnerabilities	No specific mitigation strategies
Khan et al. (2020)	Survey + Framework Study	Multi-cloud security practices	Limited geographic scope

3.3. Data Analysis Techniques

Thematic analysis is used to identify patterns and group challenges into categories such as:

- **Infrastructure vulnerabilities**
- **Data security concerns**
- **Access management issues**
- **Emerging threat vectors**

Comparative tables and visual representations are employed to summarize findings and contrast strategies.

3.4. Limitations and Ethical Considerations

- **Limitations:**
  - No access to proprietary data from cloud service providers.
  - Limited to publicly reported incidents and frameworks.
  - Focused mainly on qualitative synthesis over empirical testing.
- **Ethical Considerations:**
  - All sources are properly cited and referenced.
  - No personal or sensitive data is collected.
  - The research adheres to academic integrity and publishing guidelines.

4. Cybersecurity Challenges in Cloud-Based ICT Systems

Cloud computing introduces a complex landscape of cybersecurity challenges that differ from traditional IT infrastructures. These challenges arise due to the dynamic, distributed, and multi-tenant nature of cloud environments.

4.1. Data Breaches and Data Loss

One of the most severe threats in cloud computing is unauthorized access to sensitive data. Data breaches can occur due to:

- Misconfigured cloud storage (e.g., publicly accessible S3 buckets)
- Lack of encryption at rest or in transit
- Vulnerabilities in shared resources

Example: The 2019 Capital One breach, where data from over 100 million users was exposed due to a firewall misconfiguration.

4.2. Insider Threats and Human Error

Employees, contractors, or cloud service provider staff may accidentally or maliciously compromise data.

- Insider threats are difficult to detect and often go unnoticed until after damage is done.
- Human error, such as weak passwords or misconfigured security groups, is a leading cause of breaches.

4.3. Insecure Interfaces and APIs

APIs are essential for cloud services but can become attack vectors if:

- Poorly documented or updated
- Lacking authentication or rate limiting
- Not protected from injection or cross-site scripting (XSS)

4.4. Account Hijacking and Identity Management Issues

If an attacker gains access to user credentials:

- They may exploit resources for malicious purposes (e.g., cryptojacking)
- Users may experience data theft, service interruptions, or reputational damage
- Poor identity and access management (IAM) controls make this risk more significant

4.5. Compliance and Regulatory Challenges

Cloud environments span multiple jurisdictions, making compliance with standards like GDPR, HIPAA, or ISO/IEC 27001 challenging.

- Data sovereignty laws may conflict across borders
- Cloud providers must provide auditability and transparency

4.6. Advanced Persistent Threats (APTs)

APTs are stealthy and sophisticated cyberattacks often linked to state actors or organized groups. In cloud systems:

- They can reside undetected for months
- Exploit cloud-native tools to avoid detection
- Target government or high-value enterprise data

Table 4. 1: Common Cybersecurity Threats in Cloud ICT Systems and Their Impact.

Threat	Description	Potential Impact	Example
Data Breach	Unauthorized data access	Financial loss, legal penalties	Capital One (2019)
Insider Threats	Malicious or negligent insiders	Data theft, system compromise	Tesla Employee Case
Insecure APIs	Poorly secured endpoints	Exploits, unauthorized access	Facebook Graph API Leak
Account Hijacking	Stolen credentials	Privilege abuse, resource misuse	GitHub Token Leaks
Regulatory Non-Compliance	Violations of data laws	Fines, sanctions, reputational damage	GDPR Violations
Advanced Persistent Threats	Covert, targeted cyberattacks	Long-term espionage, data exfiltration	SolarWinds Attack (2020)

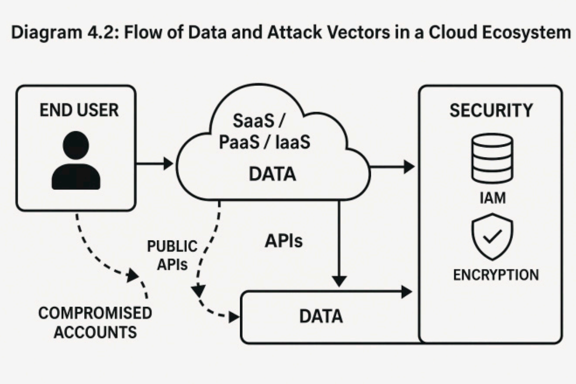

Diagram 4.2: Flow of Data and Attack Vectors in a Cloud Ecosystem

5. Emerging Threats and Vulnerabilities

As cloud computing evolves, so do the techniques and tools used by malicious actors. The complexity of hybrid and multi-cloud architectures, the rise of AI, and the proliferation of connected devices have introduced a new generation of cyber risks.

5.1. Threats from Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are now used both defensively and offensively:

- **AI-powered attacks** can adapt in real time, evade detection systems, and exploit zero-day vulnerabilities.
- Attackers may use **ML algorithms** to identify patterns in system behaviors and predict defense strategies.

Example: AI-driven spear phishing campaigns that dynamically generate personalized messages based on scraped user data.

5.2. Vulnerabilities in Multi-Cloud and Hybrid Environments

Many enterprises use **multi-cloud strategies** to avoid vendor lock-in and **hybrid models** to retain sensitive workloads on-premises.

- These systems increase complexity and reduce visibility across environments.
- Lack of centralized security governance can lead to inconsistent policies and misconfigurations.

5.3. Quantum Computing Threats (Future Risk)

Quantum computing could one day break widely used cryptographic algorithms like RSA and ECC.

- This **post-quantum vulnerability** could render current encryption schemes obsolete.
- Cloud services must prepare by adopting **quantum-safe cryptographic standards**.

5.4. Cloud Supply Chain Attacks

These occur when third-party software or services integrated into the cloud environment are compromised.

- Attackers may inject malicious code into widely used libraries or DevOps pipelines.
- Such threats are **hard to detect** and can cause **widespread damage**.

Example: The **SolarWinds breach**—an attacker inserted a backdoor into a routine software update affecting government and corporate networks worldwide.

5.5. Zero Trust Architecture (ZTA) Adoption Challenges

The **Zero Trust model** is increasingly advocated for cloud security, but it has challenges:

- Requires identity verification at every step.
- Implementation in legacy systems or multi-cloud settings can be **costly and complex**.
- Organizational resistance and lack of technical maturity slow adoption.

Table 5. 1: Summary of Emerging Threats and Their Implications.

Emerging Threat	Description	Potential Impact	Current Mitigation
AI-Driven Attacks	Adaptive, stealthy cyberattacks	Faster breaches, hard-to-detect threats	AI-enabled defense tools
Multi-Cloud Complexity	Poor integration across platforms	Misconfigurations, inconsistent policies	Unified security orchestration
Quantum Vulnerability	Breaking encryption with quantum computing	Data exposure, compromised privacy	Post-quantum cryptography
Supply Chain Infiltration	Attack via third-party tools/services	Widespread breaches	Software bill of materials (SBOM), code audits
Zero Trust Implementation	Enforcing least privilege and constant auth	Deployment and scaling challenges	ZTA toolkits, IAM refinement

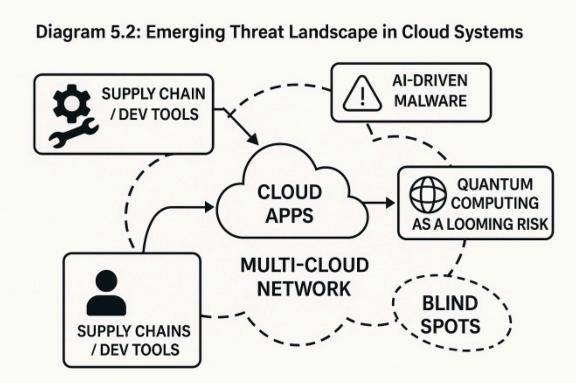
Diagram 5.2: Emerging Threat Landscape in Cloud Systems
SUPPLY CHAIN / DEV TOOLS
AI-DRIVEN MALWARE
CLOUD APPS
QUANTUM COMPUTING AS A LOOMING RISK
MULTI-CLOUD NETWORK
BLIND SPOTS
SUPPLY CHAINS / DEV TOOLS

Diagram 5.2: Emerging Threat Landscape in Cloud Systems

6. Strategies and Solutions for Mitigating Cybersecurity Challenges

Addressing the cybersecurity risks in cloud-based ICT systems requires a multi-layered, proactive approach. Solutions must cover technical safeguards, policy controls, continuous monitoring, and user behavior management.

6.1. Encryption and Data Protection Measures

Encryption is a fundamental strategy for ensuring data confidentiality:

- **At rest:** Data is encrypted in storage using AES-256 or similar algorithms.
- **In transit:** Secure protocols like HTTPS, SSL/TLS are used to protect data movement.
- **In use:** Emerging technologies like homomorphic encryption and confidential computing are gaining traction.

Key Point: Encryption must be paired with robust key management systems (KMS).

6.2. Identity and Access Management (IAM)

IAM frameworks ensure that only authorized users have access to cloud resources:

- Use of multi-factor authentication (MFA)
- Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
- Regular audits of access privileges

6.3. Zero Trust Architecture (ZTA) Implementation

ZTA is a security model based on the principle of "never trust, always verify":

- Enforces continuous authentication and authorization
- Applies least-privilege access across all network layers
- Uses micro-segmentation to isolate workloads

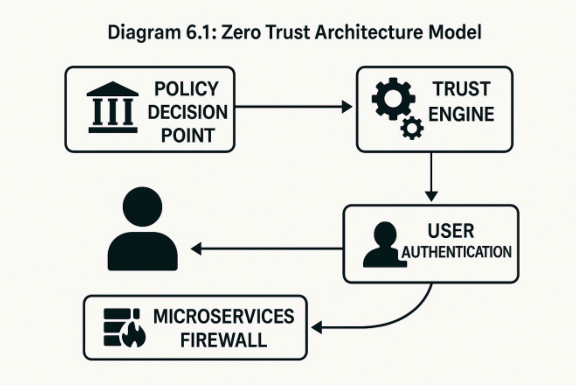

Diagram 6.1: Zero Trust Architecture Model

6.4. AI and Automation for Threat Detection

Artificial Intelligence and Machine Learning enhance real-time threat detection:

- Behavioral analytics can detect anomalies
- Automated incident response systems reduce time-to-mitigation
- Tools like SIEM (Security Information and Event Management) are evolving to include AI modules

Example Tools: CrowdStrike, IBM QRadar, Microsoft Defender for Cloud

6.5. Regulatory Compliance and Risk Management Frameworks

Adherence to global standards ensures legal compliance and enhances trust:

- **NIST Cybersecurity Framework**

- **ISO/IEC 27001**
- **GDPR, HIPAA, SOC 2** for specific sectors

Table 6. 1: Regulatory Standards and Their Focus Areas.

Framework/Standard	Scope	Industry Focus	Key Requirements
NIST CSF	Cybersecurity lifecycle	Government, general	Identify, Protect, Detect, Respond, Recover
ISO/IEC 27001	ISMS and information security	All industries	Risk assessment, continuous improvement
GDPR	Data privacy and protection	EU, global data flows	Consent, access rights, breach notification
HIPAA	Health data protection	Healthcare	Data integrity, access controls, audit trails
SOC 2	Service organization controls	Cloud, SaaS	Security, availability, confidentiality

6.6. DevSecOps Integration

DevSecOps incorporates security into every phase of the software development lifecycle:

- Automates security testing (SAST/DAST)
- Uses CI/CD pipelines to enforce compliance
- Promotes "shift-left" security practices

7. Case Studies

This section presents real-world examples to demonstrate the practical implications of cybersecurity challenges and how different strategies were employed in response.

7.1. Case Study 1: Capital One Data Breach (2019)

Overview:
Capital One, a major U.S. financial institution, suffered a breach affecting over **100 million customer records**.
Root Cause:
A misconfigured AWS web application firewall (WAF) allowed a former employee of Amazon Web Services to exploit a vulnerability and access sensitive data.
Impact:

- Exposure of customer names, addresses, social security numbers
- $80 million regulatory fine
- Reputational damage

Lessons Learned:

- Need for regular configuration audits
- Importance of IAM policies and monitoring
- Value of real-time threat detection tools

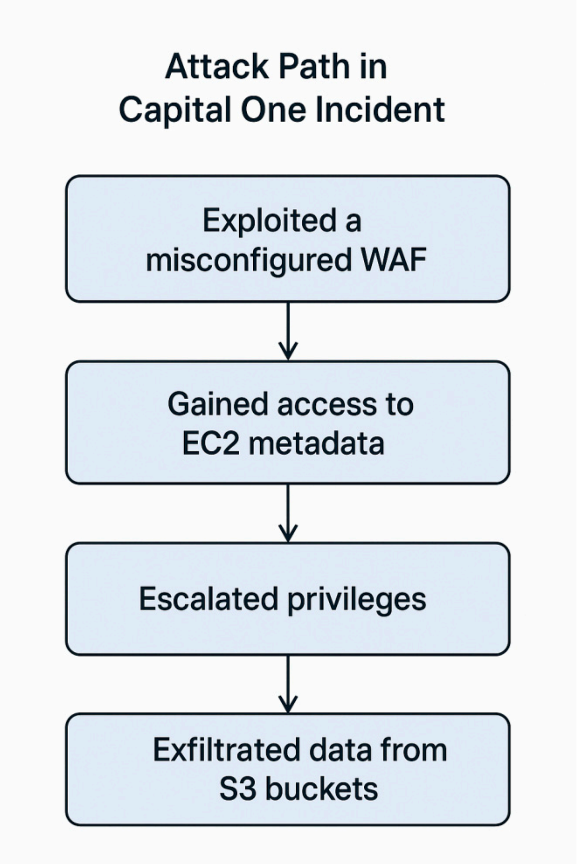
Attack Path in Capital One Incident
Exploited a misconfigured WAF
Gained access to EC2 metadata
Escalated privileges
Exfiltrated data from S3 buckets

Diagram 7.1: Attack Path in Capital One Incident

7.2. Case Study 2: SolarWinds Supply Chain Attack (2020)

Overview:
A sophisticated state-sponsored attack compromised **SolarWinds' Orion software**, affecting **over 18,000 customers**, including U.S. federal agencies.

Root Cause:
Attackers inserted a **malicious backdoor (SUNBURST)** into a routine software update.

Impact:

- Widespread data exfiltration and espionage
- Months-long undetected presence in victim networks
- Highlighted weaknesses in third-party software trust models

Lessons Learned:

- Need for **software bill of materials (SBOMs)**
- Importance of securing CI/CD pipelines

- Detection of **anomalous behavior across environments**

7.3. Case Study 3: Dropbox Credential Theft (2022)

Overview:
Dropbox employees fell victim to a **phishing campaign** that impersonated CircleCI and led to credential theft.
Root Cause:

- Compromised GitHub tokens due to social engineering
- Lack of strict MFA enforcement at the time

Impact:

- Exposure of developer credentials
- Temporary disruption to internal projects

Lessons Learned:

- Importance of **employee training**
- Enforcing **token scope and expiry**
- Deployment of **MFA for all access points**

Table 7. 1: Comparative Summary of Cloud Security Incidents.

Case Study	Breach Vector	Data Affected	Key Weakness	Mitigation Action
Capital One (2019)	Misconfigured firewall	Personal and financial records	IAM mismanagement, misconfig	AWS GuardDuty, Config audits
SolarWinds (2020)	Compromised update	Network-wide system access	Supply chain, software integrity	SBOMs, ZTA, threat hunting
Dropbox (2022)	Phishing + GitHub	Developer access credentials	Human error, weak MFA	Training, OAuth token policies

8. Discussion

This section provides a critical analysis of the challenges and strategies previously outlined, reflecting on the evolving nature of cloud cybersecurity, the gaps in current practices, and the need for proactive, scalable defense mechanisms.

8.1. Interplay Between Cloud Innovation and Security Risks

Cloud computing offers unparalleled scalability, flexibility, and cost-efficiency. However, the rapid adoption of cloud services often outpaces the implementation of robust cybersecurity practices. Key observations:

1. **Innovation vs. Security Lag** – Businesses prioritize rapid deployment over secure architecture.
2. **Complexity of Cloud Environments** – Multi-cloud and hybrid setups introduce overlapping controls and visibility challenges.

Insight: Organizations must integrate security early in the cloud adoption lifecycle rather than treat it as an afterthought.

8.2. Common Gaps in Security Implementation

Despite available tools and frameworks, several common gaps persist:

- **Inconsistent access controls** across platforms
- **Weak cloud governance policies**
- **Neglected monitoring and logging practices**
- **Over-reliance on cloud providers** for security

These gaps often stem from:

- Lack of expertise
- Budget constraints
- Misconceptions about shared responsibility models

8.3. Shared Responsibility Model Misunderstanding

Many breaches occur due to confusion over what the **cloud provider** secures vs. what the **customer** must secure.

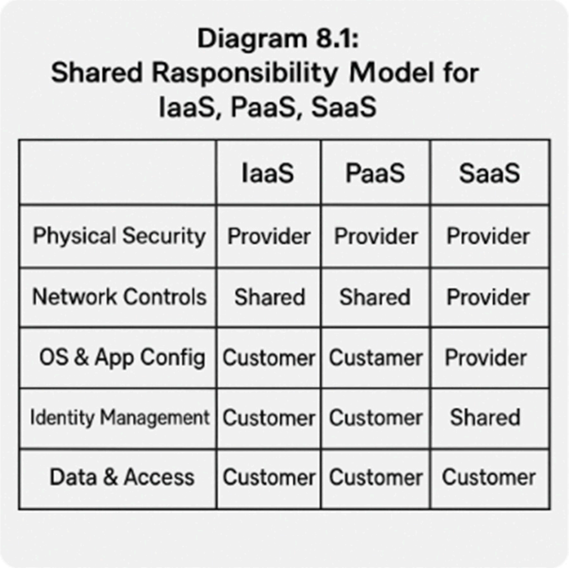

Diagram 8.1:
Shared Rasponsibility Model for IaaS, PaaS, SaaS

	IaaS	PaaS	SaaS
Physical Security	Provider	Provider	Provider
Network Controls	Shared	Shared	Provider
OS & App Config	Customer	Custamer	Provider
Identity Management	Customer	Customer	Shared
Data & Access	Customer	Customer	Customer

Diagram 8.1: Shared Responsibility Model for IaaS, PaaS, SaaS

8.4. Importance of Culture and Training

doi:10.20944/preprints202504.1651.v1

Even the best technology cannot prevent breaches caused by **human error** or **insider threats**. A culture of security awareness is essential.

Key steps include:

1. **Regular training** on phishing and social engineering
2. **Simulated attack exercises**
3. **Clear incident response procedures**

Quote: "Cybersecurity is as much about people and processes as it is about technology."

8.5. Strategic Alignment of Security with Business Goals

For long-term sustainability, cloud security efforts must align with organizational goals:

- ROI must be clear for security investments
- Compliance must be integrated with operations
- Risk appetite should guide security architecture

Table 8. 1: Security Strategy Alignment with Business Objectives.

Business Objective	Corresponding Security Strategy
Operational Continuity	Incident response, data backup & recovery
Customer Trust	Data protection, transparency, compliance
Innovation Speed	DevSecOps, secure CI/CD pipelines
Cost Optimization	Cloud-native security tools, automation

9. Conclusion and Recommendations

9.1. Conclusion

Cloud-based ICT systems have revolutionized digital infrastructure by enabling agility, scalability, and cost efficiency. However, they also introduce a new and complex threat landscape. This paper has explored the multifaceted cybersecurity challenges inherent in cloud environments, including data breaches, access management issues, insider threats, and emerging risks like AI-driven attacks and quantum vulnerabilities.

Key takeaways:

1. **Security is a shared responsibility** between cloud service providers and users.

2. **Human factors**, such as misconfigurations and lack of training, are leading contributors to cloud security incidents.
3. **Emerging technologies** both threaten and enhance cloud security; organizations must adapt quickly.
4. Proactive strategies such as **Zero Trust Architecture**, **AI-powered threat detection**, and **DevSecOps** are essential for future-proofing cloud ecosystems.

9.2. Recommendations

Based on the findings and case studies, the following recommendations are proposed:

1. Implement Zero Trust Architecture (ZTA)

- Enforce identity verification for all users and devices
- Apply least-privilege principles
- Segment network resources using microservices and access control policies

2. Adopt AI and Automation

- Integrate AI-powered Security Information and Event Management (SIEM)
- Use behavioral analytics for real-time threat detection
- Automate incident response to reduce mitigation times

3. Regularly Audit and Test Security Configurations

- Perform penetration testing, vulnerability scanning, and red team exercises
- Monitor for misconfigurations and enforce configuration baselines

4. Enhance Employee Training and Awareness

- Train staff on phishing, credential hygiene, and social engineering
- Conduct regular simulated attack drills
- Promote a culture of cybersecurity ownership

5. Prepare for Post-Quantum Threats

- Begin transitioning to **quantum-resistant encryption** standards
- Stay updated with NIST recommendations and cryptographic best practices

6. Establish Strong Governance and Compliance Practices

- Align cloud operations with NIST, ISO/IEC 27001, and sector-specific standards
- Maintain an updated **software bill of materials (SBOM)**
- Implement clear data classification and handling policies

9.3. Future Work

Future research should explore:

- AI-driven defense systems that autonomously adapt to advanced persistent threats (APTs)
- Standardized frameworks for **cloud supply chain risk management**
- The development of universal **quantum-safe cryptographic libraries**
- Ethical and privacy implications of advanced cloud surveillance tools

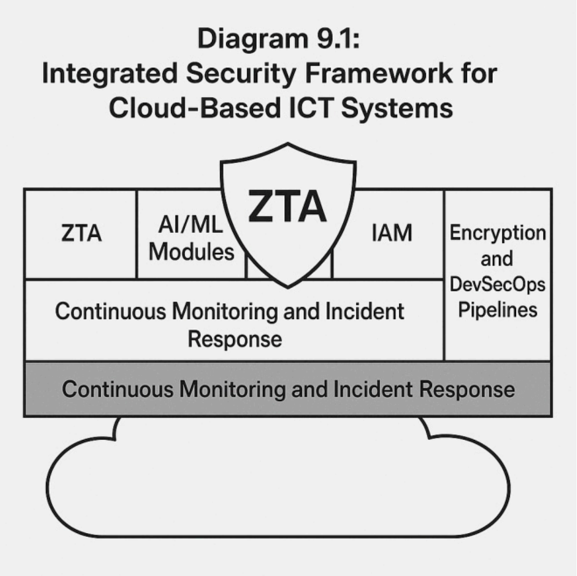
Diagram 9.1:
Integrated Security Framework for
Cloud-Based ICT Systems
ZTA
ZTA
AI/ML Modules
IAM
Encryption and DevSecOps Pipelines
Continuous Monitoring and Incident Response
Continuous Monitoring and Incident Response

Diagram 9.1: Integrated Security Framework for Cloud-Based ICT Systems

References

1. Alasmary, Waleed, Fahad Alhaidari, Rawan Alhaidari, and Tareq Alhaidari. 2022. "Cloud Computing Security Challenges and Solutions: A Systematic Review." *Computers, Materials & Continua* 70 (1): 1809–1826. https://doi.org/10.32604/cmc.2022.020562.
2. Chouhan, Manisha, and Vikram Sharma. 2021. "Enhancing Cybersecurity in Cloud Computing Using Artificial Intelligence Techniques." *Journal of King Saud University – Computer and Information Sciences.* https://doi.org/10.1016/j.jksuci.2021.10.012.
3. Fernandes, D. A. B., L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio. 2014. "Security Issues in Cloud Environments: A Survey." *International Journal of Information Security* 13 (2): 113–170. https://doi.org/10.1007/s10207-013-0208-7.

doi:10.20944/preprints202504.1651.v1

4. Hashem, Ibrahim A. T., Ibrar Yaqoob, Nor Badrul Anuar, Saleh Mokhtar, Abdullah Gani, and Samee U. Khan. 2015. “The Rise of ‘Big Data’ on Cloud Computing: Review and Open Research Issues.” *Information Systems* 47: 98–115. https://doi.org/10.1016/j.is.2014.07.006.
5. KPMG. 2021. “Cybersecurity Considerations 2021: Cloud Security.” https://home.kpmg/xx/en/home/insights/2021/06/cloud-security-cyber-considerations.html.
6. Microsoft. 2020. “The Shared Responsibility Model in Cloud Computing.” *Microsoft Azure.* https://azure.microsoft.com/en-us/resources/shared-responsibility-model/.
7. Mollah, Md Barkatullah, Md Abul Kalam Azad, and Athanasios V. Vasilakos. 2017. “Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead.” *Journal of Network and Computer Applications* 84: 38–54. https://doi.org/10.1016/j.jnca.2017.02.001.
8. National Institute of Standards and Technology (NIST). 2020. *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. https://www.nist.gov/cyberframework.
9. Shaghaghi, Abdollah, and Christopher Fidge. 2021. “Preventing Insider Threats in Cloud Computing Systems: A Review and Research Agenda.” *ACM Computing Surveys* 54 (3): 1–36. https://doi.org/10.1145/3439812.
10. Sood, Aditya K., and Richard J. Enbody. 2013. “Targeted Cyberattacks: A Superset of Advanced Persistent Threats.” *IEEE Security & Privacy* 11 (1): 54–61. https://doi.org/10.1109/MSP.2012.90.
11. Al Wahid, Sk Ayub, Nur Mohammad, Rakibul Islam, Md Habibullah Faisal, and Md Sohel Rana. "Evaluation of Information Technology Implementation for Business Goal Improvement under Process Functionality in Economic Development." Journal of Data Analysis and Information Processing 12, no. 2 (2024): 304-317.
12. Ahmed, Khandakar Rabbi, Rakibul Islam, Md Ariful Alam, Mir Araf Hossain Rivin, Mahfuz Alam, and Md Shafiqur Rahman. "A Management Information Systems Framework for Sustainable Cloud-Based Smart E-Healthcare Research Information Systems in Bangladesh." In 2024 Asian Conference on Intelligent Technologies (ACOIT), pp. 1-5. IEEE, 2024.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.