

A Study of Cloud Security: Threats, Controls & Future Directions

Shubham Rajesh Kurkute, Prof. Jadhav Ankita Ganpat, Dr. Pawar Santosh Barku
Vidya Niketan Institute of Management and Computer Applications, Bota

Abstract: *Almost every organization today, from small start-ups to banks and hospitals, keeps some part of its work in the cloud. It is cheap, flexible and easy to scale, but it also means that data and applications now live on shared systems that are reachable from anywhere on the internet. This paper looks at what that means for security. We explain the basic ideas behind cloud security, including the shared responsibility model, go through the most common threats such as data breaches, misconfiguration and account hijacking, and describe the controls that are used to defend cloud systems. We also discuss the problems that are still unsolved, like compliance, limited visibility and multi-cloud complexity, and finish with future directions: Zero Trust, confidential computing, AI-based threat detection and post-quantum cryptography.*

Keywords: Cloud Computing, Cloud Security, Data Privacy, Identity and Access Management, Zero Trust, Encryption, Confidential Computing, DevSecOps

I. INTRODUCTION

Cloud computing simply means using someone else's computers over the internet instead of buying and running your own. Servers, storage, databases and software are rented as needed and paid for by use. NIST describes it as a model that gives convenient, on-demand access to a shared pool of computing resources that can be set up quickly with very little management effort (Mell & Grance, 2011). Because of this, schools, companies and government departments have moved a large part of their work to the cloud.

The catch is that the things that make the cloud useful are the same things that make it risky. The infrastructure is shared with other customers, it can be reached from anywhere, and it is run by a third party. Our data is no longer sitting in a locked server room that we control, and we often cannot see what is happening underneath. Cloud security is the collection of policies, tools and habits that are used to keep cloud data, applications and infrastructure safe.

In this paper we review the basics of cloud security, the main threats, the defences that organizations use, the challenges that remain, and the trends that are likely to shape the field in the coming years.

II. KEY FEATURES OF CLOUD COMPUTING AND CLOUD SECURITY

2.1 Cloud Service Models

Cloud services are usually offered in three forms. How much security work falls on the customer depends on which one is used (Mell & Grance, 2011).

- Infrastructure as a Service (IaaS): The provider gives you virtual machines, storage and networks. You look after the operating system, the applications and the data.
- Platform as a Service (PaaS): The provider gives you a ready environment for building and running applications. You look after your application and its data.
- Software as a Service (SaaS): You simply use finished software through a browser, such as email or a CRM. Your main job is to control who can log in and how data is used.



2.2 Cloud Deployment Models

- Public cloud: owned by a provider and shared by many customers.
- Private cloud: built for one organization only.
- Hybrid cloud: a mix of public and private clouds that work together.
- Community cloud: shared by a group of organizations with similar needs, such as the same compliance rules.

2.3 The Shared Responsibility Model

One idea sits at the centre of cloud security: the provider and the customer share the job of protecting the system. A simple way to think about it is renting a flat. The landlord looks after the building, the main gate and the wiring, but you are still the one who must lock your own door. In the same way, the provider secures the cloud itself, meaning the data centres, hardware and core networking, while the customer secures what they put in it, meaning their data, user accounts, settings and applications. A lot of cloud incidents happen because customers assume the provider takes care of everything.

Layer	IaaS	PaaS	SaaS
Physical data centre and hardware	Provider	Provider	Provider
Virtualization and network	Provider	Provider	Provider
Operating system	Customer	Provider	Provider
Application	Customer	Customer	Provider
Identity and access management	Customer	Customer	Customer
Data and its classification	Customer	Customer	Customer

2.4 Core Security Objectives

Cloud security tries to protect the three goals known as the CIA triad:

- Confidentiality: only the right people can see the data. This is mostly done with encryption and access control.
- Integrity: data is not changed without permission. Hashing, digital signatures and audit logs help here.
- Availability: services keep working even when something fails or is attacked. Backups, redundancy and DDoS protection support this.

Besides these three, accountability, authentication, non-repudiation and privacy are also treated as important goals in cloud environments (Subashini & Kavitha, 2011).

III. MAJOR THREATS TO CLOUD SECURITY

Research papers and industry reports keep pointing to the same group of threats (Ali et al., 2015; Cloud Security Alliance, 2024). The most important ones are described below.

3.1 Data Breaches and Data Loss

This is the biggest worry for most organizations. Personal records, financial details or business secrets can be exposed because of weak passwords, unpatched software, poorly protected storage or a dishonest insider. Data can also simply be lost, for example through accidental deletion, a provider failure, or ransomware when no proper backup exists.

3.2 Misconfiguration

Cloud resources are very easy to create, and just as easy to expose by mistake. A storage bucket left open to the public, a firewall rule that is too loose, a default password that was never changed, or logging that was switched off are all common examples. Misconfiguration is widely seen as one of the leading causes of cloud incidents, and it is a human error rather than a flaw in the technology.



3.3 Insecure Interfaces and APIs

Cloud services are managed and used through APIs. If an API has weak authentication, does not limit requests, or returns more data than it should, attackers can use it to pull out or change data on a large scale.

3.4 Account Hijacking

Phishing emails, credential stuffing and leaked access keys let attackers log in as real users. Cloud administrators can control a whole environment, so taking over a single privileged account can be disastrous.

3.5 Insider Threats

Employees, contractors or partners already have legitimate access, and they may misuse it on purpose or by accident. These cases are hard to catch because the activity often looks like normal work.

3.6 Denial of Service (DoS/DDoS) Attacks

In these attacks, a huge amount of traffic is sent to a cloud service until real users can no longer reach it. The elasticity of the cloud helps absorb some of this traffic, but it can also leave the victim with a surprisingly large bill.

3.7 Multi-Tenancy and Side-Channel Attacks

In a shared cloud, virtual machines belonging to different customers can run on the same physical machine. Ristenpart et al. (2009) showed that an attacker can place their virtual machine next to a target and then use side channels to pick up information, which proves that the separation between customers is not perfect.

3.8 Supply Chain and Third-Party Risks

Modern systems depend on many outside pieces: software libraries, container images, SaaS tools and managed service providers. A weakness in any one of them can put the whole environment at risk.

Threat	Typical Cause	Main Impact
Data breach	Weak access control, unencrypted data	Loss of confidentiality
Misconfiguration	Human error, lack of automation	Unintended exposure
Insecure APIs	Poor authentication and validation	Data theft, service abuse
Account hijacking	Phishing, leaked keys	Full environment takeover
Insider threat	Malicious or careless users	Data leakage, sabotage
DDoS	Traffic flooding	Loss of availability
Side-channel attack	Shared hardware	Cross-tenant information leakage

IV. SECURITY CONTROLS AND DEFENSE MECHANISMS

4.1 Identity and Access Management (IAM)

IAM decides who can get to which resource. Good practice includes giving people only the access they really need (least privilege), using role-based access control, turning on multi-factor authentication, reviewing permissions regularly, and avoiding long-lived access keys. Many experts call IAM the foundation of cloud security, because in the cloud a person's identity has largely taken the place of the network boundary.

4.2 Data Encryption and Key Management

Data should be encrypted while it is stored, while it travels over the network and, where possible, while it is being used. In practice this means AES for stored data and TLS for communication. Looking after the keys is just as important: they should be rotated regularly, kept in a dedicated key management service or hardware security module, and preferably controlled by the customer. A more advanced idea is homomorphic encryption, which lets a system compute



on encrypted data without ever decrypting it (Gentry, 2009). It is still too slow for everyday use, but it is a promising direction.

4.3 Network and Perimeter Security

Virtual private clouds, network segmentation, security groups, firewalls, web application firewalls and intrusion detection systems all help to limit what an attacker can reach and make it harder for them to move from one system to another.

4.4 Monitoring, Logging and Incident Response

Watching logs and network activity all the time makes it possible to notice suspicious behaviour early. SIEM tools collect and connect events from different sources, and a ready incident response plan means the team knows exactly what to do to contain an attack, recover, and learn from it.

4.5 Cloud Security Posture Management (CSPM)

CSPM tools keep scanning cloud accounts for wrong settings and rule violations, and some can fix them automatically. They are a direct answer to the misconfiguration problem discussed in Section 3.2.

4.6 Secure Development and DevSecOps

Instead of checking security at the very end, DevSecOps builds it into the whole software pipeline through code analysis, dependency and container scanning, and checks on infrastructure-as-code files. Fixing a problem early is much cheaper and safer than fixing it after release.

4.7 Backup, Redundancy and Disaster Recovery

Regular, tested and separately stored backups, along with copies of services in more than one region, protect availability and make it possible to recover from ransomware or an outage.

V. CHALLENGES AND LIMITATIONS

5.1 Data Privacy and Regulatory Compliance

Cloud data can be stored in several countries at once, and their laws do not always agree. Rules such as the European Union's GDPR and India's Digital Personal Data Protection Act, 2023 place strict duties on how personal data is collected, stored and moved. Proving compliance on a shared platform is not easy.

5.2 Lack of Visibility and Control

Customers cannot look inside the provider's physical systems or hypervisor. Shadow IT, where staff use cloud tools without approval, makes the picture even less clear.

5.3 Multi-Cloud and Hybrid Complexity

Using more than one provider means learning and managing different tools, policies and APIs. When settings are not consistent across platforms, gaps appear, and attackers are quick to find them.

5.4 Vendor Lock-in and Trust in Providers

Relying on a single provider's security features makes it hard to switch and concentrates the risk in one place. Customers also have to trust what the provider says, which can only be checked through audits and certifications.



5.5 Shortage of Skilled Professionals

Cloud technology changes fast, and many organizations do not have enough people who understand both cloud architecture and security. This lack of skills is one of the reasons for the misconfigurations mentioned earlier.

5.6 Performance and Cost Trade-offs

Strong security is not free. Encryption, deep traffic inspection and detailed logging add delay and cost, so organizations must find a balance between protection and usability.

VI. FUTURE TRENDS IN CLOUD SECURITY

6.1 Zero Trust Architecture

Zero Trust works on the idea of "never trust, always verify." No user, device or network location is trusted automatically. Every request is checked and re-checked using identity, device health and context (Rose et al., 2020). It is quickly becoming the preferred security model for cloud and hybrid setups.

6.2 AI and Machine Learning for Threat Detection

Machine learning can go through huge amounts of logs and network data to spot unusual behaviour and predict attacks much faster than people can. Automated responses can isolate a compromised resource within seconds. However, attackers are also starting to use AI, and the ML systems themselves need protection from being tricked.

6.3 Confidential Computing

Confidential computing uses special hardware, called trusted execution environments, to protect data even while it is being processed. This fills the gap left by encryption at rest and in transit, and it is especially useful for sensitive work in healthcare and finance.

6.4 Privacy-Preserving Techniques and Federated Learning

Federated learning trains a model across many data sources without moving the raw data to one central place (McMahan et al., 2017). Along with homomorphic encryption and differential privacy, it allows useful analysis in the cloud while keeping personal data private.

6.5 Post-Quantum Cryptography

Future quantum computers may be able to break public-key systems like RSA and elliptic-curve cryptography that we use today. Because of this, work on quantum-resistant algorithms is becoming a priority for protecting cloud data over the long term.

6.6 Security Automation and Policy as Code

When security rules are written as code and enforced automatically, there is less room for human error, and the same protection can be applied across many clouds in the same way.

6.7 Blockchain for Integrity and Auditability

Blockchain-based records could give tamper-resistant audit trails for logs and access history. Scalability and cost are still open questions, so more research is needed.

VII. CONCLUSION

The cloud brings real benefits, but it also needs careful handling. Data breaches, misconfiguration, weak APIs and stolen accounts show that technology alone is not enough. Organizations need to understand the shared responsibility model, manage identities well, encrypt their data, monitor continuously, and train their people. Compliance rules and



the growth of multi-cloud setups make the job harder still. Looking ahead, Zero Trust, confidential computing, AI-driven defence, privacy-preserving computation and post-quantum cryptography are likely to shape the next generation of secure cloud systems. If researchers, providers and organizations work together, the cloud can stay both powerful and trustworthy.

REFERENCES

1. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357-383.
2. Armbrust, M., Fox, A., Griffith, R., et al. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
3. Cloud Security Alliance (2024). Top Threats to Cloud Computing. Cloud Security Alliance.
4. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, 169-178.
5. McMahan, B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*.
6. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (SP 800-145). National Institute of Standards and Technology.
7. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 199-212.
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology.
9. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.
10. European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).
11. Government of India (2023). The Digital Personal Data Protection Act, 2023.

