IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

A Survey on Cloud Computing Security Issues and Cryptographic Techniques

Praphulla Jitendra Chavhan, Mehul Ashok Pawar and Mrs. S P Borse
Department of Computer Science
K.R.T. Arts, B.H. Commerce and A.M. Science College Nashik
prafullchavan4948@gmail.com, mehulpawar890@gmail.com

Abstract: *Cloud computing has emerged as one of the most important technologies in the modern computing environment. It provides scalable, flexible, and cost-effective computing services through the internet. Organizations use cloud platforms for data storage, application hosting, communication, and resource management. Although cloud computing offers many advantages, security and privacy concerns remain major challenges. Data breaches, unauthorized access, cyberattacks, and insecure APIs create significant risks in cloud environments. To overcome these challenges, various cryptographic techniques such as encryption, authentication, hashing, and digital signatures are used.*

This research paper presents a detailed survey on cloud computing security issues and cryptographic techniques. The paper discusses cloud architecture, deployment models, service models, virtualization, cloud security threats, and cryptographic mechanisms used to protect cloud systems. Furthermore, the study explains modern technologies such as edge computing, artificial intelligence, and green cloud computing. The objective of this paper is to provide a comprehensive understanding of cloud computing security and modern data protection approaches.

Keywords: Cloud Computing, Cloud Security, Cryptography, Encryption, SaaS, PaaS, IaaS, Virtualization, Authentication

I. INTRODUCTION

Cloud computing is one of the most important technologies in the field of information technology. It provides computing services such as storage, servers, databases, networking, software, and applications through the internet. Instead of maintaining expensive physical infrastructure, organizations can access computing resources on demand from cloud service providers. Cloud computing enables users to store, manage, and process data remotely while reducing operational and maintenance costs.

The concept of cloud computing evolved from distributed computing, grid computing, utility computing, and virtualization technologies. In traditional computing systems, organizations were required to maintain physical hardware, software installations, and dedicated servers for data storage and application execution. These systems required high investment, regular maintenance, and skilled professionals. Cloud computing solved these problems by introducing virtualized and shared resources accessible through the internet.

Cloud computing provides several important features such as scalability, flexibility, resource sharing, rapid elasticity, and high availability. Organizations can increase or decrease computing resources according to their requirements. This flexibility helps businesses improve performance while minimizing infrastructure costs. Cloud platforms also provide automatic software updates, backup systems, and disaster recovery mechanisms that improve reliability and business continuity.

Cloud computing services are generally categorized into three major service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS allows users to access software applications through the internet, PaaS provides development platforms for building applications, and IaaS offers

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

virtualized hardware resources such as servers and storage systems. Cloud computing also includes different deployment models such as public cloud, private cloud, hybrid cloud, and community cloud.

Today, cloud computing is widely used in healthcare, education, banking, scientific research, business management, and social networking applications. Popular companies such as Amazon, Google, Microsoft, IBM, and Oracle provide cloud-based services to millions of users worldwide. Applications like Google Drive, Microsoft 365, Dropbox, and Amazon Web Services (AWS) are examples of cloud computing platforms used for data storage, collaboration, and application hosting.

Although cloud computing offers many advantages, security and privacy concerns remain major challenges. Since sensitive data is stored on remote cloud servers, organizations face risks such as unauthorized access, data breaches, cyberattacks, insider threats, insecure APIs, and data loss. These security issues may affect user privacy, business operations, and organizational reputation.

Therefore, cloud security has become an important research area in modern computing systems.

To protect cloud environments, organizations use various cryptographic techniques and security mechanisms such as encryption, authentication, hashing, digital signatures, and access control systems. Encryption techniques such as AES and RSA help secure cloud data during storage and communication. Authentication mechanisms including passwords, multi-factor authentication, and biometric systems are used to verify user identity and prevent unauthorized access.

This research paper presents a detailed survey on cloud computing security issues and cryptographic techniques. The paper discusses cloud architecture, service models, deployment models, virtualization, security challenges, and modern cryptographic approaches used in cloud systems. Furthermore, the study explores recent trends such as edge computing, artificial intelligence in cloud systems, green cloud computing, and blockchain-based security mechanisms. The objective of this paper is to provide a comprehensive understanding of cloud computing technologies and the security techniques used to protect cloud environments.

II. SERVICE & DEPLOYMENT MODELS

CLOUD SERVICE MODELS

Cloud computing provides different types of services to users through the internet. These services are categorized into three major service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Each service model provides different levels of control, flexibility, and resource management.

A. Software as a Service (SaaS)

Software as a Service (SaaS) is a cloud service model in which software applications are delivered through the internet. Users can access applications using web browsers without installing or maintaining software on local systems. The cloud provider manages servers, storage, updates, and maintenance.

SaaS is widely used because it reduces hardware requirements and simplifies software management. Users can access applications from anywhere using internet-enabled devices.

Features of SaaS

- Easy accessibility through internet
- No software installation required
- Automatic updates and maintenance
- Subscription-based payment model
- Supports remote collaboration

Advantages of SaaS

- Reduced software cost

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

- Easy maintenance
- High scalability
- Accessible from multiple devices

Disadvantages of SaaS
- Internet dependency
- Limited customization
- Data security concerns

Examples of SaaS
- Google Workspace
- Microsoft 365
- Salesforce
- Dropbox
- Zoom

B. Platform as a Service (PaaS)

Platform as a Service (PaaS) provides a development platform where developers can build, test, and deploy applications without managing hardware infrastructure. PaaS offers development tools, databases, middleware, and runtime environments.

Developers use PaaS platforms to simplify software development and improve productivity. The cloud provider manages servers, networking, and operating systems while developers focus on application development.

Features of PaaS
- Development environment for applications
- Database integration
- Middleware support
- Automatic scaling
- Application hosting

Advantages of PaaS
- Faster application development
- Reduced infrastructure management
- Improved collaboration
- Cost-effective development environment

Disadvantages of PaaS
- Vendor dependency
- Limited control over infrastructure
- Security concerns

Examples of PaaS
- Google App Engine
- Microsoft Azure
- Heroku
- Red Hat OpenShift

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

• AWS Elastic Beanstalk

C. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) provides virtualized computing resources such as servers, storage, networking, and virtual machines through the internet. Users can manage operating systems, applications, and storage while the cloud provider manages physical infrastructure.

IaaS offers high flexibility and scalability for organizations that require customized computing environments.

Features of IaaS

• Virtual machines and servers
• Scalable infrastructure
• Pay-as-you-use model
• Flexible resource management
• High storage capacity

Advantages of IaaS

• Reduced hardware investment
• Better scalability
• Flexible resource allocation
• Disaster recovery support

Disadvantages of IaaS

• Complex management
• Security risks
• Requires technical expertise

Examples of IaaS

• Amazon EC2
• Google Compute Engine
• Microsoft Azure Virtual Machines
• IBM Cloud
• Rackspace

III. CLOUD DEPLOYMENT MODELS

Cloud deployment models define how cloud infrastructure is organized, managed, and accessed by users. Different deployment models provide different levels of security, accessibility, and control.

A. Public Cloud

Public cloud infrastructure is owned and managed by third-party cloud service providers. Services are delivered through the public internet and shared among multiple users or organizations.

Public clouds are widely used because they are cost-effective and highly scalable.

Features of Public Cloud

• Shared infrastructure
• Internet-based access
• High scalability
• Pay-as-you-use pricing

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Advantages of Public Cloud
- Low infrastructure cost
- Easy deployment
- High availability
- No maintenance responsibility

Disadvantages of Public Cloud
- Security concerns
- Limited customization
- Shared resources

Examples
- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure

B. Private Cloud

Private cloud infrastructure is dedicated to a single organization. It provides better control, security, and customization compared to public cloud systems.

Private clouds are commonly used by government organizations, banks, and healthcare institutions where data privacy is critical.

Features of Private Cloud
- Dedicated infrastructure
- Better security
- Improved customization
- Enhanced privacy

Advantages of Private Cloud
- High security
- Better performance
- Full control over resources
- Improved compliance support

Disadvantages of Private Cloud
- High setup cost
- Requires maintenance
- Limited scalability compared to public cloud

Examples
- VMware Private Cloud
- OpenStack
- Microsoft Private Azure

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

C. Hybrid Cloud

Hybrid cloud combines public cloud and private cloud environments. Organizations can store sensitive information in private clouds while using public clouds for scalable resources.
Hybrid cloud provides flexibility and efficient resource management.

Features of Hybrid Cloud

- Combination of public and private clouds
- Better resource utilization
- Flexible workload management
- Improved scalability

Advantages of Hybrid Cloud

- Cost efficiency
- Better flexibility
- Improved disaster recovery
- Enhanced scalability

Disadvantages of Hybrid Cloud

- Complex infrastructure management
- Security integration challenges
- Higher implementation complexity

Applications

- Large enterprises
- Banking systems
- E-commerce platforms

D. Community Cloud

Community cloud infrastructure is shared among multiple organizations with common objectives, security requirements, or policies.
This deployment model is useful for organizations working in similar domains.

Features of Community Cloud

- Shared infrastructure
- Collaborative environment
- Common security policies

Advantages of Community Cloud

- Cost sharing
- Better collaboration
- Improved security compliance

Disadvantages of Community Cloud

- Limited scalability
- Shared security risks
- Management complexity

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Applications
- Government organizations
- Research institutions
- Healthcare systems

IV. VIRTUALIZATION

Virtualization is one of the core technologies behind cloud computing. It allows multiple virtual systems to run on a single physical machine by sharing hardware resources efficiently. Virtualization helps cloud providers maximize resource utilization, reduce hardware costs, improve scalability, and provide flexible computing services.

In traditional computing systems, a single operating system runs on a dedicated physical server. This often results in underutilization of hardware resources because many servers operate below their maximum capacity. Virtualization solves this problem by creating multiple virtual machines (VMs) on a single physical server. Each virtual machine behaves like an independent computer with its own operating system, applications, memory, and storage.

Virtualization is widely used in cloud environments because it supports efficient resource allocation, workload management, disaster recovery, and server consolidation. Cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud use virtualization technologies to deliver scalable services to millions of users.

A. WORKING OF VIRTUALIZATION

Virtualization works through a software layer called a hypervisor or Virtual Machine Monitor (VMM). The hypervisor creates and manages multiple virtual machines on a physical system.

The hypervisor allocates hardware resources such as:
- CPU
- Memory
- Storage
- Network bandwidth

to different virtual machines according to workload requirements.

Each virtual machine operates independently, even though they share the same physical hardware.

B. TYPES OF VIRTUALIZATION

Virtualization can be classified into several categories based on the type of resource being virtualized.

1. Server Virtualization

Server virtualization divides a physical server into multiple virtual servers. Each virtual server can run its own operating system and applications independently.

Advantages
- Better resource utilization
- Reduced hardware cost
- Improved scalability
- Simplified server management

Applications
- Data centers
- Cloud hosting
- Enterprise systems

2. Storage Virtualization

Storage virtualization combines multiple physical storage devices into a single virtual storage unit. Users can access storage resources without knowing the physical location of data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Advantages
- Efficient storage management
- Easy backup and recovery
- Improved scalability
- Better data availability

Applications
- Cloud storage systems
- Backup services
- Data centers

3. Network Virtualization

Network virtualization combines hardware and software resources to create virtual networks.

Features
- Virtual switches
- Virtual routers
- Software-defined networking

Advantages
- Improved network flexibility
- Better traffic management
- Reduced hardware dependency

Applications
- Cloud networking
- Virtual private networks (VPNs)
- Data center networking

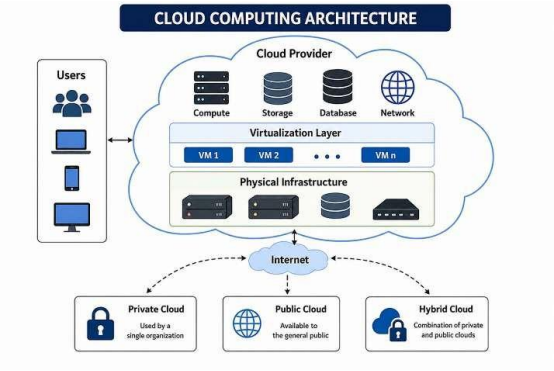
4. Desktop Virtualization

Desktop virtualization separates the desktop environment from physical devices. Users can access virtual desktops remotely through the internet.

Advantages
- Remote accessibility
- Centralized management
- Improved security
- Easy maintenance

Applications
- Remote work environments
- Educational institutions
- Enterprise systems

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2



5. Application Virtualization

Application virtualization allows applications to run without direct installation on local systems.

Advantages

- Simplified software deployment
- Reduced compatibility issues
- Easy updates and maintenance

Applications

- Cloud-based software delivery
- SaaS platforms

C. HYPERVISOR

A hypervisor is the main software component responsible for virtualization. It creates and manages virtual machines. Hypervisors are classified into two types.

1. Type 1 Hypervisor (Bare-Metal Hypervisor)

Type 1 hypervisors run directly on physical hardware without requiring a host operating system.

Advantages

- High performance
- Better security
- Efficient resource management

Examples

- VMware ESXi
- Microsoft Hyper-V
- Xen

2. Type 2 Hypervisor (Hosted Hypervisor)

Type 2 hypervisors run on top of an existing operating system.

Advantages

- Easy installation
- Suitable for testing and development

Examples

- Oracle VirtualBox
- VMware Workstation

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

D. ADVANTAGES OF VIRTUALIZATION

Virtualization provides several benefits in cloud computing environments.

1. Better Resource Utilization

Multiple virtual machines share the same hardware resources efficiently.

2. Reduced Hardware Cost

Organizations can reduce the number of physical servers required.

3. Improved Scalability

Virtual resources can be increased or decreased according to demand.

4. Faster Deployment

New virtual machines can be created quickly.

5. Disaster Recovery

Virtual machines can be backed up and restored easily.

6. Energy Efficiency

Virtualization reduces power consumption and supports green computing.

E. CHALLENGES OF VIRTUALIZATION

Although virtualization provides many advantages, it also introduces several challenges.

1. Security Risks

Attackers may exploit vulnerabilities in hypervisors and virtual machines.

Examples

- VM escape attacks
- Hypervisor attacks
- Malware infections

2. Performance Overhead

Running multiple virtual machines on the same hardware may reduce performance.

3. Resource Contention

Virtual machines may compete for CPU, memory, and storage resources.

4. Complex Management

Managing large virtual environments requires advanced monitoring tools and expertise.

F. SECURITY IN VIRTUALIZATION

Security is very important in virtualized cloud environments.

Security Techniques

- VM isolation
- Secure hypervisors

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

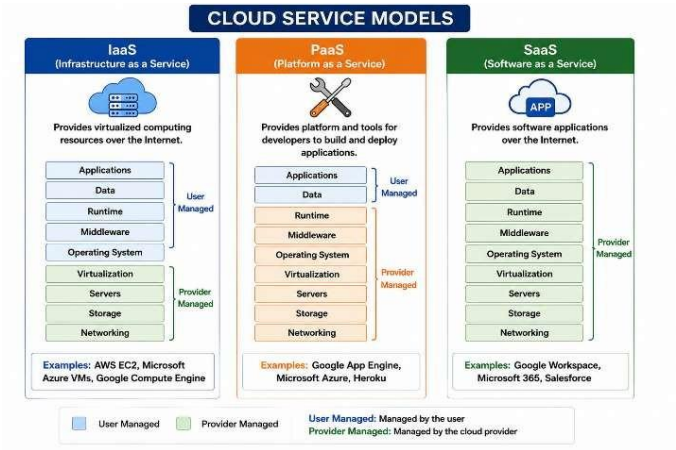
• Firewall protection
• Intrusion detection systems
• Regular security updates
Cloud providers implement these mechanisms to improve virtualization security and prevent cyberattacks.

G. APPLICATIONS OF VIRTUALIZATION

Virtualization is widely used in modern computing environments.
Major Applications
• Cloud computing
• Data centers
• Software testing
• Disaster recovery systems
• Web hosting
• Enterprise resource management

H. FUTURE OF VIRTUALIZATION

Modern virtualization technologies are evolving rapidly with cloud computing and artificial intelligence.
Future developments include:
• AI-based resource management
• Lightweight container virtualization
• Edge virtualization
• Improved security frameworks
• Energy-efficient virtualization systems Virtualization will continue to play a major role in cloud computing, distributed systems, and modern IT infrastructure.



V. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing environments face several security challenges because data and services are stored on remote servers connected through the internet. Security is one of the major concerns for organizations adopting cloud technologies. Unauthorized access, cyberattacks, insider threats, and data breaches may affect cloud systems and user privacy.

A. Data Breaches

Data breaches occur when unauthorized users gain access to confidential information stored in cloud systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Causes
- Weak passwords
- Poor authentication
- Malware attacks
- Insider threats

Effects
- Financial loss
- Reputation damage
- Privacy violations

Prevention Techniques
- Data encryption
- Multi-factor authentication
- Access control mechanisms

B. Data Loss

Data loss may occur due to hardware failures, accidental deletion, cyberattacks, or natural disasters.

Solutions
- Regular backups
- Disaster recovery systems
- Redundant cloud storage

C. Insider Attacks

Employees or internal users with privileged access may misuse cloud resources.

Security Measures
- User activity monitoring
- Role-based access control
- Authentication systems

D. Distributed Denial of Service (DDoS) Attacks

In DDoS attacks, attackers overload cloud servers with fake traffic and interrupt services.

Effects
- Service downtime
- Reduced performance
- Financial losses

Protection Methods
- Firewalls
- Traffic filtering
- Intrusion detection systems

E. Insecure APIs

Cloud applications communicate through APIs. Weak APIs may expose cloud systems to cyber threats.

Protection Methods
- Secure API authentication
- API encryption
- API monitoring

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

F. Vendor Lock-In

Organizations may face difficulties while migrating from one cloud provider to another.

Problems

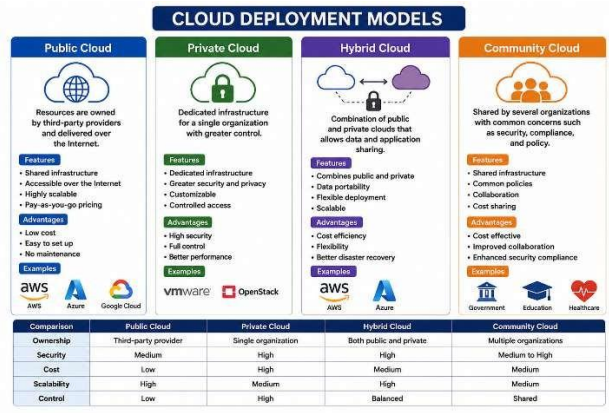
- Compatibility issues
- High migration cost
- Data transfer complexity

G. Privacy Concerns

Sensitive user information may be exposed without proper protection mechanisms.

Security Solutions

- Encryption
- Privacy policies
- Access restrictions



Comparison	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Ownership	Third-party provider	Single organization	Both public and private	Multiple organizations
Security	Medium	High	High	Medium to High
Cost	Low	High	Medium	Medium
Scalability	High	Medium	High	Medium
Control	Low	High	Balanced	Shared

VI. CRYPTOGRAPHIC TECHNIQUES IN CLOUD COMPUTING

Cryptography is used to secure cloud data and communication. It protects information from unauthorized access and cyber threats.

A. Encryption

Encryption converts readable data into unreadable ciphertext.

1. Symmetric Encryption

The same key is used for encryption and decryption.

Advantages

- Faster execution
- Suitable for large data

Examples

- AES
- DES
- Triple DES

2. Asymmetric Encryption

Different keys are used for encryption and decryption.

Advantages

- Better security
- Secure communication

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Examples
- RSA
- ECC
- Diffie-Hellman

B. Hashing
Hashing converts data into fixed-length hash values.
Applications
- Password protection
- Data integrity verification

Algorithms
- SHA-256
- SHA-1
- MD5

C. Digital Signatures
Digital signatures verify the authenticity of digital information.
Benefits
- Prevents tampering
- Ensures authenticity
- Provides non-repudiation

D. Homomorphic Encryption
Homomorphic encryption allows operations on encrypted data without decryption.
Advantages
- Better privacy
- Secure cloud computation

Limitation
- High computational complexity

VII. AUTHENTICATION IN CLOUD COMPUTING

Authentication verifies user identity before providing access to cloud services.
A. Password-Based Authentication
Users access cloud systems using usernames and passwords.
Limitation
Weak passwords may be easily attacked.

B. Multi-Factor Authentication (MFA)
MFA uses multiple verification methods such as:
- Passwords
- OTPs
- Mobile authentication

Advantages
- Improved security
- Reduced unauthorized access

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

C. Biometric Authentication

Biometric systems use fingerprints, facial recognition, or iris scanning.

Advantages

- High security
- Difficult to duplicate

D. Single Sign-On (SSO)

SSO allows users to access multiple applications using a single login.

Advantages

- Improved user experience
- Reduced password management

VIII. LOAD BALANCING IN CLOUD COMPUTING

Load balancing distributes workloads among multiple servers to improve performance and reliability.

A. Types of Load Balancing

1. Static Load Balancing

Workloads are distributed using predefined rules.

2. Dynamic Load Balancing

Workloads are distributed according to current system conditions.

B. Benefits of Load Balancing

- Better resource utilization
- Improved response time
- Reduced server overload
- Increased reliability

C. Common Load Balancing Algorithms

- Round Robin
- Least Connection
- Throttled Algorithm
- Weighted Response Time

IX. CLOUD SECURITY TOOLS

Several tools are used for cloud monitoring, testing, and security analysis.

Tool	Purpose
CloudSim	Cloud simulation
Wireshark	Network monitoring
Nessus	Vulnerability scanning
SoapUI	API testing
LoadUI	Load testing
Metasploit	Penetration testing

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

X. APPLICATIONS OF CLOUD COMPUTING

Cloud computing is widely used in various sectors.

A. Education

Cloud platforms support:

- Online learning
- Virtual classrooms
- Digital libraries

B. Healthcare

Cloud systems help manage:

- Patient records
- Medical imaging
- Telemedicine services

C. Banking

Cloud computing supports:

- Online banking
- Mobile payments
- Financial transactions

D. Business Organizations

Businesses use cloud computing for:

- CRM systems
- ERP systems
- Data storage
- Communication services

E. Social Networking

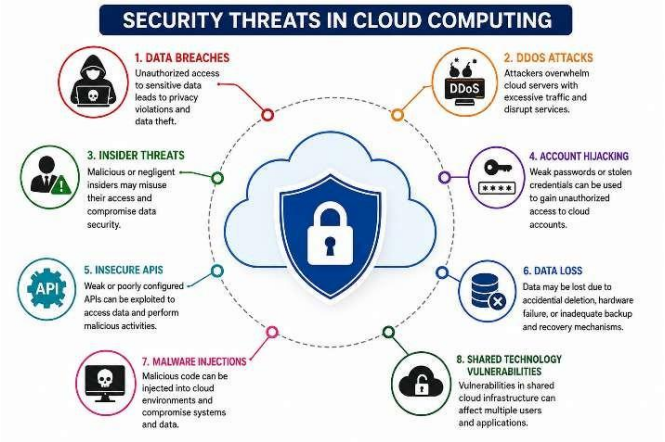
Applications such as:

- Facebook
- Instagram
- Twitter

use cloud infrastructure for scalability and data management.

F. Scientific Research

Researchers use cloud platforms for:



DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

XI. EMERGING TRENDS IN CLOUD COMPUTING

Modern cloud technologies continue to evolve rapidly.

A. Edge Computing

Edge computing processes data closer to users to reduce latency.

Advantages

- Faster processing
- Reduced network traffic

B. Artificial Intelligence in Cloud

AI improves:

- Automation
- Resource management
- Predictive analysis

C. Green Cloud Computing

Green cloud computing focuses on:

- Energy efficiency
- Reduced power consumption
- Environment-friendly systems

D. Serverless Computing

Applications run without direct server management.

Advantages

- Reduced infrastructure management
- Cost efficiency

E. Blockchain in Cloud Security

Blockchain improves:

- Secure transactions
- Transparency
- Data integrity

XII. LITERATURE SURVEY

Author	Contribution	Limitation
Armbrust et al.	Introduced cloud computing concepts	Limited security discussion
Buyya et al.	Explained cloud architecture	Complex implementation
Subashini et al.	Studied cloud security issues	Limited scalability analysis
Sharma et al.	Analyzed load balancing methods	Performance overhead
Zhang et al.	Discussed research challenges	Lack of real-time solutions

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

XIII. COMPARISON TABLES

A. Comparison of Service Models

Service Model	User Control	Provider Responsibility	Examples
SaaS	Low	Application & Infrastructure	Google Docs
PaaS	Medium	Platform & Infrastructure	Heroku
IaaS	High	Infrastructure only	AWS EC2

B. Comparison of Cryptographic Algorithms

Algorithm	Type	Security	Speed
AES	Symmetric	High	Fast
DES	Symmetric	Medium	Fast
RSA	Asymmetric	Very High	Slow
ECC	Asymmetric	High	Efficient
SHA-256	Hashing	High	Fast

C. Comparison of Deployment Models

Deployment Model	Security	Cost	Scalability	Control
Public Cloud	Medium	Low	High	Limited
Private Cloud	High	High	Medium	Full
Hybrid Cloud	High	Medium	High	Flexible
Community Cloud	Medium	Medium	Medium	Shared

XIV. FUTURE SCOPE

Future cloud systems are expected to provide:

- AI-based security systems
- Quantum cryptography
- Better privacy protection
- Energy-efficient cloud infrastructure
- Intelligent resource management

XV. CONCLUSION

Cloud computing has transformed the modern computing environment by providing scalable, flexible, and cost-effective services through the internet. However, security and privacy concerns remain major challenges in cloud systems. This paper presented a detailed survey on cloud computing security issues and cryptographic techniques used for protecting cloud environments.

The study discussed cloud service models, deployment models, virtualization, security threats, authentication mechanisms, load balancing techniques, and cloud security tools. Various cryptographic techniques such as AES, RSA, hashing, and digital signatures were explained for protecting cloud data and communication.

DOI: 10.48175/IJARSCT-35258

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

Cloud computing continues to evolve with modern technologies such as artificial intelligence, edge computing, blockchain, and green cloud computing. Future cloud systems are expected to become more secure, intelligent, scalable, and energy efficient.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, 2011.
[2] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[3] R. Buyya, C. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.
[4] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.
[5] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[6] Rajkumar Buyya, Christian Vecchiola, and S. Thamarai Selvi, "Mastering Cloud Computing: Foundations and Applications Programming," Morgan Kaufmann Publishers, 2013.
[7] K. Sharma and M. Tiwari, "Load Balancing in Cloud Computing," International Journal of Computer Applications, vol. 98, no. 6, pp. 10–15, 2014.
[8] J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," Communications of the ACM, vol. 51, no. 1, pp. 107–113, 2008.
[9] D. Minarolli and B. Freisleben, "Utility-Based Resource Allocation for Virtual Machines in Cloud Computing," IEEE, 2011.
[10] Md. Imran Alam, Manjusha Pandey, Siddharth S. Rautaray, "A Comprehensive Survey on Cloud Computing," International Journal of Information Technology and Computer Science, vol. 7, no. 2, pp. 68–79, 2015.