IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

A Comprehensive Review of Cloud Security and Trust Management: Challenges, Threats, Security Techniques, and Future Directions

Shruti Mehan[1], Dinesh Parkash[2]

Research Scholar, Department of Computer Science and Applications, Government College Chhachhrauli, Yamunanagar, Haryana, India[1]

Assistant Professor, Department of Computer Science and Applications, Government College Chhachhrauli, Yamunanagar, Haryana, India[2]

Abstract: Cloud computing has become one of the most widely used technologies for delivering computing resources and services over the internet. It provides several benefits such as flexibility, scalability, cost-effectiveness and easy access applications and data. However rapid growth of cloud services has also increased security concerns. Since sensitive and confidential information is stored over cloud platforms that are highly vulnerable to cyber-attacks, data breaches, malware attacks and insider threats. This paper presents an overview of cloud computing and its service models, along with major security threats and challenges, and also presents security solutions in the cloud environment. Various security techniques, such as encryption, authentication, access control, Artificial Intelligence-based security, and blockchain-based security, are discussed.

Keywords: Intrusion Detection Systems (IDS), Cuckoo Search Algorithms (CSA), Artificial Bee Colony Algorithm (ABC), Support Vector Machine (SVM), Naïve Bayes (NB)

1. INTRODUCTION

In today's digital world, cloud computing has become one of the most important technologies used by many organizations and businesses to store data and run applications more efficiently. Cloud computing helps users access files, software, and services anytime through the internet without depending completely on physical storage devices. Due to its flexibility, scalability, and cost-effectiveness, cloud computing is widely adopted in various sectors such as education, healthcare, banking, e-commerce, and information technology.

Although cloud computing provides many advantages, it also introduces some security and privacy challenges. A large amount of our data is stored on cloud platforms, which increases the risk of cyberattacks, unauthorized access, malware attacks, and data loss. Therefore, cloud security has become a major area of research and development.[1]

A. Cloud Computing

Cloud Computing is a technology that allows users to access computing resources such as storage, servers, databases, software, and networking services through the internet. Instead of depending completely on physical hardware or local systems, users can use cloud services anytime and from anywhere according to their requirements and pay only for the services they use. Cloud computing helps organizations improve efficiency, reduce operational costs, and easily manage large amounts of data and applications in a flexible and scalable environment.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

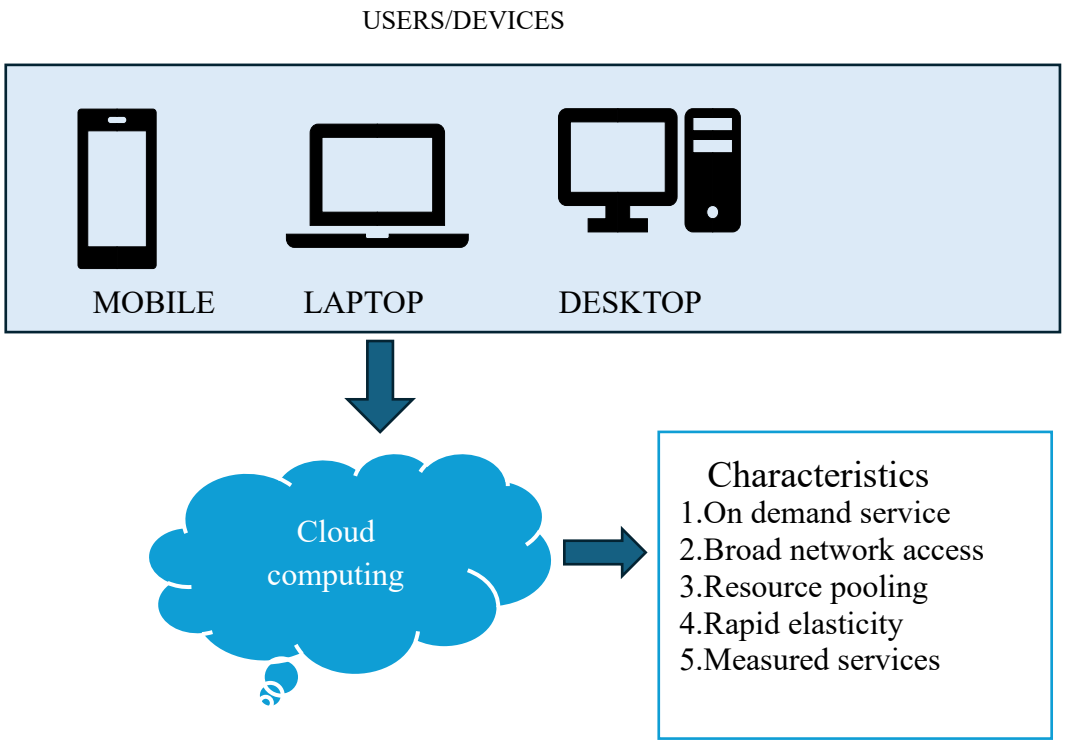

Figure 1: Cloud Computing

B. Cloud Computing Service Models

Cloud computing is delivered through three main service models which includes IaaS, PaaS and SaaS. Each model offers a different level of control, flexibility, and responsibility, making it easier for users to choose what fits their needs.

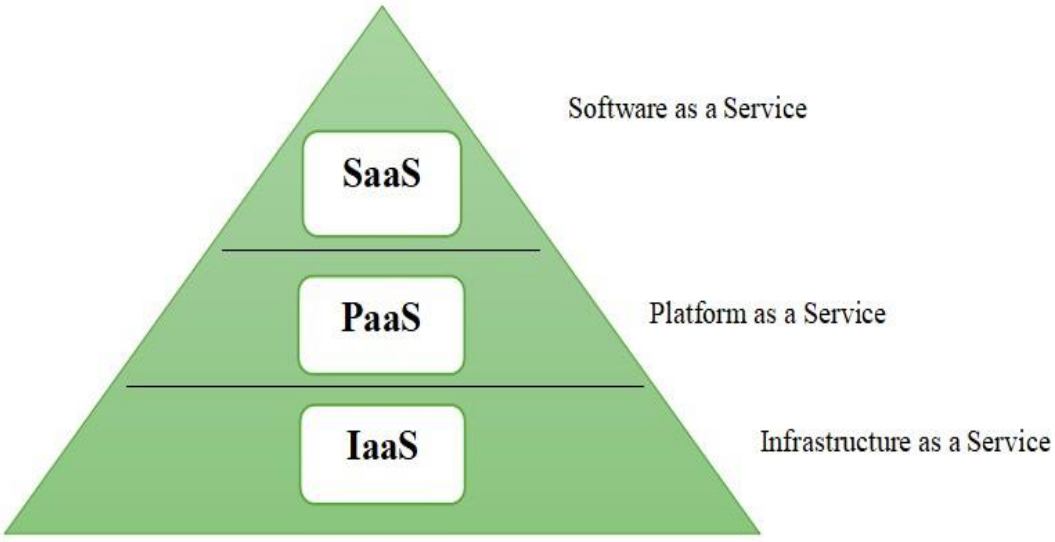

Figure 2: Cloud Computing Service Models

Infrastructure as a service (IaaS)

Infrastructure as a Service provides virtualized resources such as virtual machines, storage, servers, and networking through the internet. In this model, users do not need to purchase expensive hardware because the cloud provider manages the infrastructure, while users can control the operating systems and application according to their need. Users

DOI: 10.17148/IJARCCE.2026.15703

can easily increase or decrease resources according to their needs. IaaS is mainly used by organizations that require flexible and scalable infrastructure for their applications and data storage.

Platform as a service (PaaS)

Platform as a Service provides a complete platform for developers to build, test, and deploy applications without managing the underlying hardware or operating systems. It simplifies the application development process by offering tools, programming environments, and databases on one platform. This model is useful for developers because it saves time and reduces system management efforts.

Software as a service (SaaS)

Software as a Service allows users to access software applications directly over the internet without installing them on their local devices. The cloud provider manages the software, updates, and maintenance. Users can simply log in and use the application from any device with an internet connection. SaaS is widely used because it is easy to access, cost-effective, and user-friendly. [2]

2. LITERATURE SURVEY

D. Parkash & S. Mittal, [12] developed a new fitness function and suggested a revolutionary approach for Intrusion Detection Systems (IDS) using Cuckoo Search Algorithms (CSA). The aforementioned representation was created with reference to the KDD Cup 99 dataset in order to eliminate redundancy from the dataset and select the highest quality features that best represent qualitative data. The results of this study show that a suggested secured framework that uses the Cuckoo Search Algorithm to protect a cloud computing environment is effective in detecting intrusions and raising the security level.

In order to enhance the data security offered by cloud storage K.M. Akhil, et al. [20] proposed a method that uses the AES algorithm for transmission of data. It will be challenging for intruders to decode the information being transmitted because the suggested approach prevents third-party auditors from accessing user data.

In cloud computing, D. Parkash & S. Mittal [17] suggested an effective security framework using ABC. The planned approach has been taught using the KDD99 dataset. For effective cloud computing security, the authors have employed the Artificial Bee Colony Algorithm. After selecting features at random, the authors used the ABC Algorithm's advancement procedure. In terms of precision, accuracy, and recall limits, the suggested IDS outperformed Naïve Bayes and SVM IDS. In their suggested IDS, authors have prepared 36 preliminaries.

Table I Comparative Study of Cloud Security Models

Author & Year	Title	Methodologies	Findings	Limitations
Kumar & Ganpati (2016) [3]	An Approach for Data Security from Malicious Attacker in Cloud Computing	Empirical model, Turbo C implementation	Proposed two-key encryption to prevent insider & outsider fraud.	Basic cryptographic model; lacks scalability & stronger encryption.
Thakare & Singh (2016) [4]	Security & Privacy Issues at Service Models of Cloud Computing	Comparative study of SaaS, PaaS, IaaS	Identified audit as key solution; taxonomy of threats.	Conceptual only; no implementation details.
Padmaja & Seshadri (2016) [6]	Cloud Computing Technologies and Security Issues	Survey of Microsoft, Oracle, Google cloud	Highlighted confidentiality, integrity, availability; VM escape, DoS risks.	Survey style; lacked empirical validation.

DOI: 10.17148/IJARCCE.2026.15703

Birje et al. (2017) [7]	Cloud Computing Review: Concepts, Technology, Challenges and Security	Systematic Literature Review (77 papers)	Reviewed evolution, tools, challenges; emphasized security as critical.	Broad overview; lacked deep technical solutions.
Odun-Ayo et al. (2018) [8]	Cloud Computing Security: Issues and Developments	Industry & academic survey	Highlighted virtualization, data storage, identity management issues.	Broad survey; limited technical depth in countermeasures.
Srivastava & Khan (2018) [10]	Cloud Computing: A Review	Literature review	Explained SaaS, PaaS, IaaS; emphasized scalability & reduced infrastructure costs.	Security challenges not deeply analysed.
Malik et al. (2018) [11]	Cloud Computing Technologies	Conceptual review	Linked cloud to virtualization, SOA, grid computing; highlighted scalability.	Did not address privacy concerns.
Rashid & Chaturvedi (2019) [13]	Cloud Computing Models	Descriptive study	Reviewed SaaS, PaaS, IaaS, RaaS; discussed ERP, e-learning applications.	Security issues only briefly mentioned.
Omotosho (2019) [14]	A Review on Cloud Computing Security	Comparative review	Compared cryptographic algorithms (AES, RSA, DES) for cloud security.	Focused narrowly on encryption; ignored governance.
Alouffi et al. (2021) [15]	Systematic Literature Review on Cloud Security	SLR of 80 papers	Identified 7 major threats (data leakage, intrusion, tampering); suggested blockchain.	Blockchain role still exploratory.
Verma & Giri (2022) [16]	Survey on Cloud Computing Fundamentals	Comparative survey	Compared on-premise vs. cloud; highlighted flexibility, disaster recovery.	Cost and troubleshooting issues not deeply analysed.
Gupta et al. (2024) [18]	Review on Cloud Security: Challenges, Solutions, Innovations	Comparative analysis of 5 papers	Covered AI-driven detection, quantum-resistant encryption, multicloud frameworks.	High computational overhead; standardization issues.
Kokate et al. (2024) [19]	Security and Privacy in Cloud Computing	Literature survey + proposed framework	Suggested encryption, MFA, anonymization, compliance management.	Implementation details not tested in real-world.
Chopra et al. (2023) [21]	TOORA Cloud Architecture for Security	Case studies (railway, Gmail, blood bank)	Proposed third-party verification & key exchange.	Limited generalizable framework.

In this study proposal, D. Parkash & S. Mittal, [22] first used the Artificial Bee Colony Algorithm (ABC) to develop an IDS (Intrusion Detection System) for cloud security. Next, authors used the Particle Swarm Optimization Algorithm (PSO) to design an improved framework for cloud storage in a secure environment. In order to increase the effectiveness of the

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

suggested model, first took into account three performance measurements, such as recall, accuracy, and precision. Next, authors added two more metrics, such as the F-measure along with confusion matrix. Then contrasted this suggested model with the current models. The generated model that was trained using the NSL-KDD dataset is presented in this research proposal.

Although cloud security research has advanced, several clear gaps remain. Encryption methods like AES and RSA are strong in theory but struggle with scalability and high computational costs in large environments. Virtualization risks such as VM escape and migration attacks are well-documented, yet practical frameworks for strong isolation are missing. Privacy and compliance are often discussed, but tested enforcement models for regulations like GDPR and HIPAA are rare. Blockchain is proposed as a trust solution but remains mostly conceptual with limited real-world adoption. AI-driven threat detection shows promise, yet it requires constant retraining and heavy resources, making real-time use difficult.

Multi-cloud setups also lack standardized security policies, and most studies rely on simulations rather than enterprise-level testing.

3. THE FUNCTION OF TRUST IN CLOUD COMPUTING

The concept of trust encompasses many different aspects, such as confidence in reliability, dependability, capacity, steadfast quality, etc. the administration or face-to-face confession.
A dependable component will typically have a high degree of immovability, which means that it won't crash and burn through cooperation, will execute an entity or action within a reasonable time frame, will tell the truth and be clear about associations, and won't reveal confidential information. The various qualities that make up trust include enduring quality, immovability, validity, sincerity, security, ability, and common sense. These qualities may be seen as contingent on the environment in which trust is being resolved.

A. Parameters in Trust

In cloud computing, there are three core elements of trust: (a) SLA; (b) Performance; and (c) Security.[5]

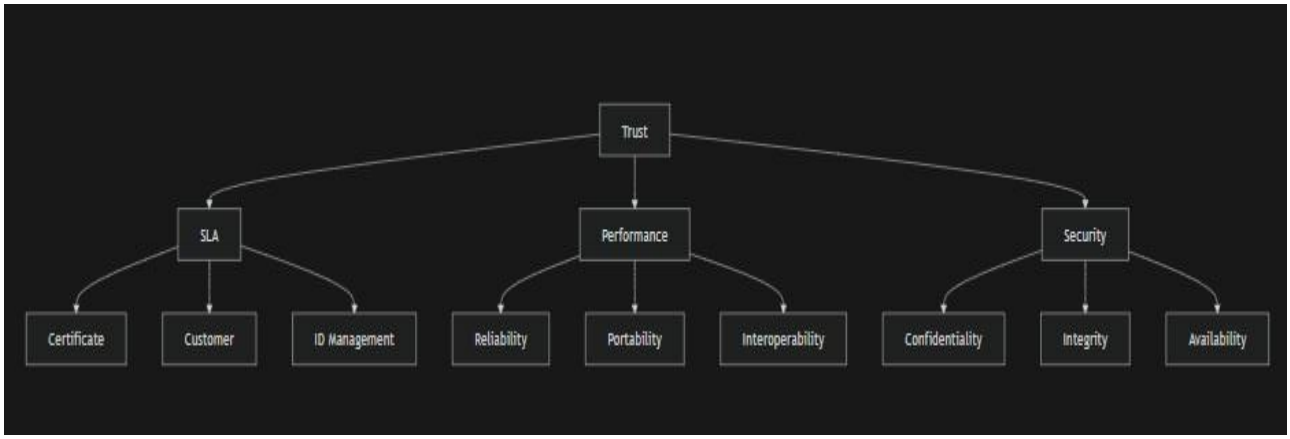

Figure 3: Parameters in Trust

4. CLOUD COMPUTING SECURITY

Cloud security is an important part of cloud computing that focuses on protection of our data, cloud-based systems, applications, and cloud services from cyber threats and unauthorized access. As more organizations move their information and services to cloud platforms, the need for secure cloud environments has increased significantly. Cloud security helps ensure that user's data remains safe, private, and accessible only to authorized individuals.
Cloud environments are connected through internet, which increases the risk of data breaches, hijacking, malware attacks and data loss, such that strong security mechanisms are required.[9]

4.1 Security Objectives

The main goals of cloud security are that help protect cloud systems, applications and users' data from cyber threats and unauthorized access. These objectives ensures that information stored in the cloud remain safe, accurate and available to only authorized users.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

(a) Confidentiality

Those only with consent can access sensitive data thanks to confidentiality. It aids in avoiding unwanted access to financial, private, and sensitive information. Confidentiality is preserved in cloud environments using widely used methods like encryption, authentication, and access restriction.

(b) Availability

Availability guarantees that customers may access cloud services, applications, and data whenever needed. It guards against system malfunctions, hacks, and service disruptions. In cloud computing environments, availability is maintained through the use of load balancing techniques, backup systems, and disaster recovery strategies.

(c) Integrity

Integrity guarantees that information stored in the cloud is correct, comprehensive, and unaltered throughout transmission. It shields data from unauthorized alteration, erasure, or corruption. Data integrity is preserved by the use of hashing, digital signatures, and data validation techniques.[12][5]

Figure 4: Security Objectives of Cloud Computing

5. SECURITY THREATS AND CHALLENGES IN CLOUD COMPUTING

Cloud computing provides flexibility, scalability and cost-effective services but it also introduces several security threats and challenge. Since cloud platforms store large amount of sensitive and confidential information, they become attractive targets for cybercriminals. Therefore, understanding these threats is important for maintaining secure cloud services.

a) **Data Breaches:** when an unauthorized user gain access to sensitive information stored in the cloud, data breaches occur. This can expose the personal, financial or organizational data and may lead to serious privacy and security issues.

b) **Data Loss:** Data loss is one of the major challenges in cloud computing. Important information may be lost because of accidental deletion, hardware failure, cyberattacks, or system crashes. Without proper backup and recovery mechanisms, recovering lost data can become difficult.

c) **Account Hijacking:** Account hijacking happens when attackers steal user credentials such as usernames and passwords to gain unauthorized access to cloud accounts. Once access is obtained, attackers may misuse sensitive data, modify information, or perform malicious activities.

d) **Insecure APIs and Interfaces:** Cloud services are commonly accessed through APIs and online interfaces. If these interfaces are not properly secured, attackers can exploit vulnerabilities to access cloud resources and confidential data.

e) **Malware and Cyberattacks:** Cloud systems can become targets of malware, ransomware, phishing attacks, and other cyber threats. These attacks may damage cloud infrastructure, steal information, or interrupt cloud services.

f) **Insider Threats:** Insider threats occur when employees, administrators, or authorized users misuse their access privileges intentionally or unintentionally. Such threats can lead to data leakage, unauthorized modifications, or security policy violations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

g) **Denial of Service (DoS) Attacks:** In a Denial-of-Service attack, attackers overload cloud servers with excessive requests, making services slow or unavailable to legitimate users. These attacks can affect the availability and performance of cloud systems.

h) **AI-Powered Cyberattacks:** Modern attackers increasingly use Artificial Intelligence (AI) to automate hacking activities, bypass security systems, and launch intelligent phishing or malware attacks against cloud platforms.

i) **Zero-Day Vulnerabilities:** Zero-day attacks exploit unknown software vulnerabilities before security updates or patches are released. These attacks are difficult to detect and can seriously compromise cloud systems.

j) **Multi-Cloud Security Challenges:** Many organizations use multiple cloud providers to improve flexibility and performance. However, managing security policies across different cloud platforms becomes more difficult and increases security complexity.[23]

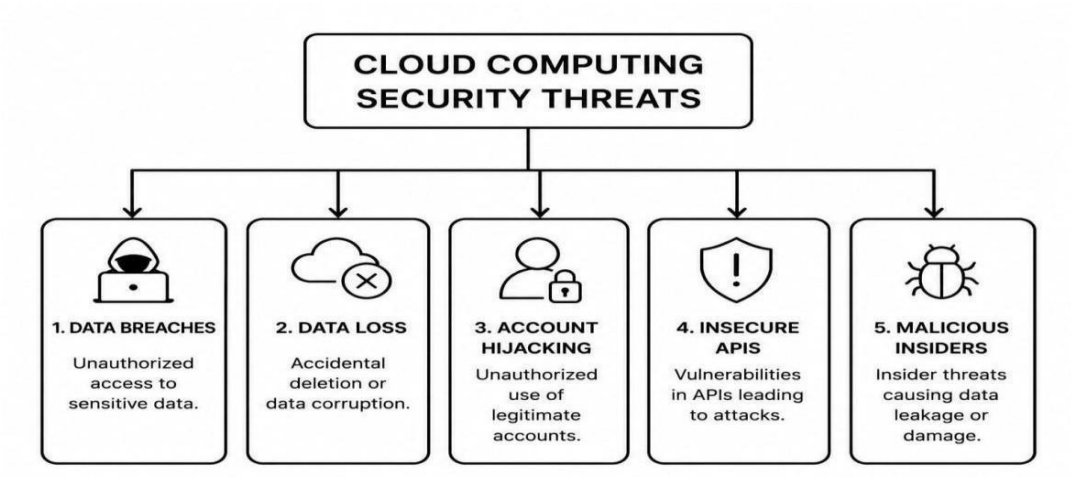

Figure 5: Cloud Computing Security Threats

6. CLOUD SECURITY TECHNIQUES AND SOLUTIONS

As the use of Cloud Computing continues to grow, protecting cloud environments from cyber threats has become very important. Different cloud security techniques and solutions are used to protect data, prevent unauthorized access, and maintain the reliability of cloud services.

i. **Encryption:** Encryption is one of the most effective methods used in cloud security. It changes data into a coded form so that unauthorized users cannot understand or access it. Encryption helps secure data while it is being stored or transferred through the internet.

ii. **Authentication and Multi-Factor Authentication:** Authentication helps verify the identity of users before they can access cloud resources. Along with passwords, many organizations use Multi-Factor Authentication (MFA), where users must complete additional verification steps such as OTPs or biometric scans. This provides an extra layer of protection and reduces the chances of unauthorized access.

iii. **Access Control:** Access control techniques are used to manage who can access specific cloud resources and data. These methods allow organizations to give permissions according to user roles and responsibilities. By limiting access to authorized users only, cloud systems become more secure and easier to manage.

iv. **Firewalls:** Firewalls are used to monitor and control network traffic entering or leaving cloud systems. They help block suspicious activities and protect cloud infrastructure from cyberattacks and unauthorized access attempts.

v. **Intrusion Detection and Prevention Systems:** Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) continuously monitor cloud networks to identify unusual or harmful activities. These systems can detect potential attacks and help organizations respond quickly before serious damage occurs.

vi. **Backup and Disaster Recovery:** Backup and disaster recovery solutions are important for maintaining data availability in cloud environments. Regular backups help organizations recover important information after accidental deletion, hardware failure, or cyberattacks. These techniques reduce the risk of permanent data loss.

vii. **Artificial Intelligence-Based Security: Artificial Intelligence (AI) is now widely used in cloud security to detect threats and analyze suspicious behavior more efficiently.** AI-based systems can identify unusual activities in real time and improve the speed and accuracy of threat detection.

viii. **Blockchain-Based Security:** Blockchain technology is also being explored to improve cloud security. It stores records in a secure and decentralized manner, making it difficult for attackers to modify or tamper with data. This helps improve transparency and data integrity in cloud environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026
DOI: 10.17148/IJARCCE.2026.15703

ix. **Security Monitoring and Auditing:** Regular monitoring and security auditing help organizations identify vulnerabilities and maintain secure cloud operations. Continuous observation of cloud activities makes it easier to detect security risks and ensure compliance with security policies.

x. **Zero Trust Security Model:** The Zero Trust security model follows the idea that no user or device should be trusted automatically. Every user must be verified before accessing cloud resources, even if they are already inside the network. This approach helps reduce both internal and external security threats.[24]

These techniques work together to improve the overall security and reliability of cloud services.

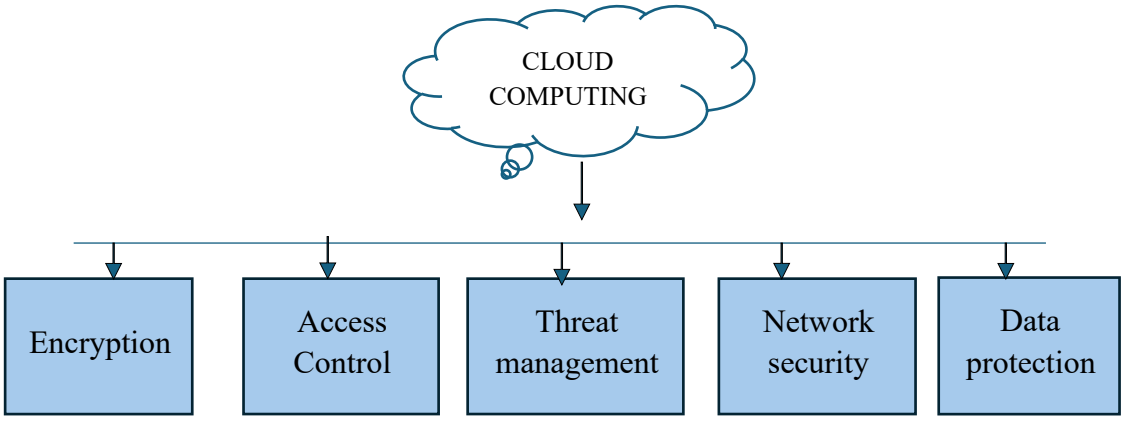

Fig. 6 Security Solutions

7. CONCLUSION AND FUTURE DIRECTIONS

Cloud computing security research from shows clear progress, moving from basic encryption and service model concerns to advanced solutions like AI-driven detection, blockchain integration, and quantum-resistant cryptography. Yet, most studies remain limited to theoretical models or simulations, with gaps in scalability, compliance enforcement, and real-world validation. Looking ahead, future work should focus on developing lightweight, resource-efficient AI models, stronger virtualization and multi-cloud frameworks, and practical adoption of blockchain and quantum security. There is also a need for tested compliance models that ensure global regulations are consistently applied. In short, the journey of cloud security is shifting from theory to practice, and the next step lies in building scalable, industry-ready solutions that balance performance, trust, and privacy. In our future research, we will propose a IDS to secure the cloud computing environment using any latest dataset.

REFERENCES

[1] D. Parkash and S. Taneja, "Cloud computing survey: Architecture, models, performance, storage and technologies", *International Journal of Computer Informatics & Technological Engineering (IJCITE)*, 1(7), pp 96–106 (2014).

[2] S. Habib, S. Hauke, S. Ries & M. Mühlhäuser, "Trust as a facilitator in cloud computing: A survey", *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1), 19 (2012).

[3] S. Kumar & A. Ganpati, "An approach for data security from malicious attacker in cloud computing", *Indian Journal of Science and Technology*, 9(32), pp 2-8 (2016).

[4] P. Thakare & A. Singh, "Security and privacy issues at service models of cloud computing", *Indian Journal of Science and Technology*, 9(38), pp 1-14 (2016).

[5] D. Parkash & S. Mittal, "Comparative study and performance analysis of various data security and cloud storage models", *Solid State Technology*, 63(2) pp 6318-6331 (2020).

[6] K. Padmaja & R. Seshadri, "Cloud computing technologies and security issues", *Indian Journal of Science and Technology*, 9(45), pp 1-8 (2016). [7] M.N. Birje, P.S. Challagidad, R.H. Goudar, M.T. Taple, "Cloud computing review: Concepts, technology, challenges and security", *International Journal of Cloud Computing*, 6(1), pp 32-57 (2017).

[8] I. Odun-Ayo, S. Misra & O. Daramola, "Cloud computing security: Issues and developments", *Journal of Computer Networks and Communications*, 2018, pp 1–12 (2018).

[9] D. Parkash & S. Mittal, "Comparative Analysis of Data Security and Cloud Storage Models Using NSL KDD Dataset", *International Journal on Recent and Innovation Trends in Computing and Communication* 11(10), pp 1222-1232 (2023).

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15703

[10] S. Srivastava & R. Khan, "Cloud computing: A review", *International Journal of Advanced Research in Computer Science and Software Engineering*, 8(6), pp 17-20 (2018).

[11] M.I. Malik, S.H. Wani & A. Rashid, "Cloud computing technologies" *International Journal of Advanced Research in Computer Science*, 9(2), pp 379–384 (2018).

[12] D. Parkash & S. Mittal, "An Enhanced Secure Framework Using CSA for Cloud Computing Environments" In: D. Gupta, A. Khanna, S. Bhattacharyya, A.E. Hassanien, S. Anand and A. Jaiswal, *International Conference on Innovative Computing and Communications*. Lecture Notes in Networks and Systems, vol 471. Springer, Singapore. https://doi.org/10.1007/978 981-19-2535-1_27 (2023).

[13] M. Rashid & S. Chaturvedi, "Cloud computing models", *International Journal of Computer Sciences and Engineering*, 7(2), pp 421-426 (2019).

[14] A. Omotosho, "A review on cloud computing security", *International Journal of Computer Science and Mobile Computing*, 8(9), pp 245-257 (2019).

[15] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami & R. Alharthi, "A systematic literature review on cloud security challenges and solutions", *IEEE Access*, pp 1-15 (2017).

[16] P. Verma & S. Giri, S, "Survey on cloud computing fundamentals", *International Journal of Engineering Research and Technology,* 11(1), pp 431-433 (2022).

[17] D. Parkash & S. Mittal, "An Efficient Security Framework Using ABC in Cloud Computing." *2nd International Conference on Research Trends in Engineering and Management, Proceedings of ICRTEM*- 2022, pp 60-64 (2022).

[18] L. Gupta, Y. Sharma & A. Chaudhary, A. "Review on cloud security: Challenges, solutions, innovations" *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 4(2), pp 528-530 (2024).

[19] S. Kokate, P. Raiskha, S. Pandey, B. Jaydev "Security and privacy in cloud computing", *International Journal of Novel Research and Development (IJNRD),* 9(4), pp b935-b937 (2024).

[20] K.M. Akhil, M.P. Kumar & B.R Pushpa, B. R, "Enhanced cloud data security using AES algorithm". *International Conference on Intelligent Computing and Control (I2C2).* doi:10.1109/i2c2.2017.8321820 (2017).

[21] A. Chopra, R. Sharma, & P. Singh, P, "TOORA cloud architecture for security", *International Journal of Computer Applications*, 182(12), pp 25– 31 (2023).

[22] D. Parkash & S. Mittal, "An Enhanced Security Framework for Storage using PSO in Cloud Computing", *International Journal of Intelligent Systems and Applications in Engineering*, 12 (5s), pp 513–520 (2024).

[23] A. Alshammari, S. Alhaidari, A. Alharbi & M. Zohdy, "Security threats and challenges in cloud computing", *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* pp. 46-51, IEEE (2017).

[24] N. Kumar, J. Surolia & D. Goyal, "Adaptive Security Techniques in Hybrid Cloud Environments: A Comprehensive Review of Emerging Trends and Technologies", *Intelligent Systems Using Semiconductors for Robotics and IoT*, pp 210-214 (2026).

