Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

# Cyber security Challenges in Cloud Computing

[1]Mr.JJelsteen,[2]Nivitha A,[3]Srinithi S

[1]Assistant Professor, [2,3]Student

Department of computer applications

Sri Krishna arts and science college, Coimbatore

Abstract

Cloud computing has become, like, one of the most commonly used technologies for stowing, handling, and overseeing data through Internet-based services. A lot of organizations across different fields—education, healthcare, banking, commercial operations, and also government— are increasingly leaning on cloud platforms because they bring scalability, adaptability,costeffectiveness,andsimpleaccessibility.Still,cloudcomputingdoesnotcome only with positives, it also brings major cybersecurity issues that endanger the confidentiality, integrity, and availability of sensitive information. In practice, cyber threats like data exposure, malwareinfections,ransomwareincidents,insiderabuse,weakapplicationprogramming interfaces(APIs),accounttakeovers,andDistributedDenial-of-Service(DDoS)attackskeep rising inside modern cloud environments. In this review paper, we look at the big cybersecurity challenges tied to cloud computing and we discuss the protection mechanisms that are used for safeguarding cloud infrastructures. The analysis covers key security tools such as encryption approaches, Identity and Access Management (IAM), Multi-Factor Authentication (MFA),Intrusion Detection and Prevention Systems (IDS/IPS), firewalls, and Zero Trust Architecture.Also,thepaperexploresnewerdirectionslikeArtificialIntelligence(AI),MachineLearning (ML), Blockchain, Edge Computing, and Quantum-Resistant Cryptography, as future trends for strengthening cloud security. Overall, it underscores the need for layered defensive strategies,steadysurveillance,andsmarterthreat-spottingsystems,socloudenvironmentsremainsecure anddependable.Theconclusionsofthisreviewofferusefulviewpointsintopresentcloud security problems, existing protection mechanisms, and, in general,how teams can reduce cyberrisk more effectively, in order to keep sensitive data safer.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

security problems, existing protection mechanisms, and, in general,how teams can reduce cyberrisk more effectively, in order to keep sensitive data safer.

## 1. Introduction

Cloudcomputingkindofbecame one of the most influential technologies in moderncomputing,helpingorganizations tapintocomputingresourcesviathe Internet, without having to keep a costly physical setup. In practice it offers services thatyoucanscaleupordown,likeraw computing power, storage, database layers, networkcapacity,andeven software applications.Thatmixletsbusinessesget betterdaytodayefficiency,whileatthe same time loweringinfrastructure expenses. And moreand morecompaniesare cybersecurityheadaches,mostly becausethearchitectureisspreadout, resources can be shared,and everything is reachable through the Internet. So, it's fairtosaythatshieldingcloudenvironments fromcyberthreatsisnowamainissue, both for organizations using cloud services and for the cloud service providers too.

### 1.1 BackgroundofCloud Computing.

Cloud computing is one of the most important developments in information technology. By accessing computing resources over the Internet without physical infrastructure, users can have complete control over their operations. Organizations can access computing services on demand, which enhances the flexibility, scalability, and affordability of information technology resources. Cloud computing has caused a swift transformation in the management of digital assets across various sectors such as businesses,schoolsandhealthcare facilities. The reason why organizations are shifting their applications and data to cloud services is because cloud-based services reduce infrastructure costs, improve operational efficiency, and enable remote access from any location. Cloud computingis commonly divided into three primary servicemodels:Ias,Pap,andSaaS.The userandcloudserviceproviderhave varyingdegreesofcontroland responsibility in these service models. Additionally,organizationscanchoosefrom a range of cloud deployment models including Public Cloud, Private CloudHybrid Cloud and Community Cloud to ensure that the environment meets their operational and security needs. Although it has numerous advantages, cloud computing still presents severalsecurityvulnerabilities.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Due to the fact that organizational data is storedandprocessed onremoteservers,it is susceptible to cyber threats such as unauthorized access, data breaches,malware attacks or ransomware. The security risks may compromise data confidentiality, integrity, and availability, resulting in financial losses, legal action, or reputational harm. Hence, cybersecurity is now an essential aspect of cloudcomputing.' To ensure the safety ofsensitive informationandsecure cloud-based environments, organizations must employ appropriate security measures, policies, and best practices.

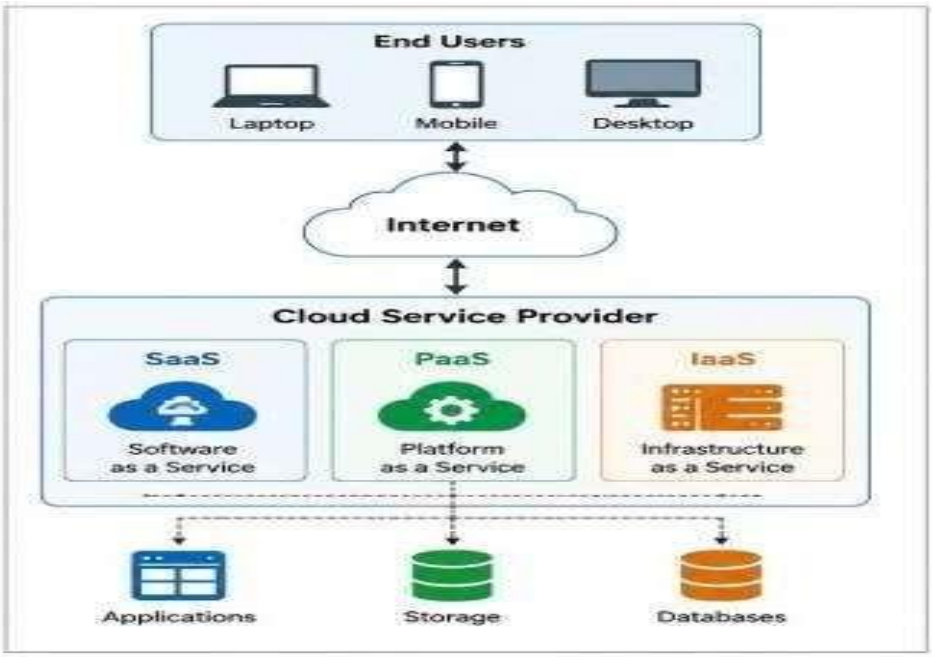


**Fig. 1.** Basic Architecture of Cloud Computing

## 1.1 Importance of Cybersecurity in Cloud Computing

The fast growth of cloudcomputing has really pushed the amountof sensitive information up, so a lot more personal and private things now sit on cloud platforms. You can find personal info, financial records, healthcare data, educational materials, even business applicationsbeinghostedthere.Becauseof this, cloud systems are basically turned into tempting destinations for cybercriminals. Cybersecurity isneededto guard cloud resources from all kinds of issues like data leaks, malware infections, ransomware events, phishing attempts, insider risks, account hijacking, poorly secured APIs, and also DistributedDenial-of-Service (DDoS) attacks.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

When cloud security is done well, it protects confidentiality, integrity, and availabilityof the information—often called the CIA Triad, or you know the core three principles. Cloud security usually followsa shared responsibility model, which sounds simple but it matters. Cloudservice

providers handle the base infrastructure, while customers are expected to secure their own parts, like user accounts, applications, access rights, and the data that is stored. Soorganizations should put into place things such as encryption, multi factor authentication (MFA), identity and access management (IAM), intrusion detection systems (IDS), plus ongoing security monitoring. This is meant to lower cyber risks, even when new vulnerabilities keep appearing.


**Fig. 2.** CIA Triad in Cloud Security

## 1.3 ObjectivesoftheStudy

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

The main objective of this review paper is, to look at the big cybersecurity obstacles tied to cloud computing andalso to discuss how security mechanisms are typically used to safeguard cloud environments, kinda end to end. More specific objectives are listed below, but they are basically aiming at both understanding and evaluation. To give an overview of the core concepts behind cloud computing, and cloud security. To pin-point the major cybersecurity threats that commonly show up in cloud environments. To examine the security techniques that already exist, includingthe best practices that organizations tendto follow. To explore new or evolving technologies like Artificial Intelligence (AI), Machine Learning (ML),Blockchain

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

### 1.4 Scopeof theReview

This review focuses on cybersecurity topics linked with cloud computing settings. It talks about the security headaches organizations oftenfacewhentheyadoptcloudservices,and it also reviews the kinds of technologies that have been created to deal with those issues. In general the coverage includes cloud service models, deployment models, well known cyber threats, security solutions, as well as emerging patterns in how cloud protection is being handled today. The review draws on published research papers, books, and technical reportsthatarerelatedtocloudsecurity. It is intended to help students, researchers, and industry professionals gain a more complete, even if practical, understanding of cloud cybersecurity, and what future developments might look like.

## 2. LiteratureReview

The literature review looks at earlier work about cybersecuritychallenges and security solutions in cloud computing.Alotofresearchershaveproposed different approaches like encryption, authentication, intrusion detection systems, blockchain based mechanisms, and even artificial intelligence driven defenses, to makecloud platforms more protected. In this part, the goal is to summarize keyresearch contributions, point out what seems weak or limited in existing studies, andalso mention where future workcould go. It is a bit messy but you can say this section tries to connect the dots.

### 2.1OverviewofPreviousStudies

Cloud computing security has grown into a big research area, because organizations more and more store sensitive information on cloud services. Many authors have studied cloud weaknesses, cyber threats, and security frameworks, all aiming to strengthen the protection of cloud environments. Earlier studies mostly concentrated on: Data confidentialit Accesscontrol Authentication mechanisms Secure virtualization Encryption techniquesMore recent studies broaden the pictureby combining cloud protection with: Artificial Intelligence , Machine Learning Blockchain technology Zero Trust Architecture Multi-cloud security frameworks Overall, the researchers tend

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

proposed different approaches like encryption, authentication, intrusion detection systems, blockchain based mechanisms, and even artificial intelligence driven defenses, to makecloud platforms more protected. In this part, the goal is to summarize keyresearch contributions, point out what seems weak or limited in existing studies, andalso mention where future workcould go. It is a bit messy but you can say this section tries to connect the dots.

### 2.3Research Gap

Even though earlier studies have helped a lot with cloud security research, there are still some limitations that really bother me. Many older methods seem to concentrate on securing single cloud parts, insteadoftryingtobuildamore connected security framework, you know, the kind that works across everything.Also, the fast expansion of Artificial Intelligence (AI), Internet of Things (IoT), edge computing, and multi-cloud settings has created fresh attack surfaces. Unfortunately,moststandarddefensesjust do not cover them properly, or they cover them only partially and then moveon. So the research gaps can be seen as a few recurring points, like: - Real-timethreat detection is limited - Automated security response systems are missing Multi-cloudprotectionisweakScalability keeps causing issues Implementation complexity is high in the future, research should probably aim at blendingAI,blockchain,andZeroTrust

## 3 CybersecurityChallengesinCloud Computing

In cloud computing environments there are a lot of cybersecurity threats, especially because the architecture is spread out, the infrastructure is shared,the services are Internet accessible, andthe data is kept remotely. So, thesesecurity pressures can, in practice,weakenconfidentiality,integrityand even availability of sensitive information that lives inside cloud platforms. Because of that, organizations should recognize possible risks sooner rather than later,then apply solid security mechanisms, so cloud infrastructures are not easily compromised by cyberattacks.

### 3.1 Data Breaches

A data breach happens when unauthorized people get into confidential information that lives inside cloud systems. It’s one of those really serious cybersecurity threats, because cloud

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

platforms usually hold sensitive thingslike personal details, financial records, healthcare data and also business information, all together in one place. Thingsthatcommonlyleadtodatabreaches include, but aren't limited to, these: Weak passwords Lack of proper access control Insecure APIs Cloud misconfigurations, especially whensettings are left too open Insider attacks Malware infections After a data breach, organizations may face consequences like Financial losses Legal penalties Damageto reputation A real loss of customer.

### 3.2 DataLoss

Data loss is when cloud data gets accidentally or on purpose destroyed, deleted, or corrupted. Sometimes it just happens because the system, or people, do something wrong. Other times it is from cyberattacks, hardware failures, human error, software malfunction or natural disasters. It can be messy, you know, andit does not always show up right away. Some big causes that often lead to dataloss are: Accidental deletion Ransomware attacks Hardware failure Power interruption Software errors Not having adequate backup systems to reduce the damage when something like this occurs, organizations should create solid backup strategies, and also keep disaster recovery plans ready. This helps when the situation goes bad, and the recovery needs to befast, and still controlled

### 3.3 Insiderthreats

Insider threats come from employees, contractors, or otherauthorized users who, in a not so good moment, misuse their allowed access to steal, change, or ruin organizational data. Insider based attacks can be hard to spot, because the person inside already haslegit access to the cloud resources, and it can look normal. Some types of insider threats are, like: Malicious employees Careless or negligent users Third party contractors Former employees who still have active accounts to lower insider threats, organizations need constant monitoring, log of user activity, andstrong access control rules.

### 3.4 MalwareAttacks

Malware is malicious software, made to harm systems, take sensitive data, orjustmessupcloudservices—sometimesallof those. You'llusually hear about viruses, worms,

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

spyware, trojans, and ransomware, as commontypes. Cloud environments can feel especiallyvulnerabletomalware,because people often reach cloud services using Internet connected devices, not always with good settings. The malware might slip in through a few doors, like phishing emails. or unsafe downloads and alsoinfectedwebsites.Weakendpointsecurity can make it worse too, like really. To lower those malware risks,organizations should rely on antivirus software, firewalls, as well as intrusion detection systems. The goal is to reducethe chance of infection before anything spreads, sort of early and proactive.

### 3.5 DistributedDenial-of-Service (DDoS) Attacks

A Distributed Denial-of-Service (DDoS) attack is a type of cyberattack where several compromised systems, all together, overwhelm a cloud server or network by sending too much traffic, so cloud services become unavailable to real users. In practice, DDoS attacks can strongly harm both availability and day to day performance for cloud based applications and services, even if the restof the architecture is fine. In cloudsettings, attackers frequently lean on botnets, those are networks of infected computers plus Internet of Things (IoT) devices, and they use them to trigger large scale DDoS waves. Some common effects of DDoS attacks, include the following kind of issues Service interruption Decreased network performance financial loss Customer dissatisfaction Resource exhaustionOrganizations

Firewalls Traffic filtering Load balancing Intrusion Prevention Systems (IPS) DDoS mitigation services.

### 3.6 Weak Authentication and Access Control

Authentication and access controlare kinda essential for shielding cloud systems from access that is not allowed. When passwords are weak, identity management is kinda messy, and the authentication setup is not very solid, then the odds of account takeover go up, plusdata theft usually follows. Some authentication related problems that pop upa lot are Weak passwords Password reuseNo Multi-Factor Authentication (MFA) Access permissions that are wrong, or too broad Credential theft, basically in many cases attackers take advantage of theseweak authentication mechanisms via phishing, brute force attempts, andcredential stuffing. It’s like they just try many angles at once, until something opens up. Organizations should really focus on: Strong password policies Multi-Factor Authentication (MFA) Identity and Access Management (IAM) practices Role-Based Access Control (RBAC)

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

## 4. Security Solutions in Cloud Computing

Cloud computing environmentsreally do need strong security, to protect sensitive information, and to keepoperations secure in general. Since cyber threats keep changing, organizations are using more advanced security technologiesto shield cloud infrastructures from illegal access, malware strikes, data leaks, and service interruptions. Cloud security is not one single thing though, it usually comes from a mix of encryption, authentication systems, access control methods,surveillance and monitoring technologies, plussmarterthreatdetectionframeworks.Encryption Techniques Encryption is one of the most used security mechanismsin cloud computing. It safeguards important information by changing readable data into an unreadable form called ciphertext. Then only authorized users, who have the right decryption key can recover the original content.Inpractice,encryptionmattersa lot for protecting stored data, transmitted information, and even user credentials that must stay confidential, so nobody else can get in. Cloud service providers commonly rely on encryption algorithms likeAdvanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), andSecure Hash Algorithms (SHA) for confidentiality and integrity. By using encryption, the danger of data theft drops, and that helps build confidence in cloud computing environments too.

### 4.1 Identity and Access Management (IAM)

Identity and Access Management, often shortened to IAM, is basically a security framework that controls who cangettocloudresources.Inpracticeit verifies user identities and then attaches permissions to them, following the organizational policies. When access is limitedtotherightusersonly,ithelps block unauthorized access. it also reduces the chance of insider attacks, you know. Most modern cloud platforms use IAM solutions for authentication, authorization and even user activity monitoring. Within these systems, Role-Based Access Control (RBAC) is quite common, so users end up with access only to the resources they actually need for their responsibilities. If IAM is done well, cloud security gets stronger and the organization gains better control over cloud resources.

### 4.2 Multi-Factor Authentication (MFA)

Multi-FactorAuthentication, sometimescalledMFA,improvescloud securitybyaskingusersforseveralkinds ofproofbeforetheycanactuallyreach cloudsystems.Intherealworld,password based sign-in aloneiskindashaky, since it

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

canbetargetedwithphishing,credentialtheft, or even brute-force attempts. MFA helps lower those problems, because it usesa mix of verification factors such as passwords, One-Time Passwords (OTP), biometric checks, or smart cards. WhenMFA is putin place properly,the chancesof account hijacking and unwanted access drop a lot. Also, a growing number of cloud providers view MFA as basically a must have security measure, meant for safeguarding cloud accounts and protecting sensitive organizational information.

### 4.3 IntrusionDetectionand Prevention Systems (IDS/IPS)

Intrusion Detection Systems, IDSand Intrusion Prevention Systems, IPS basically help you keep an eye on cloud networks and catch cyber threats as they happen. An IDS continuously inspects network traffic and system activities, so it can spot shady patterns or outright harmful attacks. AnIPS adds a further layer,because it can automatically block, or more formally prevent, the attacks it finds. Together these tools can flag malware infections,unwantedorunauthorizedaccess attempts, DDoS attacks, plus weird network behavior that doesn’t look right. In newer setups, IDS/IPS tools often lean on Artificial Intelligence (AI) and Machine Learning (ML) for better threat recognition,

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

## 5. Future Trends in Cloud Cybersecurity

Withcloudcomputingchanging fast, the demand for smarter cybersecurity mechanisms keeps getting bigger, mainly because new cyber threats keep showing up. Old-style security setups are not really enough anymore for today cloud infrastructures, since attacks are growing more sophisticated, more automated andalso harder to spot. Because of that, researchers as well as organizations are looking into newer technologies, plus intelligent security frameworks, tostrengthencloudprotectionandkeepsecure digital spaces functioning well. 5.1 ArtificialIntelligenceandMachine Learning in Cloud Security Artificial Intelligence, usually called AI and Machine Learning (ML) are turning into basic partsof cloud cybersecurity systems. In practice, these approaches let cloud platforms spotodd actions on their own, figure outabnormal user patterns, and then react to threats in real time. Compared with older security models that rely on fixed rules, AI-driven frameworks can keep learning from network behavior and gradually sharpentheir ability to detect danger. Machine learningisbeingusedmoreandmoreinside Intrusion Detection Systems (IDS), malware analysis, fraud detection, and behavioral analytics too. AI-powered cybersecurity tools can process huge sets of cloud data more efficiently, which helps surface disguised attack structures that conventional defenses might overlook. And as cloud services keep expanding, AI and ML are likely to matter a lot for intelligent threat prevention, and even for automatic incident response, not just monitoring.

### 5.1 Blockchain Technology in Cloud Security

Blockchain technology is emerging as a promising solution for enhancing cloud securityduetoitsdecentralizedand tamper-resistant nature. Blockchain stores information in distributed blocks that are linked together using cryptographic techniques, making unauthorized data modification extremely difficult.Researchers are exploring blockchain-based authentication systemsand decentralized cloud storage models to reduce dependence on centralized cloud infrastructures. Although blockchain technology offers strong securityadvantages, challenges such as scalability, energy consumption, and implementation complexity still require further research.

### 5.2 EdgeComputing Security

Edge computing is an emerging approach where data gets processed nearthe source, not only inside one centralized cloud. In practice this can speed things up, make delays shorter, and enable real-time serviceslikeInternetofThings(IoT), smart healthcare, self-driving vehicles, and

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

industrialautomation.Still,edgecomputing brings fresh cybersecurity problems,sinceinformationishandledby a lot of scattered devices, plus edge nodes that are spread around. Keeping edgedevices safe from malware, unwanted access, and also tampering with data has turned into an important research topic. Looking ahead, cloud security frameworks will probably blend edge protections—like lightweight encryption, hardened communication protocols, and monitoring systems that use AI—to safeguard these distributed computing environments in a more complete way.

## 6. Conclusion

Cloud computing has kind of transformedmoderninformation technology, offering scalable, flexible, and cost-effective computing services through the Internet. In practice, organizations from different sectors lean more and more on cloudplatformsfordatastorage, application hosting, communications, and day-to-daybusinesswork.Yet,evenwithall these advantages, cloud computing also brings real cybersecurity issues that can endanger the confidentiality, integrity, and availabilityofimportantinformation.In this review paper, we looked at the main cybersecurity challenges linked to cloud computing, like data breaches, data loss, insider threats, malware infections, ransomware, Distributed Denial-of-Service (DDoS) attacks, insecure APIs, weak authentication, account takeover/hijacking, and cloud misconfigurations. These threats keep evolving, and they still create heavy risks for both organizations and cloudservice providers. We also reviewed key security solutions, including encryption approaches, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Intrusion Detection and Prevention Systems (IDS/IPS),firewalls, and Zero Trust Architecture. In short, these mechanisms have a major partin shielding cloud infrastructures from unauthorizedaccess,aswellasfroma broad set of cyberattacks. Also, several newer directions were discussed as future research topics such as ArtificialIntelligence (AI), Machine Learning (ML), Blockchain, Edge Computing, Quantum-Resistant Cryptography, and multi-cloud securityframeworks.Theexpectationis that these tools can support more automated threat detection, smarter securitymonitoring,steadierauthentication

## REFERENCES

1] Cloud Computing: Concepts, Technology & Architecture, Thomas Erl, Ricardo Puttini, and Zaigham Mahmood, Prentice Hall, 2013.

[2] Cloud Security and Privacy, Tim Mather, Subra Kumaraswamy, and Shahed Latif, O'Reilly Media, 2009.

[3] Computer Security: Principles and Practice, William Stallings and Lawrie Brown, 4th ed., Pearson,

2018.

[4] Cryptography and Network Security: Principles and Practice, William Stallings, 8th ed., Pearson, 2020.

[5] Security Engineering, Ross Anderson, 3rd ed., Wiley, 2020.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖