Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 1 (2026)

A Survey on Security Challenges in Community and Multi-Cloud Computing

J. Karthikeyini[1], Dr. K. S. Mohanasathiya[2], Dr. S. Prasath[3]

[1]Author, Ph.D Research Scholar, Department of Computer science, VET Institute of Arts and Science (Co-Education) College, Thindal, Erode

[2]Co Author**,** Associate Professor and Head, Department of IT & CT, VET Institute of Arts and Science(Co- Education) College, Thindal, Erode

[3]Co Author, Associate Professor and Head, Department of CSA, VET Institute of Arts and Science(Co- Education) College, Thindal, Erode

Abstract

Cloud computing has become an essential technology for organizations and individuals due to its scalability, flexibility, and cost-effectiveness. However, the rapid adoption of cloud services has also introduced several security challenges. This paper reviews recent Security Issues in cloud computing, including Data Breaches, Insecure APIs, Insider Threats, Ransomware Attacks, and Multi-cloud vulnerabilities Furthermore, future research directions for improving cloud security are highlighted. The study aims to provide insights into the evolving security landscape of cloud computing environments. It enables users to access shared computing resources on an on-demand and pay-per-use basis. It offers significant benefits such as reduced capital costs, scalability, and operational efficiency. However, security remains a major challenge that limits the widespread adoption of cloud computing. Security vulnerabilities can lead to personal, financial, and ethical risks. This paper explores the key security challenges faced by cloud entities, including Cloud Service Providers (CSPs), data owners, and cloud users. This paper also discusses current security solutions such as Encryption, Identity management, Artificial Intelligence-based Threat Detection, and Zero Trust Architecture. It focuses on crypto-cloud environments involving communication, computation, and Service Level Agreements (SLAs). Additionally, this paper analyzes the causes and impacts of various cyber attacks and discusses possible security enhancements to improve cloud reliability and protection.

Keywords: Cloud Computing, Cloud Security, Data Breaches, Cybersecurity, Zero Trust, Encryption

1. Introduction

Cloud computing enables users to access computing resources such as storage, servers, and applications through the internet. The increasing use of cloud services has transformed various industries including healthcare, education, banking, and e-commerce.Despite its advantages, cloud computing faces major security concerns due to the storage and transmission of sensitive information over the internet. Cyberattacks targeting cloud environments have increased significantly in recent years. Security challenges such as unauthorized access, data leakage, malware attacks, and insecure application programming interfaces (APIs) threaten the reliability of cloud platforms.This paper reviews recent security challenges in cloud computing and discusses emerging security mechanisms to address these threats. Cloud computing provides a network-based environment that enables users to share computing resources and services regardless of location.

Cloud computing is characterized by features such as on-demand self-service, broad network access, rapid elasticity, resource pooling, and measured service. It supports four deployment models: public, private, hybrid, and community clouds. Additionally, cloud services are delivered through three major service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).Although cloud computing improves scalability, efficiency, and cost reduction, security challenges remain significant across all service layers. Higher layers are browser-dependent, while lower layers focus more on web services and infrastructure management. The choice of deployment model depends on user and organizational requirements.

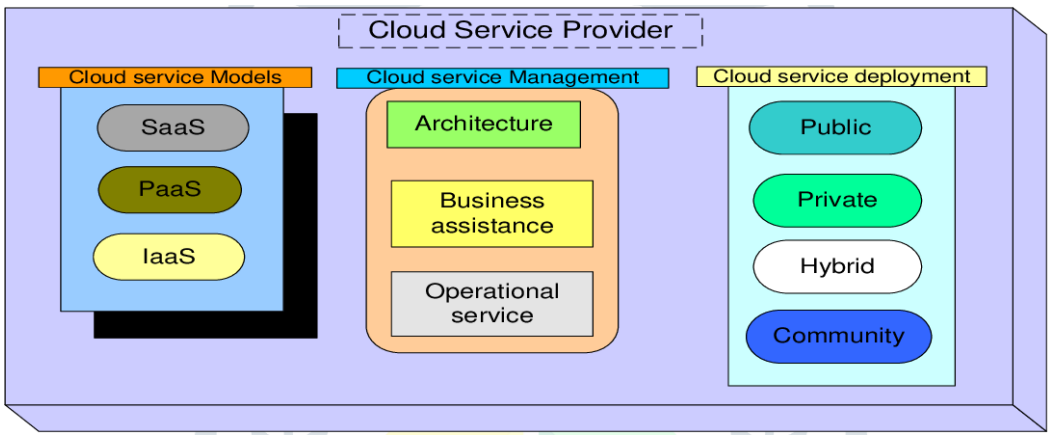


Fig. basic cloud architecture

2. Overview of Cloud Computing

Cloud computing provides on-demand access to shared computing resources. It is generally classified into three service models:

- **Infrastructure as a Service (IaaS)**

Infrastructure as a Service (IaaS) provides computing hardware resources such as virtual machines, storage, servers, processors, memory, and data centers as on-demand services. It has transformed business investments in IT infrastructure by enabling flexible allocation of physical and virtual resources. IaaS offers scalability and efficient resource provisioning through technologies such as hypervisors, reducing the need for high investment in hardware and maintenance. It also incorporates security mechanisms including firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual machine monitoring. Despite these advantages, IaaS continues to face several security challenges and vulnerabilities.

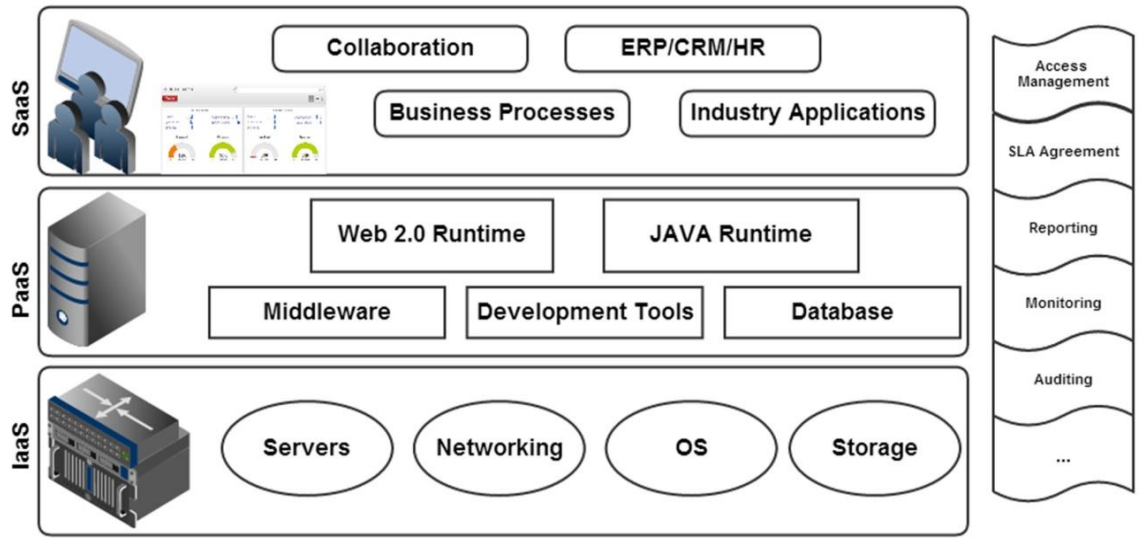
- **Platform as a Service (PaaS)**

Platform as a Service (PaaS) acts as the middleware layer in cloud computing and provides services such as development tools, frameworks, architectures, applications, and Integrated Development Environments (IDEs). It allows users to develop and manage applications without controlling the underlying infrastructure. PaaS is especially useful for collaborative software development among developers located in different regions. A well-known example of PaaS is Google App Engine, which supports programming languages such as Python, Java, and Go through its Software Development Kit (SDK). Compared to SaaS, PaaS offers greater flexibility and extensibility by providing ready-to-use development features. However, PaaS also faces security challenges related to application runtime environments, third-party integrations, software development lifecycle management, and underlying infrastructure security.

- **Software as a Service (SaaS)**

Software as a Service (SaaS) is the top layer of the cloud service model and provides applications over the internet through third-party vendors. In this model, users can access and use applications hosted on the cloud infrastructure of Cloud Service Providers (CSPs) without managing the underlying systems. SaaS is one of the fastest-growing segments in the cloud computing market due to its ease of access and cost efficiency. Popular SaaS providers include Google Workspace and Salesforce. However, from the customer's perspective, security remains a major concern, as configuration errors and vulnerabilities can expose sensitive data and applications

to cyber threats. Cloud systems provide flexibility and scalability but require strong security mechanisms to protect user data.



Cloud deployment models include:

Public Cloud

A public cloud is a cloud environment that provides services to the public through internet-based access under a defined Service Level Agreement (SLA) between the customer and provider. Public cloud infrastructures are commonly owned and operated by businesses, academic institutions, or government organizations. Since resources are shared among multiple users and organizations, issues related to resource ownership, location, and security become more complex. This shared environment increases the difficulty of protecting data and infrastructure from cyberattacks and unauthorized access.

Private Cloud

A private cloud is a cloud computing environment that is operated and managed within an organization's own data center for exclusive use by that organization. It is commonly used by business units that require greater control over their infrastructure and data. Since the cloud infrastructure is owned and managed internally, the relationship between the provider and users is clearly defined. As a result, security risks are easier to monitor, detect, and manage compared to other cloud deployment models.

Hybrid Cloud

A hybrid cloud combines two or more cloud deployment models, such as public, private, or community clouds. In this model, data and applications are integrated using standardized technologies, enabling seamless communication between different cloud environments. Hybrid cloud offers the benefits of multiple deployment models, including flexibility, scalability, and improved resource management. Compared to public cloud environments, hybrid clouds provide better organization and enhanced security while still allowing internet-based access to resources and services.

Community cloud

A community cloud is a cloud infrastructure shared by multiple organizations with common concerns such as security requirements, policies, mission objectives, and compliance standards. It may be owned and managed by one or more organizations, third-party providers, or a combination of both, and can be hosted on-site or off-site. By enabling resource sharing among organizations, the community cloud model reduces the security risks associated with public clouds while lowering the cost compared to private cloud deployments.

3. Recent Security Impacts in Cloud Computing

3.1 Data Breaches

Data breaches are among the most serious cloud security threats. Sensitive user information stored in cloud servers can be accessed by unauthorized users due to weak authentication or poor security practices.

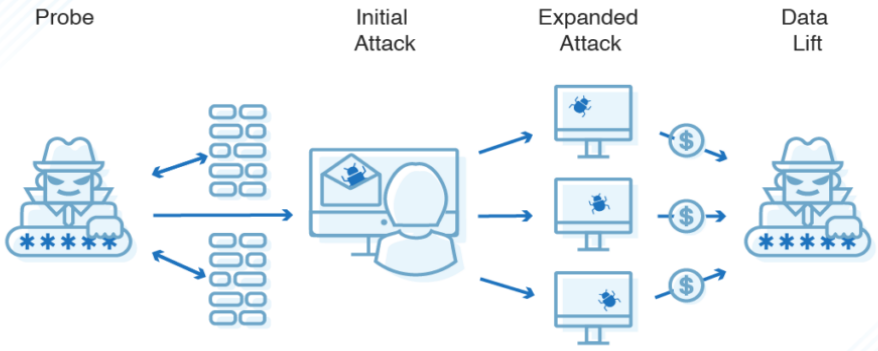


Fig. how a data breach occur

- **Financial loss**

One of the main effects of cloud computing security breaches is financial loss. Organizations may suffer large financial losses as a result of cyberattacks including ransomware assaults, data breaches, and unauthorized access. Companies may have to pay for data recovery, legal fines, user compensation, and service interruptions. Furthermore, reputational harm and a decline in customer trust can hinder long-term corporate growth and lower revenue. Strong security measures must therefore be put in place in order to reduce financial risks in cloud systems.

- **Reputation damage**

Reputation damage is a serious consequence of security incidents in cloud computing. Cyberattacks, service lapses, and data breaches can erode consumer confidence and harm a company's reputation. Customers may lose faith in the company's ability to secure data if sensitive user information is hacked. Customer loss, less economic prospects, and long-term effects on brand value are possible outcomes of this. To safeguard an organization's reputation, robust security procedures and dependable cloud services are crucial.

- **Privacy violations**

When private or sensitive information kept in cloud settings is accessed, shared, or revealed without permission, privacy violations take place. Inadequate access control, data breaches, and weak security measures can expose private data to hackers or unauthorized users. Such infractions could result in identity theft, legal repercussions, and a decline in user confidence. Therefore, to guarantee privacy in cloud computing settings, robust encryption, access control methods, and data protection rules are crucial.

3.2 Insecure APIs

Cloud services rely heavily on APIs for communication and integration. Poorly secured APIs can expose systems to attacks such as unauthorized access and data manipulation.

- **Weak authentication**

A significant security flaw in cloud computing is weak authentication, which gives unauthorized users access to critical information and cloud resources. Inadequate identity verification procedures, poor password practices, and a lack of multi-factor authentication raise the possibility of assaults such account hijacking and data leaks.

Enhancing cloud security requires the use of robust authentication techniques, such as secure password restrictions and multi-factor authentication.

- **Injection attacks**

Cyberattacks known as "injection attacks" involve inserting malicious code or commands into an application in order to alter databases or system functions. Attackers in cloud computing use flaws in online apps or APIs to obtain unauthorized access, steal information, or interfere with services. Command injection and SQL injection attacks are two common varieties. To stop injection attacks in cloud systems, proper input validation, secure coding techniques, and frequent security testing are crucial.

- **Token theft**

Theft of authentication tokens, which are used to confirm user identities and get access to cloud services, is a security risk in cloud computing. Without the need for passwords, stolen tokens might give unauthorized users access to private information and programs. Malware, phishing scams, and unsafe storage methods are common causes of token theft. Token theft risk can be decreased by implementing multi-factor authentication, encryption, short token expiration times, and secure token administration.

3.3 Insider Threats

Insider threats occur when employees or authorized users misuse their access privileges. These threats are difficult to detect because insiders already have system access. Insider threats are security concerns brought on by people who work for a company, such as contractors, employees, or authorized users, abusing their access rights. These risks can result in data loss, illegal access, or system damage and can be deliberate or unintentional. Because insiders already have authorized access to resources, insider threats in cloud computing are challenging to identify. Insider-related risks can be decreased by putting in place stringent access controls, ongoing monitoring, and user activity audits.

3.4 Ransomware Attacks

Ransomware attacks encrypt cloud data and demand payment for recovery. The increasing use of cloud storage has made cloud systems a major target for attackers. These attacks are cyberattacks in which malicious software encrypts the data of a business and requests payment to unlock it. Ransomware can cause data loss and service interruption in cloud computing by targeting virtual machines, cloud storage, and linked systems. These assaults have the potential to cause serious operational and financial harm. To stop ransomware attacks in cloud environments, regular data backups, robust access restrictions, updated security solutions, and employee awareness are crucial.

3.5 Multi-Cloud Security Issues

- **Lack of centralized control**

One of the biggest problems with cloud computing is the absence of centralized control, particularly in distributed and multi-cloud settings. It can become difficult and inconsistent to manage security rules, data

access, and system configurations across several cloud platforms. This raises the possibility of misconfigurations, security flaws, and illegal access. Organizations can maintain improved visibility, control, and security across cloud infrastructures by putting centralized administration and monitoring solutions into place.

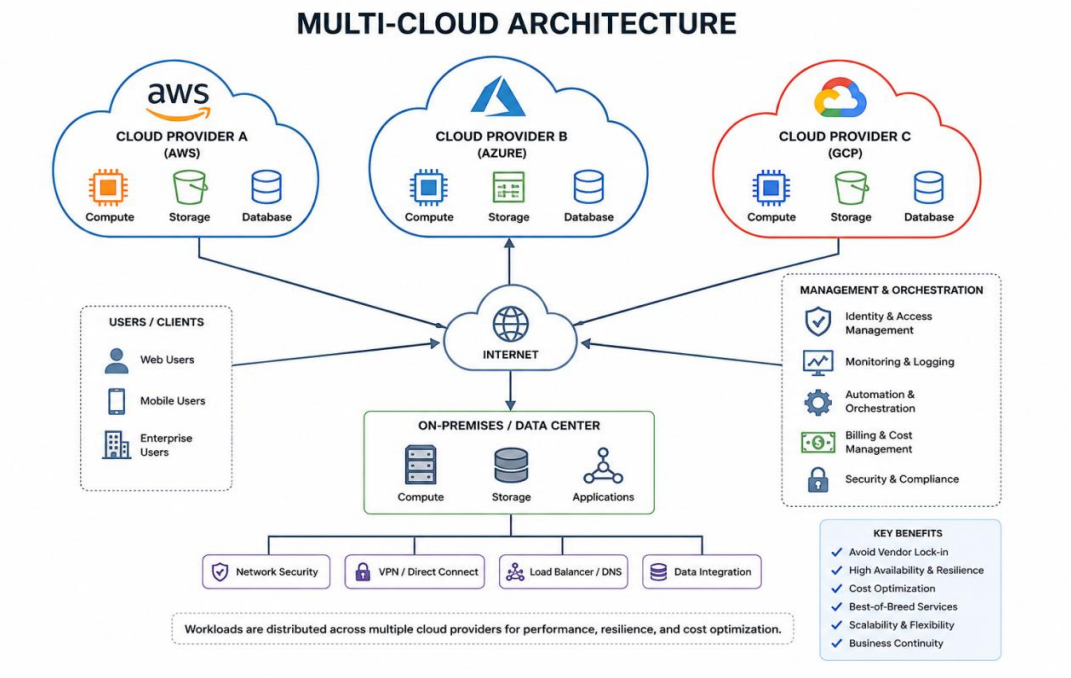


Fig. multicloud architecture

- **Configuration errors**

Insecure default setups, inappropriate access rights, or erroneous system settings can all lead to configuration errors, which are frequent security problems in cloud computing. Sensitive information, programs, and services may be vulnerable to cyberattacks or illegal access due to improperly configured cloud resources. These blunders are frequently the result of human error or a lack of security knowledge. To lower configuration-related risks in cloud settings, regular security audits, automated configuration management, and appropriate access control measures are crucial.

- **Inconsistent security policies**

When several cloud platforms or departments adhere to distinct security standards and procedures, inconsistent security rules arise. This may lead to security flaws, making it challenging to implement consistent security throughout the cloud system. Unauthorized access, problems with compliance, and heightened susceptibility to cyberattacks can result from uneven policies in multi-cloud systems. Consistent cloud security requires the establishment of centralized policy administration and uniform security frameworks.

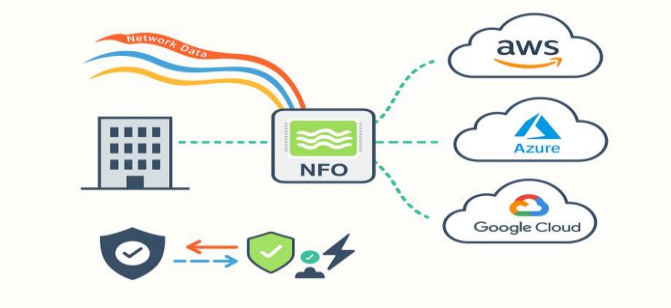


Fig.Bridging the Visibility Gap for Hybrid and Multi-Cloud Environments

3.6 Distributed Denial of Service (DDoS) Attacks

DDoS attacks overwhelm cloud servers with excessive traffic, causing service disruptions and downtime. Cloud security is dynamic and often relies on automation and orchestration to respond quickly to emerging cyber threats. The scalability of cloud environments also enables advanced security services, such as Distributed Denial-of-Service (DDoS) protection and threat intelligence, to be deployed on demand. Both traditional IT systems and cloud environments share common security challenges, including malware protection, secure data storage, and user authentication. However, cloud computing introduces additional concerns such as multi-tenant resource sharing, configuration vulnerabilities, and dependence on Cloud Service Providers (CSPs) for security management. With the growing adoption of hybrid and multi-cloud architectures, integrating traditional security practices with cloud-native security solutions has become essential. Effective cloud security requires continuous monitoring, regular security audits, and compliance with industry standards across the entire IT infrastructure.

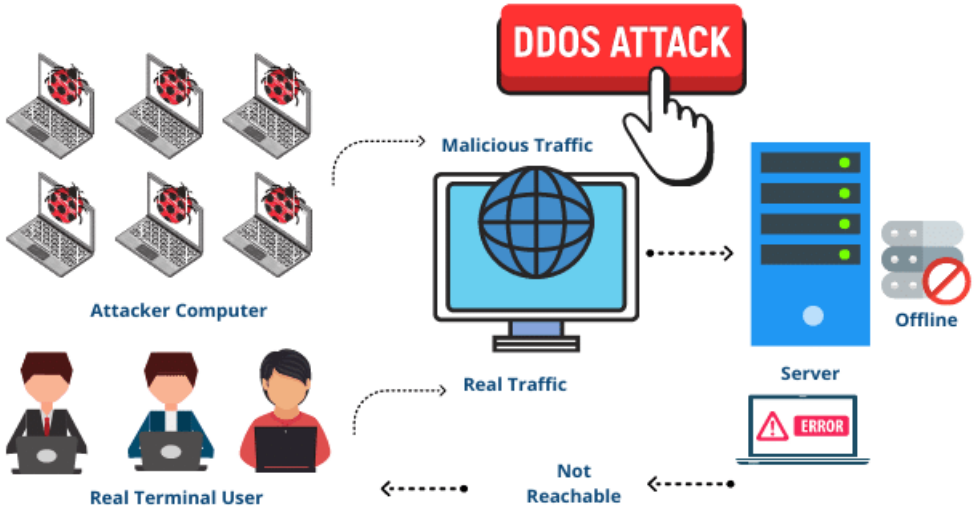


Fig. operation of DDOS attacks

Key Aspects of DDoS Attacks

Mechanism: Attackers use malware to gain control of networked devices (computers, IoT devices) and command them to simultaneously send traffic to a target.

Impact: Common consequences include slow performance, complete service unavailability, significant financial losses, and reputational damage.

Types:

Volumetric Attacks: Overwhelm bandwidth by flooding the network with high volumes of data.

Protocol Attacks: Exhaust server resources (e.g., firewalls, load balancers) by exploiting network protocols.

Application Layer Attacks: Target specific applications (like web servers) with seemingly legitimate HTTP requests, often harder to detect.

Motivations: Attacks are driven by extortion (ransom), hacktivism, competition, or disrupting business during critical times.

4. Security Solutions and Technologies

Security in traditional IT systems mainly focuses on protecting physical infrastructure and internal networks managed within an organization. Organizations maintain direct control over servers, applications, and network security using mechanisms such as firewalls, intrusion detection systems, and access controls. In this model, the

organization is fully responsible for maintaining and updating the entire infrastructure. In contrast, cloud computing security addresses additional challenges because data is transmitted over the public internet and stored on shared infrastructures operated by third-party Cloud Service Providers (CSPs). Cloud environments follow a shared responsibility model, where the CSP secures the cloud infrastructure, while customers are responsible for protecting their data, applications, and user access. Cloud security adopts a data-centric approach by implementing encryption for data at rest and in transit, Identity and Access Management (IAM), and continuous monitoring for real-time threat detection. Compared to traditional IT systems, cloud computing requires more dynamic and scalable security mechanisms to manage distributed and multi-tenant environments effectively.

4.1 Encryption Techniques

Encryption protects sensitive information during storage and transmission. Advanced encryption standards improve data confidentiality. In cloud computing, encryption techniques are crucial security measures that shield private information from unwanted access. Using cryptographic techniques, encryption transforms legible data into an unintelligible format, guaranteeing confidentiality throughout data transport and storage. Symmetric encryption, asymmetric encryption, and sophisticated standards like AES (sophisticated Encryption Standard) are examples of common encryption techniques. Encryption lowers the danger of cyberattacks and data breaches, protects user information, and preserves data privacy in cloud environments.

4.2 Multi-Factor Authentication (MFA)

MFA enhances security by requiring multiple verification methods before granting access. Before gaining access to cloud services or systems, users must authenticate themselves using two or more authentication factors. This security measure is known as multi-factor authentication, or MFA. Passwords, one-time verification codes, biometric authentication, and security tokens are a few examples of these variables. By lowering the possibility of unwanted access, account hijacking, and credential theft, MFA improves cloud security. Even in the event that user credentials are hacked, it offers an extra degree of security.

Fig. multifactor authentication

4.3 Artificial Intelligence applications in Cloud Security

AI-based systems can detect unusual behavior and identify cyber threats in real time. In cloud computing, artificial intelligence (AI) improves data processing, automation, and security. Large-scale data analysis, anomalous activity detection, and real-time cyber threat identification are all possible with AI-powered systems. AI is used by cloud platforms for activities including threat intelligence, automated resource management, predictive analytics, and intrusion detection. AI integration with cloud computing enhances decision-making, scalability, and efficiency while bolstering cloud security in general.

Intrusion detection

In a cloud computing context, intrusion detection is a security tool used to spot cyberattacks, suspicious activity, or unauthorized access. In order to identify possible security risks including malware, illegal access attempts,

and unusual activity, intrusion detection systems (IDS) continuously monitor network traffic and system activity. IDS enhances security in cloud environments by generating alerts, detecting threats in real time, and responding to incidents more quickly.

Threat prediction

Threat prediction is a security strategy that detects possible cyberthreats before they happen by utilizing cutting-edge technology like artificial intelligence (AI) and machine learning. Threat prediction in cloud computing looks for suspicious patterns and potential assaults by analyzing system activity, network traffic, and user behavior. Organizations may lower security risks, enhance incident response, and fortify overall cloud security with this proactive approach.

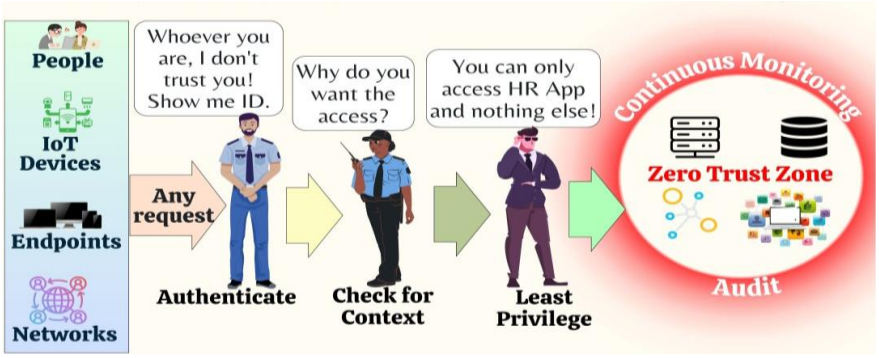
Automated response systems

In cloud computing environments, an Automated Response System is a security mechanism that automatically recognizes, evaluates, and reacts to cyberthreats without the need for human intervention. Artificial Intelligence (AI) and machine learning technologies are used by these systems to swiftly detect suspicious activity and take prompt action, such as blocking malicious traffic, isolating impacted systems, or creating security warnings. Automated response systems increase overall cloud security, decrease human error, and speed up incident reaction times.

4.4 Zero Trust Architecture

Zero Trust security assumes that no user or device should be trusted automatically. Continuous verification improves security. The security architecture known as Zero Trust Architecture (ZTA) is predicated on the idea that "never trust, always verify." It is predicated on the idea that no user, device, or application should be immediately trusted, even if they are connected to a network. Before allowing access to resources, Zero Trust continuously checks user identities, device status, and access permissions in cloud computing. This strategy lowers security risks, helps stop unwanted access, and fortifies defenses against insider threats and cyberattacks. Zero trust architecture is security model that assumes no one is trust worthy even those already inside the network. Access to resources is granted only when necessary and with the least privilege possible.

Fig. zero trust architecture



5. Comparative Analysis of Security Challenges

Comparative analysis of cloud computing security issues aids in determining the distinctions, effects, and remedies related to different cyberthreats. Cloud infrastructures are impacted differently by security issues like ransomware attacks, insider threats, unsecured APIs, data breaches, and Distributed Denial-of-Service (DDoS) assaults. While ransomware attacks interfere with data availability and operations, data breaches primarily jeopardize confidentiality. While insider threats are challenging to identify because of legitimate user credentials, insecure APIs and lax authentication procedures raise the danger of unwanted access. By contrasting these difficulties, businesses may increase cloud security by better understanding their risks and putting in place suitable security measures such encryption, multi-factor authentication, intrusion detection systems, and centralized security management.

Security Threat	**Impact**	**Possible Solution**
Data Breach	Data loss	Encryption
Insecure APIs	Unauthorized access	API security testing
Insider Threats	Information leakage	Access control
Ransomware	Data encryption	Backup systems
DDoS Attacks	Service downtime	Traffic filtering

6. Future Directions

Recent studies provide a comprehensive overview of evolving cloud security threats and the role of emerging technologies such as Artificial Intelligence (AI) and blockchain in enhancing cloud security. However, limited research exists on the scalability, resource requirements, and practical implementation of these technologies in large-scale cloud infrastructures. Understanding the challenges associated with AI-driven threat detection and blockchain-based security mechanisms is essential for real-world adoption. Future research should focus on both qualitative and quantitative approaches to address these gaps. Qualitative studies may include case studies on advanced Identity and Access Management (IAM) systems and legal compliance in cloud environments, while quantitative research can evaluate the performance and scalability of emerging security technologies. Collaborative interdisciplinary research involving legal experts, computer scientists, and industry professionals can further support the development of effective cloud security solutions. Will follow by Quantum-resistant encryption , Automated incident response systems. Emerging technologies will help improve cloud reliability and user trust.

7. Conclusion

Cloud computing offers significant benefits but also introduces serious security challenges. Recent threats such as data breaches, ransomware attacks, insecure APIs, and insider threats have increased the need for advanced security mechanisms. Technologies such as encryption, AI-based threat detection, MFA, and Zero Trust architecture provide effective solutions for improving cloud security. Continuous research and innovation are necessary to build secure and reliable cloud environments.

References

[1] Malallah HS, Qashi R, Abdulrahman LM, Omer MA, Yazdeen AA. Performance Analysis of Enterprise Cloud Computing: A Review. Journal of Applied Science and Technology Trends. 2023 Feb 5

[2] Gammelgaard B, Nowicka K. Next generation supply chain management: the impact of cloud computing. Journal of Enterprise Information Management. 2023 Mar 28.

[3] L'Esteve RC. New Horizons in Distributed Cloud Computing. InThe Cloud Leader's Handbook: Strategically Innovate, Transform, and Scale Organizations 2023 Jul 6 (pp. 123-134). Berkeley, CA: Apress.

[4] Ionescu SA, Diaconita V. Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing and Advanced Data Management Technologies. International Journal of Computers Communications & Control. 2023 Oct 30

[5] Yang C, Huang Q, Li Z, Liu K, Hu F. Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth. 2017 Jan 2

[6] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13

[7] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics. 2021 Dec 22

[8] Dittakavi RS. Evaluating the Efficiency and Limitations of Configuration Strategies in Hybrid Cloud Environments. International Journal of Intelligent Automation and Computing. 2022 Nov 17

9] Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: A survey. Wireless Personal Communications. 2023 Jan

[10] Chauhan M, Shiaeles S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 2023 Sep 12

[11] Ranaweera P, Jurcut AD, Liyanage M. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials. 2021 Feb 26

[12] A. M. Andrew, "Cloud Computing: Views on Cybersyn," Kybernetes, Vol. 41, No. 9, 2012 http://dx.doi.org/10.1108/03684921211275450[CrossRef]

[13] S. Dhar, "From Outsourcing to Cloud Computing: Evolution of It Services," Management Research Review, Vol. 35, No. 8, 2012 http://dx.doi.org/10.1108/01409171211247677[CrossRef]

[14] 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, 2011 http://www.sciencedirect.com/science/article/pii/S1084804510001281 http://dx.doi.org/10.1016/j.jnca.2010.07.006[CrossRef]

[15] B. R. Kandukuri, V. R. Paturi and A. Rakshit, "Cloud Security Issues," Proceedings of the 2009 IEEE International Conference on Services Computing, Washington DC, 21-25 September 2009 http://dx.doi.org/10.1109/SCC.2009.84[CrossRef]

[16] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Computer Security Division, IT Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[17] M. Jensen, J. Schwenk, N. Gruschka and L. Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing, Bangalore, 21-25 September 2009

[18] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012 http://www.sciencedirect.com/science/article/pii/S0167739X10002554 http://dx.doi.org/10.1016/j.future.2010.12.006[CrossRef]

[19] F. Gens, "New IDC It Cloud Services Survey: Top Benefits and Challenges," 2009. http://blogs.idc.com/ie/?p=730

[20] C. Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 era," Journal on Telecommunications and High Technology Law, Vol. 8, No. 2, 2010

[21] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[22] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, Vol. 1, Hangzhou, 23-25 March 2012

[23] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security Privacy, Vol. 9, No. 2, 2011 http://dx.doi.org/10.1109/MSP.2010.115[CrossRef]

[24] M. Almorsy, J. Grundy and I. Müller, "An Analysis of the Cloud Computing Security Problem," Proceedings of the 2010 Asia Pacific Cloud Workshop, Australia, 30 November 2010.

[25] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer, Vol. 42, No. 1, 2009 http://dx.doi.org/10.1109/MC.2009.20[CrossRef]

[26] K. Popovic and Z. Hocenski, "Cloud Computing Security Issues and Challenges," Proceedings of the 33rd International Convention in MIPRO, 2010,

[27] D. Jamil and H. Zaki, "Cloud Computing Security," International Journal of Engineering Science and Technology, Vol. 3, No. 4, 2011

[28] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proceedings IEEE in INFOCOM, San Diego, 14-19 March 2010,

[29] A. Lenk, M. Klems, J. Nimis, S. Tai and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Washington DC, 23 May 2009, http://dx.doi.org/10.1109/CLOUD.2009.5071529[CrossRef]

[30] J. Shamsi, M. Khojaye and M. Qasmi, "Data-Intensive Cloud Computing: Requirements, Expectations, Challenges, and Solutions," Journal of Grid Computing, Vol. 11, No. 2, 2013, pp. 281-310. http://dx.doi.org/10.1007/s10723-013-9255-6

[31] M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, Vol. 53, No. 4, 2010, pp. 50-58. http://dx.doi.org/10.1145/1721654.1721672[CrossRef]

[32]. Klyuev Vitaly, Oleshchuk Vladimir. Semantic retrieval: an approach to representing, searching and summarising text documents. Int J Inform Technol Commun Converg 2011

Google Scholar

[33] Nyre Åsmund Ahlmann, Jaatun Martin Gilje. A probabilistic approach to information control. J Internet Technol 2010 Google Scholar

[34] Ling Amy Poh Ai, Masao Mukaidono. Selection of model in developing information security criteria for smart grid security system. J Converg 2011 Google Scholar

[35] National Institute of Standards and Technology. The NIST definition of cloud computing ; 2011.

Google Scholar

[36] Baek Sung-Jin, Park Sun-Mi, Yang Su-Hyun, Song Eun-Ha, Jeong Young-Sik. Efficient server virtualization using grid service infrastructure. J Inform Process Syst 2010 Google Scholar

[37] Gartner: Seven cloud-computing security risks. InfoWorld. 2008 - 07 - 02.

Google Scholar

[38] Cloud Security Front and Center. Forrester Research. 2009 - 11 - 18.

Google Scholar

[39] http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html