Trends and Challenges in Securing Cloud Computing Environments: An Overview of Current Techniques

Waqas Ahmed

ABSTRACT

Cloud computing has changed the way organizations manage their data and applications. It is highly scalable and cost-efficient. Nevertheless, the widespread adoption of cloud services poses significant security challenges in the face of emerging threats, complexities of shared responsibility, and compliance. This study considers current trends in cloud security, from adopting Zero Trust architecture to integrating artificial intelligence and machine learning for advanced threat detection. It discusses the essential techniques—including encryption, access controls, and cloud-related standards—that are being utilized to address vulnerabilities and shield multi-tenant environments. The research highlights the need for a multi-layered approach to security, proper responsibility demarcation, and technological advancement. However, there are still areas for further research, especially in adversarial attacks and defining robust security for hybrid and multi-cloud configurations. The research suggested improved collaboration among stakeholders along with investment in privacy-preserving technologies. This study highlights the importance of continuous innovation and proactive action in securing the dynamic cloud environment.

Keywords: Cloud security, Zero trust architecture, Ai and machine learning, Multi-cloud environments, Data protection techniques

Air University, Islamabad, Pakistan

Correspondence to:
Waqas Ahmed,
waqaskhattak99@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Ahmed W. Trends and Challenges in Securing Cloud Computing Environments: An Overview of Current Techniques. Premier Journal of Computer Science 2024;1:100004

DOI: https://doi.org/10.70389/PJCS.100004

Received: 20 November 2024
Revised: 28 November 2024
Accepted: 30 November 2024
Published: 19 December 2024

Ethical approval: N/a
Consent: N/a
Funding: No industry funding
Conflicts of interest: N/a
Author contribution: Waqas Ahmed – Conceptualization, Writing – original draft, review and editing
Guarantor: Waqas Ahmed
Provenance and peer-review: Commissioned and externally peer-reviewed
Data availability statement: N/a

Introduction

Background

Cloud has become the most worthwhile IT adoption and is expected to grow bigger in all industries. Cloud does not affect only the IT industry, but it is also a revolutionary idea in other industries around the world. There is an increasing demand for cloud services from various industries; hence, technical giants like Google, Microsoft, and Amazon Web Services are working hand in hand to revolutionize the future of large enterprises.[1] More than 90% of global enterprises worldwide today claim to use cloud as part of their business.[2] Financial services companies are the most likely to run in a multi-cloud environment. According to the report, 84% of companies report that their environment uses multiple platforms.[3] Manufacturing companies have some of the most skilled cloud engineers, with 66% of technologists reporting significant experience using one or more cloud platforms. 77% of manufacturing companies use multiple cloud platforms primarily to leverage "best of breed" cloud-native services and improve resiliency.[3] They are also quick to adopt new cloud services. 90% of companies adopt new cloud services before, or as soon as, best practices are established. The technology industry is more than twice as likely to have brand-new cloud talent than other industries surveyed.[3]

The cloud computing market size is estimated at USD 0.68 trillion in 2024 and is expected to reach USD 1.44 trillion by 2029, growing at a CAGR of 16.40% during the forecast period (2024-2029).[4] However, this rapid adoption also introduces challenges, particularly in ensuring the security and integrity of cloud environments, which are increasingly targeted by sophisticated cyberattacks (Figure 1).[5]

Despite these challenges, cloud computing continues to evolve, with organizations increasingly adopting hybrid and multi-cloud strategies to optimize performance and reduce risks.[6] Understanding these trends and challenges is crucial for securing cloud environments and enabling their sustainable growth.

Importance of Security

With the increasing adoption of cloud computing, the secure nature of cloud environments has become an important requirement for organizations. Cloud computing, by design, is inherently vulnerable; since it generally stores data and uses the Internet to access it, cybercriminals can seize such vulnerabilities to jeopardize the confidentiality, integrity, and availability of data.[7] Multi-tenancy compounds these vulnerabilities as multiple users share the same cloud infrastructure, hence expanding the attack surface.[8]

According to the IBM Cost of a Data Breach report, the global average cost of a data breach stands at USD 4.88 million; however, the impact varies significantly from region to region. For example, the average cost of a data breach in the United States is USD 9.36 million, nearly four times higher than it is in India at about USD 2.35 million.[9] In the event of a data breach in an organization, leaking of critical business data—including customer information, financial transactions, intellectual property, and confidential correspondences—can be disastrous to the organization. Securing systems and data with multi-layered protection lies at the core of cloud security.

Research Objectives

The following are the research objectives of the proposed research study.

a. To analyze current trends in cloud computing security, focusing on emerging threats and vulnerabilities affecting cloud environments.
b. To evaluate existing techniques and frameworks to secure cloud computing environments, including encryption, access control, intrusion detection systems, and threat intelligence.

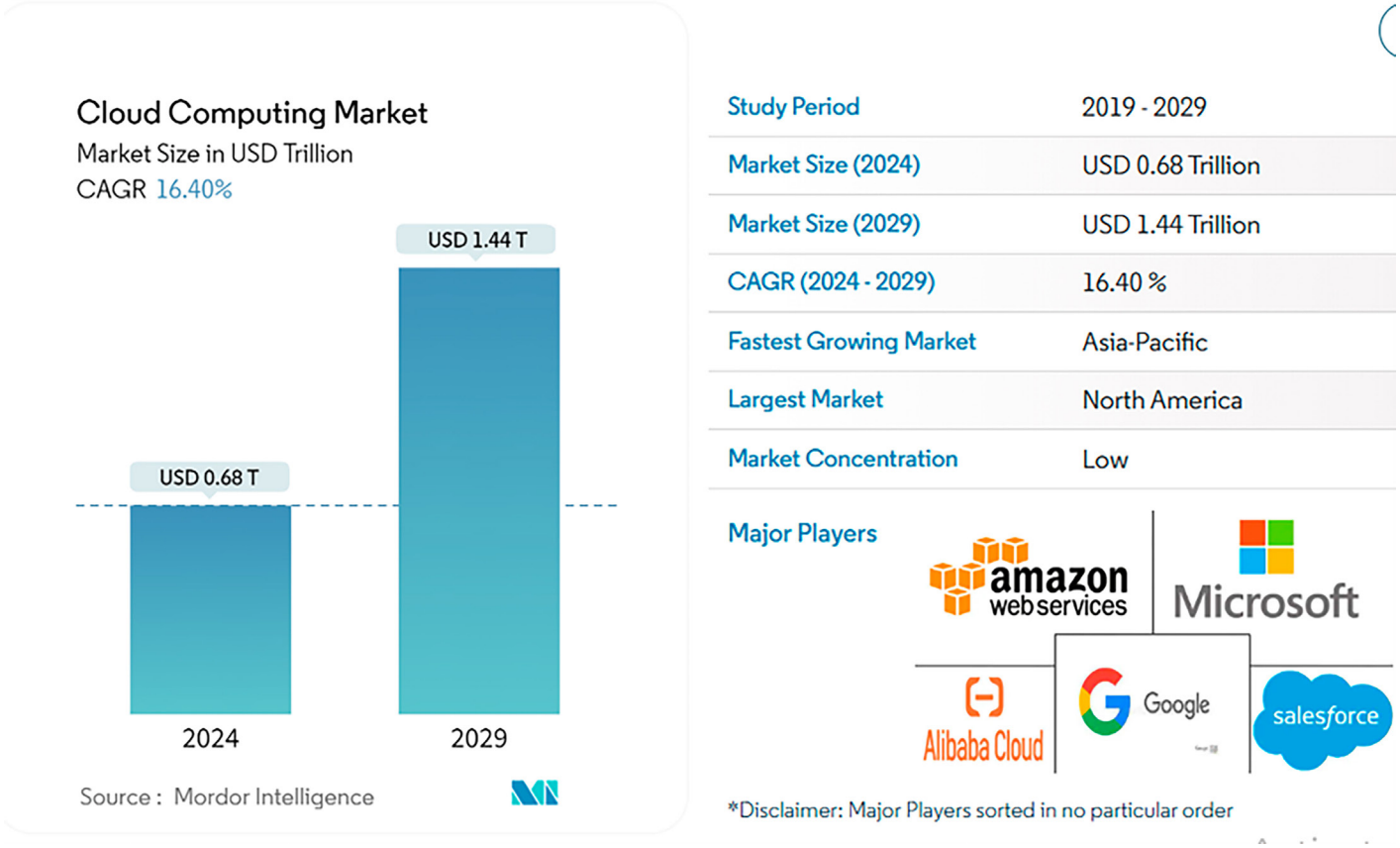

Fig 1 | Cloud computing market4 (market is expected to grow to USD 1.44 T by 2029 with the largest market in North America and major players such as Amazon, Google, and Microsoft)

c. To identify the challenges and gaps in current cloud security measures and propose future directions for improving the protection of cloud environments.

Scope

This article focuses on the existing trends, techniques, and challenges in securing cloud environments. It would particularly focus on emerging threats, advanced security frameworks, and the role of technologies such as artificial intelligence (AI) and Zero Trust architecture (ZTA) while considering shared responsibility and compliance coupled with multi-tenant security concerns.

Current Trends in Cloud Security

Emerging Threats and Vulnerabilities

Cloud computing has rapidly spread and, therefore, rapidly introduces a dynamic and ever-changing threat environment, paving the way for vulnerabilities that challenge the traditional frameworks in place to secure them. Such vulnerabilities are brought about by the rapidly growing complexity of cloud infrastructures, the diversity in users, and the integration of emerging technologies such as AI and IoT.[10]

The most common vulnerability of cloud computing is misconfiguration, accounting for the largest proportion of data breaches. Configuration mistakes, such as insecure buckets for storage or weak access controls, occur due to inadequate knowledge of cloud security tools or a failure to apply best practices. Studies show that 88% of cloud environment breaches result from such mistakes; hence, there is a need for better scrutiny and training in cloud security.[11,12] A well-known example of this weakness is the Capital One data breach in 2019, in which a misconfigured web application firewall allowed an attacker to exploit a vulnerability and access over 100 million customers' sensitive data.[47]

Insider threats also represent a significant challenge in cloud environments, especially where shared access to resources is expected. The lack of robust monitoring and identity management policies exacerbates the risks associated with insider threats, making it imperative for organizations to implement stringent access controls and activity logging.[13]

Ransomware and malware attacks contribute to additional risks associated with cloud computing. Attackers encrypt or exfiltrate data by exploiting vulnerabilities, demanding a ransom for its release. Ransomware attacks in cloud systems experienced a 105% surge in 2023, with attackers targeting backup repositories and cloud storage services often.[14]

The cloud environment with a multi-tenant model that allows several customers to utilize the same infrastructure is more susceptible to data leakage

DOI: https://doi.org/10.70389/PJCS.100004 | Premier Journal of Computer Science 2024;1:100004

and cross-tenanted attacks. Security breaches in one tenant's environment can potentially impact other tenants, hence increasing the risks of operation in shared infrastructures.[15] Supply chain vulnerabilities in the cloud environment have also emerged as a growing source of concern, as attackers use third-party dependencies and integrations for their exploitations. The SolarWinds breach in 2020 is a stark example in which the compromised software updates were used to infiltrate cloud networks globally.[16]

Emerging technologies such as AI and IoT introduce new security challenges in cloud environments. AI systems are prone to adversarial attacks that could corrupt data or manipulate machine learning models, thus producing biased or faulty decision-making processes.[17] Similarly, IoT devices often lack robust security measures, making them easy targets for attackers seeking entry points into cloud systems.[18]

Adoption of Zero Trust Models

Zero Trust cloud security adopts the principle that no one should be trusted—whether it is a user, a device, a system, or an action, regardless of whether it is on an entity's network. This approach lowers the risk of breaches and other cyber threats by limiting access to sensitive information and resources against the user role, or the security posture of the device from where it is accessed, based on contextual factors (Figure 2).[20]

The advent of the cloud, however, means that data and applications are distributed across multiple services and locations, which makes it difficult to maintain uniform security. 91% of organizations around the world have adopted a new security strategy. They have opted for the adoption of advanced technologies such as Zero Trust solutions, AI-driven threat detection, and enhanced data encryption protocols to better protect their data and assets against evolving cyber threats.[21]

Therefore, identity and access management is a core element of a Zero Trust model. Commonly employed techniques include multi-factor authentication (MFA), behavioral analytics, and least privilege access that enforce Zero Trust. For instance, with MFA, organizations will authenticate users with adequate factors, such as passwords and biometric scans, making it significantly harder for attackers to gain access.[22] Furthermore, least-privilege access controls the number of rights that are required by users and applications to perform duties to ensure that damage from a compromised account is minimized.[23]

Zero Trust integrated into a cloud environment is demonstrated to improve security as well as the operational efficiency of an organization. It allows for more granular access control, meaning their attack surface is minimized, and once a breach does occur, it is difficult for the attacker to move laterally within the network.[24] Forrester lists that among organizations with Zero Trust model implementations, 64% reported a significant improvement in their security posture due to the model implementation.[25]

Zero Trust also comes with its own set of challenges. The deployment of such a model involves a deep transformation in IT infrastructure, workflows, and security practices. According to Kang et al,[26] implementing Zero Trust is resource-intensive and can be difficult for organizations that have already developed legacy systems and traditional security models. Zero Trust models also use micro-segmentation to isolate workloads, limiting the spread of attacks. Despite its benefits, adopting Zero Trust requires significant investment in infrastructure and training, which can pose challenges for smaller organizations.

Integration of AI and ML

The potential exists in AI and ML for actual real-time threat detection, automated response, and continuous adaptation to evolving security challenges (Figure 3).[27]

One of the main applications of AI and ML in cloud security is anomaly detection. Patterns in cloud usage data, which include user behavior, network traffic, and the utilization of resources, can be analyzed by

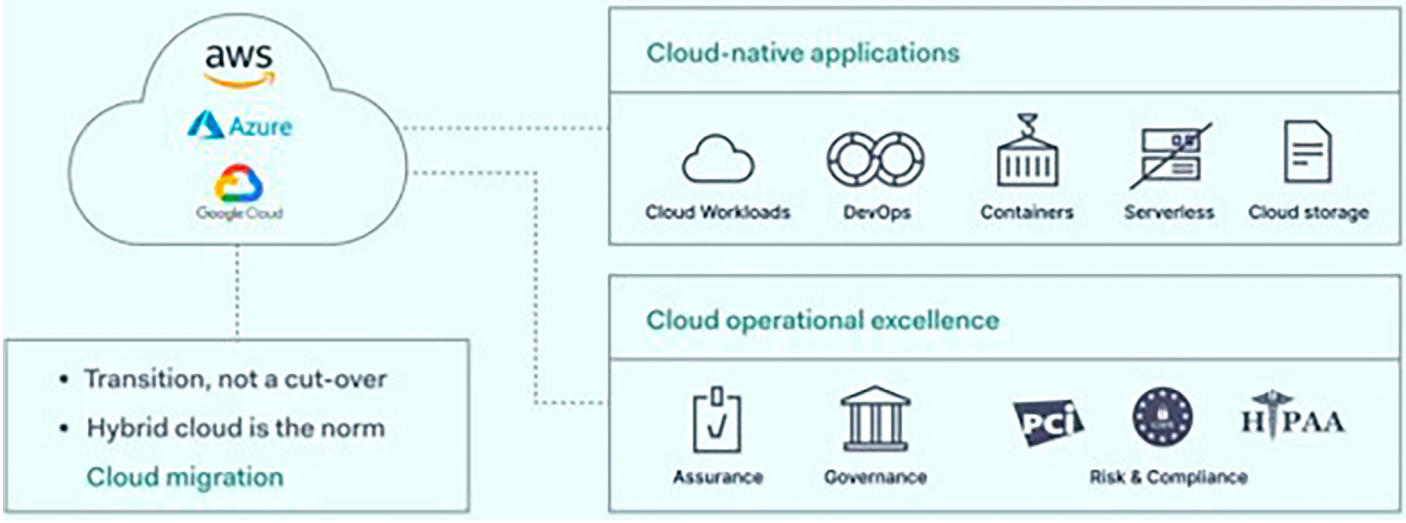

Fig 2 | Why the Cloud Zero Trust model?19 Zero Trust came about as the security model eliminating implicit trust in any connection: internal or external. The figure indicates that Zero Trust model integrates cloud applications to reduce cyber threats

Fig 3 | Integration of AI and ML in cloud security27 AI and ML have emerged as powerful tools in this context, offering

machine learning algorithms to identify any deviation that could describe a potential threat.[27] Deep learning models can identify zero-day threats based on deviations from baseline behavior without predefined signatures. Their effectiveness, however, is only as good as the quality and diversity of training data. Poor or biased data leads to false positives: security teams get bogged down by too many unnecessary alerts or false negatives, where threats go unnoticed.[28]

Another highly advancing feature is AI-powered threat intelligence. Based on various data analyses, monitoring dark web activities, and global threat feeds, AI-powered systems predict the potential threats and block them before they impact cloud systems. This predictive ability greatly enhances the security postures of organizations and allows them to respond to threats faster than ever before.[29]

Further, AI and ML contribute to automated incident response in cloud environments. These technologies help systems respond to identified threats autonomously while isolating affected resources, blocking malicious IP addresses, or revoking compromised credentials. Such automation minimizes human intervention, reduces response times, and swiftly mitigates threats.[30]

In addition, AI and ML in cloud security also lead to problems. These technologies entirely depend on a quality dataset for training and performance improvement. Low-quality or biased data could easily generate false positives or negatives, affecting the security systems' credibility. Integrating AI/ML with Zero Trust models further enhances security by automating identity verification and continuously assessing user and device behavior, creating a layered defense against sophisticated threats.[31]

Techniques for Securing Cloud Environments

Data Protection Techniques

Data protection forms an integral part of cloud security. It guards against unauthorized access, data breaches, and loss. Techniques that are usually employed in securing sensitive information include encryption, tokenization, as well as data masking. Encryption converts data into unreadable forms while it is either at rest or in motion to ensure that it is accessible only through the correct decryption keys. Advanced encryption standards, such as AES-256, are commonly employed in cloud environments to protect sensitive data.[32] The management of encryption keys introduces significant complexity; compromised keys can render even the most secure systems vulnerable. Furthermore, encryption is computationally intensive, which can impact performance in large-scale cloud operations.[32]

Tokenization substitutes sensitive data with non-sensitive tokens that can be processed without actually exposing information. This is useful for complying with data privacy regulation laws such as GDPR and PCI DSS. Data masking, however, involves changing data in a form that makes sensitive information in it nonsensitive; thus, organizations are allowed to use it in testing or development without risking exposure.[33]

Access Control Mechanisms

The access control mechanisms are fundamental to the limitation of unauthorized access to cloud resources and data. Two models commonly used are (1) *role-based access control*, in which the assignment of permissions is done based on a user's role, and any individual can only access the resources needed for his or her role, and (2) *attribute-based access control*, which is more granular—as it reviews attributes in terms of user location, device type, and time of access to be granted permission—and much more flexible.[34]

The implementation of MFA further strengthens access controls by requiring multiple credentials for user authentication. Combining passwords, biometric data, and physical tokens ensures that even if one factor is compromised, unauthorized access remains difficult.[35]

Threat Detection and Response

Advanced threat detection and response mechanisms are a must to handle and mitigate threats in cloud environments. IDS and IPS are applied in various ways to track the indication of malicious activity in network traffic. Machine learning algorithms are increasingly used in these systems for enhanced detection accuracy as well as to identify unknown threats.[36] EDR solutions extend security to devices that access cloud systems by providing visibility into potential threats and allowing for automated responses to contain breaches. Security information and event management platforms further

DOI: https://doi.org/10.70389/PJCS.100004 | Premier Journal of Computer Science 2024;1:100004

enhance threat detection capabilities by collecting and analyzing logs and events from multiple sources and providing a centralized view of the security landscape.[37]

This proactive threat hunting complements these automated systems by employing human analysts to seek out threats that may elude detection. The strategy makes use of experience and intelligence gathered through global threat databases to uncover and neutralize advanced attacks.[38]

Cloud-Specific Standards and Compliance

For organizations in regulated industries, compliance with cloud-specific standards is of prime importance. Standards relating to cloud-specific security controls specifically speak to the protection of customer data and customer privacy, such as ISO/IEC 27017 and ISO/IEC 27018.[39] That an organization adheres to standards shows a commitment to following strong security practices. The Cloud Security Alliance developed the Cloud Controls Matrix (CCM), a framework designed to help organizations assess and manage cloud-specific risks. The CCM maps security controls to significant industry standards, such as GDPR, NIST, and HIPAA, helping streamline compliance efforts and mapping with regulatory requirements.[40]

Challenges in Securing Cloud Computing Environments

Complexity of Shared Responsibility

One of the primary challenges that cloud security faces is the complexity of the shared responsibility model. There are issues of shared responsibility regarding security as cloud providers and customers share security responsibilities. Providers manage the security of the cloud infrastructure, while customers have to ensure protection in the cloud for data, applications, and access controls. Still, this often leads to misunderstandings and gaps in security coverage.[41]

For instance, while a cloud provider would ensure that the physical and network security measures are robust, the customer must configure the access controls and secure their data. Most commonly, misconfigurations and failure to limit access to storage buckets or databases make it easy for data breaches to occur in cloud environments.[42]

Scalability and Resource Constraints

Due to their dynamic nature, cloud environments have resources and workloads scaling up or down with regard to demand. There arises a challenge for security, mainly because most traditional tools and strategies fail to adapt to the constantly changing nature of cloud infrastructure. Small and medium-sized enterprises usually face resource constraints, thereby limiting the degree to which comprehensive security measures can be implemented.[43]

Scalable security solutions, such as automated threat detection systems and elastic firewalls, become necessary to overcome this challenge. However, these solutions are often expensive and require deep domain expertise, which not all organizations can afford. The ever-increasing velocity with which components scale within a cloud environment also opens up the attack surface, as it requires real-time response capabilities to maintain a healthy security posture.[44]

Regulatory and Compliance Issues

One significant challenge with cloud security lies in compliance with regulatory standards, particularly for multi-jurisdictional business operations. Requirements for storage, processing, and transferring sensitive data under GDPR, HIPAA, and CCPA can be extremely strict. Moreover, it is quite complex to navigate the regulations in the cloud as data might be stored across various locations and jurisdictions without the knowledge of the explicit customer.[45]

Organizations must work with cloud providers to ensure that the latter adhere to relevant standards and frameworks, such as ISO/IEC 27001 or SOC 2. In an important sense, relying on third-party compliance opens other risks, which arise from a lack of transparency concerning the provider's internal processes. Non-compliance may bring significant penalties and damage to an organization's reputation, and it emphasizes the need to address regulatory challenges in cloud security.[46]

Security of Multi-Tenant Environments

The multi-tenancy nature of cloud environments, where a large number of customers are hosted on a shared physical infrastructure, exposes them to specific security threats. Even though virtualization and isolation mechanisms prevent cross-tenant data breaches by the cloud provider, vulnerabilities in these mechanisms can expose sensitive information to other tenants.[47]

For example, side-channel attacks, which exploit the common hardware resources shared between tenants to extract information from other tenants, could be a significant form of threat within multi-tenancy in a cloud computing environment. Further, a malicious insider in one tenant organization could exploit some loopholes to attack the neighboring tenants.[47]

Future Directions

Recommendations for Improving Cloud Security

Organizations need to adapt to a ZTA in cloud computing environments to improve their security. This kind of model focuses on strict access control, continuous monitoring, and verification of all devices and users from any location.[36] Integrating AI and ML in security operations is another approach to achieving improved threat detection and automating incident responses to reduce response time and mitigate risk.[29]

Improvements in cloud misconfiguration management must be combined with the proper utilization of automated tools to identify and remediate configuration errors in real time. Training programs can reduce human errors in security breaches by improving training for IT professionals and end-users.[42]

Collaboration between cloud providers, customers, and regulatory bodies is significant in solving compliance problems. To show commitment to security issues, the providers should furnish clear information on data storage and processing locations and embrace industry standards such as ISO/IEC 27001 and SOC 2.[46]

Research Gaps

Despite these developments, several research gaps remain in cloud security. First, few studies were made on adversarial attacks that target AI and ML systems integrated into cloud environments; instead, their vulnerabilities need robust and resilient AI models.[17] One of the potential solutions is through adversarial training models, where algorithms are trained on simulated attack scenarios to increase their robustness. In addition, the integration of XAI into cloud security systems will allow for more transparency in AI decision-making, thus helping security teams to detect anomalies more effectively and understand possible manipulation attempts.

The effectiveness of security strategies in multi-cloud and hybrid cloud environments is largely unexplored. Organizations are increasingly adopting these architectures, so tailored security frameworks and solutions are needed.[38] Organizations could benefit from adopting a federated security model, where a centralized control plane oversees security policies across all environments, ensuring consistency and interoperability.

Lastly, there is a lack of research on privacy issues in multi-tenant environments, particularly data isolation and cross-tenant vulnerabilities. Innovative approaches such as homomorphic encryption and secure multi-party computation may also offer promising solutions.[44]

Conclusion

Summary of Findings

The following are the key takeaways of this study:

- Complexity of Threats: Misconfigurations, insider risks, advanced attacks on shared infrastructure, and AI-integrated systems threaten diverse cloud environments.
- Multi-layered Approach: Security strategies should integrate robust techniques such as encryption, access controls, ZTA, and real-time threat detection to address vulnerabilities.
- Shared Responsibility: This requires a clear understanding and implementation of the shared responsibility model. The end-to-end security assurance is implemented jointly by both the cloud service providers and customers.
- Compliance Challenges: The regulatory and privacy issues increase stakeholders' awareness of the need to cooperate candidly, follow established standards, and innovate to meet compliance worldwide.
- Technological Integration: Emerging technologies such as AI and ML are transforming threat detection and response capacity but pose new challenges, such as adversarial attacks.

Implications

The study highlights that a multi-layered security approach with advanced technologies like ZTA, AI, and ML should be devised to better assist cloud security. Coordination and cooperation between cloud providers and users, along with effective regulatory frameworks, are necessary to ensure utmost cloud security and compliance. Besides, autonomic tools and training programs can help prevent or eliminate misconfigurations and human errors, thereby strengthening the cloud system's security posture.

Future Work

Future research should focus on developing robust defense mechanisms against adversarial attacks in AI-driven security systems. The hybrid (on-premises and cloud) and multi-cloud (using services from multiple cloud providers) environments increase complexity in securing data and applications. Future frameworks should highlight unified security policies and centralized management systems that operate across different platforms without a hitch.

For example, a conceptual model can include:

- Federated Identity Management Systems: They enable users to access the resources of other cloud services through single credentials and with fine-grained access controls in place.
- Interoperable Encryption Mechanisms: Data encrypted in one cloud environment should remain secure and readable when transferred to another provider.
- Automated Compliance Engines: Continuously monitors compliance and enforces a given set of regulatory standards across multi-cloud deployment.

References

1 Prasad A. Cloud adoption across industries – A perspective [Internet]. MSR Cosmos. 2022 [cited 2024 Nov 20]. Available from: https://www.msrcosmos.com/blog/cloud-adoption-across-industries-a-perspective/
2 Mukherjee A. Impact of cloud computing in different industries [Internet]. www.infiflex.com. 2023. Available from: https://www.infiflex.com/impact-of-cloud-computing-in-different-industries
3 Pluralsight Content Team. How are different industries using cloud tech in 2023? [Internet]. Pluralsight.com. 2023 [cited 2024 Nov 20]. Available from: https://www.pluralsight.com/resources/blog/software-development/industry-verticals-cloud-computing-2023
4 Mordor Intelligence. Cloud computing market size & share analysis – industry research report – growth trends [Internet]. www.mordorintelligence.com. 2024. Available from: https://www.mordorintelligence.com/industry-reports/cloud-computing-market
5 Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Comput. 2018;22(2):42–51.
6 Tozzi C. Why supercloud architectures could upend cloud computing – or not | IDC Blog [Internet]. Idc.com. 2024 [cited 2024 Nov 20]. Available from: https://blogs.idc.com/2024/07/01/why-supercloud-architectures-could-upend-cloud-computing-or-not/

7 Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Comput Security [Internet]. 2021;114:102580. Available from: https://www.sciencedirect.com/science/article/pii/S0167404821003977
8 Liu Z, Xu B, Cheng B, Hu X, Darbandi M. Intrusion detection systems in the cloud computing: a comprehensive and deep literature review. Concurr Comput Pract Expe. 2021;34(4). DOI:10.1002/cpe.6646
9 SentinelOne. Why is cloud security important? [Internet]. SentinelOne. 2024. Available from: https://www.sentinelone.com/cybersecurity-101/cloud-security/why-is-cloud-security-important/
10 Ashraf M, Shah M, Ilyas I. A survey on data security in cloud computing using blockchain: challenges, existing state of the art methods, and future directions [Internet]. 2021. Available from: https://core.ac.uk/download/pdf/539886665.pdf
11 Pansy. 80 + cloud security statistics to know for 2024 [Internet]. Sprinto. 2024. Available from: https://sprinto.com/blog/cloud-security-statistics/
12 IBM. Cost of a data breach 2024 [Internet]. IBM. 2024. Available from: https://www.ibm.com/reports/data-breach
13 Chitreddy K, Anthony AM, Bandaru CM, Abiona O. Information security in the cloud: emerging trends and challenges. Int J Commun Netw Syst Sci. 2024;17(05):69–80.
14 Gihon S. Ransomware trends Q4 2023 report [Internet]. Cyberint. 2024. Available from: https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/
15 Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw [Internet]. 2015;76:146–64. Available from: http://tarjomefa.com/wp-content/uploads/2016/07/5009-English.pdf
16 Marelli M. The SolarWinds hack: lessons for international humanitarian organizations. Int Rev Red Cross. 2022;104(919):1–18.
17 Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples [Internet]. arXiv.org. 2014. Available from: https://arxiv.org/abs/1412.6572
18 Kolias C, Meng W, Kambourakis G, Chen J. Security, privacy, and trust on Internet of Things. Wirel Commun Mobile Comput. 2019;2019:1–3.
19 NordLayer. What is Zero Trust for the cloud? | NordLayer Learn [Internet]. nordlayer.com. 2024. Available from: https://nordlayer.com/learn/zero-trust/cloud-security/
20 Ahmadi S. Zero Trust architecture in cloud networks: application, challenges and future opportunities [Internet]. Ssrn.com. 2024. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4725283
21 Martinez J. What is Zero Trust for the cloud? (and why it's important) [Internet]. Strongdm.com. StrongDM, Inc.; 2024 [cited 2024 Nov 20]. Available from: https://www.strongdm.com/blog/zero-trust-cloud
22 EDO OC, Tenebe T, Etu E, Ayuwu A, Emakhu J, Adebiyi S. Zero Trust architecture: trend and impact on information security. Int J Emerg Technol Adv Eng. 2022;12(7):140–7.
23 Azad MA, Abdullah S, Arshad J, Lallie H, Ahmed YH. Verify and trust: a multidimensional survey of zero-trust security in the age of IoT. Internet Things. 2024;101227–7.
24 Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of Zero Trust networks in cloud computing: a comparative review. Sustainability [Internet]. 2022;14(18):11213. Available from: https://www.mdpi.com/2071-1050/14/18/11213/htm
25 Forrester. Zero Trust security: the business benefits and advantages [Internet]. Forrester. 2024. Available from: https://www.forrester.com/zero-trust/
26 Kang H, Liu G, Wang Q, Meng L, Liu J. Theory and application of Zero Trust security: a brief survey. Entropy [Internet]. 2023;25(12):1595. Available from: https://www.mdpi.com/1099-4300/25/12/1595
27 Abdel-Wahid T. AI-powered cloud security: A study on the integration of artificial intelligence and machine learning for... [Internet]. ResearchGate. Unknown; 2024. Available from: https://www.researchgate.net/publication/383095008_AI-POWERED_CLOUD_SECURITY_A_STUDY_ON_THE_INTEGRATION_OF_ARTIFICIAL_INTELLIGENCE_AND_MACHINE_LEARNING_FOR_IMPROVED_THREAT_DETECTION_AND_PREVENTION
28 Wang S, Balarezo JF, Kandeepan S, Al-Hourani A, Chavez KG, Rubinstein B. Machine learning in network anomaly detection: a survey. IEEE Access [Internet]. 2021;9:152379–96. Available from: https://ieeexplore.ieee.org/document/9610045
29 Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2016;18(2):1153–76.
30 Reddy A. Automating incident response: AI-driven approaches to cloud security incident management [Internet]. 2020. Available from: https://www.researchgate.net/publication/379219509_AUTOMATING_INCIDENT_RESPONSE_AI-DRIVEN_APPROACHES_TO_CLOUD_SECURITY_INCIDENT_MANAGEMENT
31 Prakash S, Malaiyappan JNA, Thirunavukkarasu K, Devan M. Achieving regulatory compliance in cloud computing through ML. Adv Int J Multidiscipl Res [Internet]. 2024;2(2). Available from: https://www.aijmr.com/papers/2024/2/1038.pdf
32 NIST. Cryptographic standards and guidelines development process | CSRC [Internet]. Nist.gov. 2020. Available from: https://csrc.nist.gov/Projects/crypto-standards-development-process
33 Tabrizchi H, Rafsanjani MK. A survey on security challenges in cloud computing: Issues, threats, and solutions. J Supercomput [Internet]. 2020;76(12):9493–532. Available from: https://link.springer.com/article/10.1007/s11227-020-03213-1
34 Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to attribute based access control (ABAC) definition and considerations. Guide to attribute based access control (ABAC) definition and considerations [Internet]. 2014; Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf
35 Moulds K. Unlocking the benefits of multi-factor authentication for enhanced cyber security [Internet]. Intercede. 2024. Available from: https://www.intercede.com/unlocking-the-benefits-of-multi-factor-authentication-for-enhanced-cyber-security/
36 Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity [Internet]. 2019;2(1):1–22. Available from: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7
37 Akitra. Security information and event management (SIEM): Centralized threat monitoring and analysis [Internet]. Medium. 2024 [cited 2024 Nov 20]. Available from: https://medium.com/@akitrablog/security-information-and-event-management-siem-centralized-threat-monitoring-and-analysis-9b70d922bb7e
38 Mahboubi A, Luong K, Aboutorab H, Bui HT, Jarrad G, Bahutair M, et al. Evolving techniques in cyber threat hunting: A systematic review. J Netw Comput Appl. 2024;104004–4.
39 ISMS. ISO/IEC 27017 Standard for cloud security controls and cloud services [Internet]. ISMS.online. 2021. Available from: https://www.isms.online/iso-27017/
40 CSA. What is the cloud controls matrix (CCM)? | CSA [Internet]. cloudsecurityalliance.org. 2020. Available from: https://cloudsecurityalliance.org/blog/2020/10/16/what-is-the-cloud-controls-matrix-ccm
41 Understanding the shared responsibility model for SaaS Applications | Metomic [Internet]. Metomic.io. 2022 [cited 2024 Nov 20]. Available from: https://www.metomic.io/resource-centre/the-shared-responsibility-model-for-saas-applications
42 Chou TS. Security threats on cloud computing vulnerabilities. Int J Comput Sci Inf Technol. 2013;5(3):79–88.
43 Varghese B, Buyya R. Next generation cloud computing: new trends and research directions. Future Gen Comput Syst. 2018;79(3):849–61.
44 Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Compu Appli. 2011;34(1):1–11.
45 Butt UA, Mehmood M, Shah SBH, Amin R, Shaukat MW, Raza SM, et al. A review of machine learning algorithms for cloud computing security. Electronics [Internet]. 2020;9(9):1379. Available from: https://www.mdpi.com/2079-9292/9/9/1379
46 Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gen Comput Syst [Internet]. 2019;28(3):583–92. Available from: https://www.sciencedirect.com/science/article/pii/S0167739X10002554
47 Khan S, Kabanov I, Hua Y, Madnick S. A systematic analysis of the CapitalOne data breach: critical lessons learned. ACM Trans Privacy Security [Internet]. 2022;26(1). Available from: https://dl.acm.org/doi/10.1145/3546068