Navigating the Cybersecurity Landscape in Cloud Computing: Challenges, Strategies, and Future Directions

Milad Akbari
DITEN – University of Genoa
Genoa, Italy
milad.akbari@edu.unige.it

Roberto Bruschi
DITEN – University of Genoa
CNIT – S2N National Lab
Genoa, Italy
roberto.bruschi@unige.it

Alessandro Carrega
DITEN – University of Genoa
CNIT – S2N National Lab
Genoa, Italy
alessandro.carrega@unige.it

***Abstract*—As the adoption of cloud computing accelerates across various sectors, the associated cybersecurity vulnerabilities and risks have become increasingly pronounced. This paper delves into the intricate relationship between cloud computing and cybersecurity, emphasizing the need for robust security frameworks to address emerging threats and vulnerabilities. It provides a comprehensive overview of cloud computing models, including public, private, community, and hybrid clouds, and their respective security implications. The study highlights critical cybersecurity challenges such as data security, network security, infrastructure security, and compliance, underscoring the importance of a multi-layered security approach that incorporates advanced technologies like AI and machine learning. Furthermore, the paper reviews recent literature to identify gaps in current research and offers a comparative analysis of recent studies while proposing a structured taxonomy of cloud security challenges and solutions, highlighting unaddressed areas and guiding future research directions. By fostering a deeper understanding of these issues, organizations can better navigate the complexities of securing cloud environments while leveraging its benefits.**

Keywords—Cloud computing, Cloud security, Cybersecurity, Cloud computing cybersecurity, Cyber threats.

I. INTRODUCTION

Cloud computing is a revolutionary technological model that delivers shared computing resources such as processing power, storage, and networking as a utility over the internet. This approach allows organizations to access Information Technology (IT) infrastructure with greater flexibility, eliminating the need for large capital investments in physical hardware. As a result, cloud computing has become an essential platform across various sectors including industry, academia, business, and online platforms. It enables users to utilize a range of services, tools, and applications customized to their specific needs [1]-[4].

The primary benefit of cloud computing lies in its scalability, agility, and cost-efficiency. Organizations can dynamically adjust resource usage on demand, paying only for what they consume. This adaptability not only reduces operational costs but also improves business responsiveness to market changes. The ability to scale quickly and effectively enhances overall performance, fosters innovation, and enables data-driven decision-making. organizations can optimize operations, uncover new growth opportunities, and remain competitive in fast-evolving markets [5]-[7]. Moreover, cloud computing serves as a foundation for emerging technologies such as Artificial Intelligence (AI), big data analytics, and the Internet of Things (IoT). These technologies generate and process vast volumes of data, which cloud platforms can manage efficiently due to their scalable nature. Cloud infrastructure supports real-time data processing and decision-making, making it crucial for organizations aiming to leverage advanced digital tools [8]-[10].

However, the widespread adoption of cloud services brings significant cybersecurity challenges. As organizations migrate their data and applications to the cloud, the risk of cyber threats increases. Cloud environments, by nature, introduce a larger attack surface, exposing sensitive data to threats such as data breaches, ransomware, insider attacks, misconfigurations, and Distributed Denial-of-Service (DDoS) attacks. These threats can lead to data loss, reputational harm, financial losses, and legal consequences, especially under stringent data protection regulations like the General Data Protection Regulation (GDPR) [11]-[14]. To mitigate modern cyber threats, a multi-layered security approach is essential. This includes strong encryption, Multi-Factor Authentication (MFA), continuous monitoring, and regular vulnerability assessments. Real-time threat detection and quick incident response mechanisms are critical in identifying and neutralizing threats before they cause significant damage. Emerging frameworks like Zero Trust Architecture (ZTA) emphasize the principle of "never trust, always verify," enforcing strict access controls and minimizing potential internal and external threats [15]-[17]. Organizations must also recognize the human element in cybersecurity. Social engineering and phishing attacks often take advantage of human error, which is why employee training and awareness are essential parts of any solid security strategy. Promoting a security-first mindset, carrying out regular audits, and taking a proactive approach to threats are all important steps in reducing risk and strengthening overall protection. Additionally, AI and machine learning are increasingly used in cloud security to analyze behavior patterns, detect anomalies, and predict potential threats. These AI-driven systems enhance threat intelligence and provide more proactive security management. Automation, along with continuous monitoring, reinforces the stability and reliability of cloud infrastructures [18]-[21].

The remainder of this paper is structured as follows: Section 2 overviews the fundamental concepts of cloud computing and cybersecurity. Section 3 examines key cybersecurity challenges in cloud environments, including major threats, vulnerabilities, and security concerns. Section 4 reviews the current state of the art, covering recent advancements, security frameworks, and technologies for risk mitigation. Section 5 presents results and analysis, highlighting trends, research findings, and their implications for cloud security. Finally, Section 6 concludes by

979-8-3315-0196-9/25/$31.00 ©2025 IEEE

summarizing key takeaways and identifying future research directions, emphasizing the ongoing need for innovation in securing cloud environments.

II. Fundamentals

As cloud computing continues to expand across various sectors, its widespread adoption brings significant benefits but also raises growing concerns about cybersecurity threats. The increasing reliance on cloud-based services exposes cloud users to a broader threat landscape, where data breaches, unauthorized access, and service disruptions can have serious consequences. To effectively safeguard digital assets and maintain trust in cloud environments, it is essential to first understand and implement the core principles of cloud computing architecture and cybersecurity [22]-[24].

A. Cloud computing

According to the National Institute of Standards and Technology (NIST) [25], cloud deployment is categorized into four main models: *i) Public cloud*, that is a cloud deployment model where the infrastructure is made available for use by the public. It is owned, managed, and operated by a third-party provider. Public cloud services are hosted on the provider's infrastructure and are accessible to individuals and organizations over the internet; *ii) Private cloud*, which is designed for the exclusive use of a single organization, serving multiple internal users such as different business units. The infrastructure can be owned, managed, and operated by the organization, a third-party provider, or jointly by both. This model offers enhanced security, greater control over resources, and customization options, making it ideal for businesses with strict regulatory requirements or specialized computing needs; *iii) Community cloud*, that is designed for the exclusive use of a specific group of organizations that share common concerns, such as security, research, or application needs. Community clouds can be viewed as a cluster of private clouds, offering the benefits of resource sharing while ensuring greater control, compliance, and operational efficiency for participating organizations; and *iv) Hybrid cloud*, it combines two or more distinct cloud infrastructures such as private, public, or community clouds while maintaining their individual identities. These infrastructures are interconnected using standardized or proprietary technology, allowing seamless data and application portability between them. Hybrid cloud is ideal for businesses that require the security and control of a private cloud while benefiting from the scalability and cost-effectiveness of a public cloud.

Additionally, based on the NIST cloud computing reference architecture [26], cloud computing is structured around three primary service models: *i) Software as a Service (SaaS)*, it delivers software applications over the internet on a subscription basis, eliminating the need for users to install, maintain, or manage software on their local devices. SaaS providers host applications on their cloud infrastructure, handling updates, security, and maintenance, allowing users to access them anytime, anywhere, through web browsers, mobile applications, Application Programming Interfaces (APIs); *ii) Platform as a Service (PaaS)*, it provides a platform allowing users to build, deploy, and manage applications without managing the underlying infrastructure. PaaS providers offer a set of tools, programming languages, libraries, and services that facilitate application development, while taking care of the servers, storage, and networking. This model enables developers to focus on program development, without worrying about hardware or system updates; and *iii) Infrastructure as a Service (IaaS)*, offers users on-demand access to essential computing resources such as processing power, storage, and networking. IaaS enables consumers to deploy and manage various software, including operating systems and applications, without the responsibility of managing the underlying physical infrastructure. The cloud provider handles the physical hardware and its maintenance, while users retain control over virtualized resources like operating systems, storage, and applications.

Organizations can select the most suitable deployment model based on factors such as security, scalability, cost, and operational flexibility, while also considering regulatory compliance, workload requirements, and resource management preferences to align with their goals and technical needs. Additionally, they can choose the most appropriate service model based on their operational needs, technical expertise, and resource management preferences [25]-[28].

B. Cybersecurity

Confidentiality, Integrity, and Availability (CIA) triad represents the core principles of cybersecurity, ensuring the protection of digital assets and maintaining trust in cloud environments. These principles include: *i) Confidentiality*, it ensures that sensitive data is only accessible to authorized users and systems, preventing unauthorized access or disclosure; *ii) Integrity*, it guarantees that data is accurate, complete, and trustworthy by preventing unauthorized modifications or tampering. It guarantees that information remains consistent and unaltered unless authorized; and *iii) Availability*, it Ensures that data and systems are accessible and operational when needed, allowing authorized users to access resources without interruptions. It involves minimizing downtime and ensuring reliable access to information and services. The CIA triad covers key principles of information security, protecting sensitive data from unauthorized access, tampering, and loss. Together, these principles form a strong foundation for securing digital assets in a complex threat landscape [23]-[24].

Alongside the CIA triad, it is essential to define the following concepts: *i) Authentication*, is the process of verifying the identity of a user, device, or system to ensure that they are who they claim to be. This is typically done through methods like usernames, passwords, biometrics, or MFA; *ii) Authorization*, is the process of granting or denying access to specific resources or actions based on the authenticated identity. After authentication, authorization ensures that the user or system has the appropriate permissions to access or perform certain tasks; and *iii) Risk management*, is the systematic process of identifying, assessing, prioritizing, and mitigating risks that may negatively affect an organization's assets, operations, or reputation. In the context of cybersecurity, it involves evaluating potential threats like hacking, malware, or insider threats and vulnerabilities such as system weaknesses, outdated software and determining how to reduce or eliminate their impact. By risk management organizations can minimize the severity of security breaches [16], [19], [23].

III. Key cloud cybersecurity challenges

This section introduces the main cybersecurity challenges associated with cloud computing, highlighting the risks that arise from increased data exposure, shared infrastructure, and complex cloud configurations. It also explores the evolving threat landscape and the need for robust security strategies to protect cloud environments.

A. *Data security and privacy*

As In the cloud era, data security and privacy are more important than ever. Organizations must protect sensitive information from unauthorized access, breaches, and misuse, while also ensuring that personal and corporate data is handled responsibly and in line with privacy laws. Techniques like encryption, access control, and data masking help keeping information safe both when it is stored and when it is being transferred [23].

Privacy goes a step further by emphasizing how data is collected, used, and shared, making compliance with regulations such as GDPR and California Consumer Privacy Act (CCPA) essential. Since cloud data is often spread across various locations, providers and companies need clear policies to stay in control. Strong data governance and regular risk assessments help ensure that data stays private, secure, and used in ways that people can trust [14].

B. *Network security*

Network security in cloud computing involves a comprehensive set of policies, tools, and practices designed to protect cloud environments from threats across different networks. It involves technologies like firewalls, Intrusion Detection and Prevention Systems (IDS/IDPS), Virtual Private Networks (VPNs), and secure communication protocols to defend against unauthorized access and data breaches. Cloud providers also implement protection against DDoS attacks to maintain service availability and prevent disruptions. Secure network virtualization and micro-segmentation further enhance network isolation and control, helping to mitigate potential threats and ensure safe interaction between services, users, and devices in distributed cloud environments. Additionally, continuous monitoring, real-time threat detection, and automated response mechanisms are crucial to quickly identify and neutralize security risks, strengthening the cloud environments against evolving cyber threats [11], [18], [23].

C. *Infrastructure security*

Infrastructure security focuses on protecting the core components that form the backbone of cloud computing environments such as physical servers, Virtual Machines (VMs), storage systems, and network resources. As organizations increasingly rely on virtualized and containerized environments using technologies such as Docker and Kubernetes (K8s), securing these layers becomes essential. This involves securing the hypervisor layer, managing access controls, and ensuring that security practices are consistently applied across clouds [11], [18].

A key part of modern infrastructure security is the use of Cloud Security Posture Management (CSPM) tools, which help organizations automatically detect and address security risks such as misconfigurations through continuous monitoring and enforcing security policies across their cloud environments. CSPM plays a proactive role in identifying potential weaknesses before they become serious vulnerabilities [29].

D. *Application security*

Application security in cloud environments involves integrating protection measures throughout the entire Software Development Lifecycle (SDLC). This includes adopting secure coding, making regular vulnerability assessments, applying timely patches, and using tools such as Web Application Firewalls (WAFs) to defend against threats like Structured Query Language (SQL) injection and cross-site scripting (XSS). With the rise of cloud-native applications and microservices, security must also include container security, API protection, and Development, Security, and Operations (DevSecOps) integration. Key aspects include secure API development, strong web application security, and the protection of cloud-based AI/ Machine Learning (ML) applications, which often handle sensitive data and require additional layers of defence. By integrating security from the start and throughout the development process, organizations can better manage risks and ensure their applications stay robust in cloud [8]-[10], [14], [18]-[21].

E. *Compliance and governance*

Compliance and governance in cloud environments involve the frameworks, policies, and procedures that organizations adopt to ensure they meet regulatory requirements and internal standards. This includes adhering to data protection laws like GDPR, CCPA, other industry specific regulations like Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS), and the security policies of cloud service providers. Governance also extends to risk management, access controls, data classification, security audits, and accountability for cloud usage across the organization. Key standards and frameworks, such as NIST, ISO/IEC 27017:2015, and security auditing and logging practices, help organizations maintain compliance while ensuring continuous risk assessment and management. By incorporating these strategies, organizations can protect their cloud operations, minimize compliance risks, and maintain robust control over their cloud environments [14], [30], [31].

Finally, under the shared responsibility model, both cloud providers and customers must work together to keep the infrastructure secure and resilient against evolving threats [19], [21], [23], [24].

IV. Literature Review and Analysis

For the literature review, four recent review articles have been selected, each focusing on a distinct aspect of cloud computing security. These studies provide comprehensive insights into the major security challenges and mitigation strategies within different layers of the cloud ecosystem, offering a well-rounded understanding of current research trends and gaps.

The paper [32] offers a comprehensive analysis of cybersecurity challenges and strategies within cloud computing environments, highlighting the implications of the rapid and widespread adoption of such technology. It begins by outlining the core benefits of cloud computing which have driven its market growth, projected to increase from $371.4 billion in 2020 to $832.1 billion by 2025. This expansion is further fueled by the integration of emerging technologies, including edge computing, the IoT, AI/ML, and fifth generation (5G) mobile telecommunication networks. As more organizations migrate workloads to the cloud, cybersecurity has emerged as a critical concern.

The study examines cybersecurity practices across public, private, and hybrid cloud deployment models. Public clouds, while offering scalability and ease of access, are especially vulnerable due to their large and diverse user base. Key security challenges in this domain include insecure APIs, broad network access, and reduced governance control. In contrast, private clouds provide better security but face their own issues such as patch management, hypervisor vulnerabilities, and compliance with complex regulatory requirements. Hybrid clouds, combining elements of both, present additional difficulties related to secure data transmission, redundancy, and maintaining consistent security policies across environments. Ensuring adequate visibility and control is essential for mitigating risks in these architectures.

The paper emphasizes that while major cloud service providers including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) continue to advance their security offerings, responsibility for securing cloud resources is shared with the users. This is particularly true in IaaS and PaaS models, where much of the security implementation remains in the hands of customers. Despite ongoing risks, many organizations are driven to the cloud for its potential to enhance their overall cybersecurity posture.

A comparative analysis is presented, identifying the best practices and key vulnerabilities across the different cloud models. The study concludes by underscoring the importance of evolving security frameworks and a deep understanding of user-side security concerns. Overall, this work offers valuable insights for organizations seeking to strengthen their cloud security strategies in the face of emerging threats.

Building on the analysis of security challenges across deployment models, the authors of [33] focus on Secure Resource Management (SRM) in cloud computing. As cloud services rely heavily on virtualization, security concerns arise from issues such as inefficient resource allocation, VM co-residency, and system misconfigurations. These vulnerabilities can lead to data breaches, unauthorized access, and service disruptions. Motivated by the rising rate of cyberattacks and frequent misconfigurations among major cloud service providers, the study underscores the need for robust SRM strategies. It introduces an interactive model where applications send tasks to cloud servers, often deploying multiple VMs for user workloads. Malicious VMs sharing resources with legitimate ones pose a significant threat, especially when coupled with poor resource allocation practices.

The paper outlines key research challenges, including balancing security and performance, detecting malicious activity in multi-tenant environments, and adapting security mechanisms based on data sensitivity. It categorizes existing security solutions into three groups: *i) Defensive strategies:* focused on prevention; *ii) Mitigating strategies:* aimed at quick detection and recovery; and *iii) Hybrid strategies:* combining prevention and response for a more balanced approach.

A final analysis is conducted alongside experimental evaluations that compare strategies based on resource usage, power consumption, and threat prevention effectiveness. The findings suggest that hybrid strategies generally provide the most effective balance between performance and security.

Shifting focus to intelligent security mechanisms, the next study [34] explores the integration of ML and Cyber Threat Intelligence (CTI) to enhance cloud security. It begins by outlining the challenges faced by IT organizations with traditional local infrastructures such as limited scalability and high operational costs, which have led to the widespread adoption of cloud computing. Despite its benefits cloud computing also introduces significant security concerns. Traditional security mechanisms are often inadequate in addressing the evolving threats. The paper argues that machine learning offers a proactive solution, capable of predicting failures and detecting anomalies. It also highlights the importance of threat intelligence in identifying vulnerabilities and rapid responses.

The paper reviews common cloud security threats, including data loss, account hijacking, hypervisor attacks, and DDoS incidents. It categorizes these threats into areas such as network security, identity management, and compliance challenges. A significant focus is placed on ML techniques, particularly supervised learning algorithms used in IDS, and the growing relevance of unsupervised methods for anomaly detection. It underscores how integrating ML with CTI surpasses traditional approaches, particularly in handling internal threats and improving incident response. Despite this, a gap remains in fully realizing integrated, scalable solutions. The paper presents experimental results showing high accuracy for ML models in controlled settings, but also notes challenges such as data quality, real-time adaptability, and model scalability.

Finally, the authors state the need for real-time, adaptive security systems that dynamically respond to new threats. They highlight the potential of hybrid models that combine anomaly detection, contextual analysis, and threat intelligence to achieve proactive and robust cloud defense.

Complementing the previous technical approaches, [35] presents a comprehensive review of cloud security challenges and opportunities, with a particular emphasis on the importance of establishing trust between users and cloud service providers. Through a systematic literature review of 1,324 research papers, they employ the Design Science Research (DSR) framework to categorize findings into four artifact types: *i) Constructs*, *ii) Models*, *iii) Methods*, and *iv) Instantiations*, each analyzed across different layers of cloud architecture.

The paper identifies several critical security challenges, including data breaches, unauthorized access, and advanced cyberattacks, underscoring the need for a deep understanding of these threats to build secure and resilient cloud systems. It also highlights a range of emerging technologies that offer promising opportunities to strengthen cloud security, such as blockchain, ZTA, multi-cloud strategies, and AI/ML. These technologies are discussed in the context of various domains, including healthcare, IoT, and smart cities.

In addition, the authors propose a research framework to support organizations in managing digital transformation while maintaining a strong cybersecurity posture. This framework offers valuable insights into both the challenges and opportunities present in the evolving cloud landscape, contributing significantly to both academic discourse and practical implementations. The paper concludes by advocating for the integration of AI/ML into cloud security strategies as a key enabler for proactive, adaptive threat management.

Table 1. Studies and their key aspects

Aspect	[32]	[33]	[34]	[35]
Focus	Cloud deployment models and security implications	SRM in virtualized environments	ML and CTI for proactive cloud security	Trust, frameworks, and emerging technologies in cloud security
Scope	Deployment-level threats across public, private, and hybrid clouds	VM co-residency, resource allocation, and performance-security balance	Intelligent threat detection and response using ML and CTI	Comprehensive review using DSR framework
Methodology	Comparative analysis of deployment models and their vulnerabilities	Categorization of SRM strategies (defensive, mitigating, hybrid) plus experimental evaluation	Review of ML-based cloud security techniques with experimental results	Systematic review of 1,324 papers with DSR categorization
Key security challenges	Insecure APIs, network exposure, visibility, user-side responsibilities	VM misconfigurations, multi-tenancy risks, performance-security tradeoffs	Evolving threats, anomaly detection, real-time adaptability	Data breaches, trust management, advanced persistent threats
Proposed strategies	Shared responsibility model, evolving frameworks, best practices	Hybrid strategies for effective SRM	Real-time adaptive ML models, integration with CTI	Research framework, integration of AI/ML, use of blockchain and ZTA
Discussed technologies	Edge computing, IoT, AI/ML, 5G	Virtualization, VM isolation, resource scheduling	Supervised/unsupervised ML, IDS, CTI platforms	Blockchain, Zero Trust Architecture, AI/ML, Multi-cloud
Contribution	Overview of threat landscape by deployment model; emphasizes user responsibility	Emphasizes need for balance in SRM; introduces taxonomy of strategies	Advocates integration of CTI and ML; highlights implementation gaps	Offers high-level synthesis and future research agenda; focuses on trust and adaptability

Together as depicted in Table 1, these studies illustrate the varied nature of cloud security research, spanning technical, architectural, and organizational challenges. They highlight the shift toward intelligent, adaptive systems, the importance of secure cloud resource management, and the continued need for comprehensive security frameworks tailored to diverse deployment models.

V. Conclusions

This article reviewed four recent papers addressing different aspects of cloud computing security. The analysis shows that while cloud computing continues to revolutionize IT infrastructure through scalability, flexibility, and cost-efficiency, it also introduces complex and evolving security challenges. Each of the studies highlight a unique aspect of cloud security: from infrastructure-level concerns across deployment models, to intelligent threat detection mechanisms, to secure resource management strategies, and trust-building between users and providers.

Common concerns across the papers include the growing need for adaptive and proactive security frameworks, the increasing reliance on AI/ML for intelligent threat detection, and the persistent challenge of balancing performance with security. Moreover, the shared responsibility model across all layers of cloud environments underscores the importance of user-side security awareness and implementation. Emerging technologies such as blockchain, ZTA, and advanced AI/ML techniques are identified as promising solutions, though gaps remain in terms of integration, real-time responsiveness, and scalability.

Finally, this review contributes a comparative analysis and a structured taxonomy of cloud security challenges and solutions, highlighting gaps and convergences across the literature. It provides a roadmap for researchers and practitioners, reaffirming that cloud security is a multidimensional problem requiring coordinated technical, organizational, and strategic efforts. Future research should focus on interoperable, real-time, and scalable solutions to meet the evolving demands of secure cloud environments.

Acknowledgment

This work has been partially supported by the Horizon European project HORSE (grant agreement no. 101096342) and by the SERICS (PE00000014) project under the NRRP MUR program funded by the EU– NGEU.

References

[1] B. Varghese, and R. Buyya "Next generation cloud computing: New trends and research directions," in Future Generation Computer Systems, vol. 79, part. 3, pp. 849-861, Feb. 2018, doi: 10.1016/j.future.2017.09.020.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia "A view of cloud computing," in Communications of the ACM, vol. 53, issue. 4, pp. 50-58, Apr. 2010, doi: 10.1145/1721654.1721672.

[3] A. G. Prajapati, S. J. Sharma, and V. S. Badgujar, "All About Cloud: A Systematic Survey," in International Conference on Smart City and Emerging Technology (ICSCET), Jan. 2018, doi: 10.1109/ICSCET.2018.8537277.

[4] J. Surbiryala, and C. Rong, "Cloud Computing: History and Overview," in IEEE Cloud Summit, Aug. 2019, doi: 10.1109/CloudSummit47114.2019.00007.

[5] A. Chaugule, and S. Shaikh "The Impact of Cloud Computing on Business Agility," in International Research Journal of Modernization in Engineering Technology and Science, vol. 6, issue. 2, Feb. 2024, doi: 10.56726/IRJMETS49710.

[6] M. Zheng, R. Huang, X. Wang, and X. Li "Do firms adopting cloud computing technology exhibit higher future performance? A textual analysis approach," in International Review of Financial Analysis, vol. 90, Nov. 2023, doi: 10.1016/j.irfa.2023.102866.

[7] H. Subhi, R. Qaghi, L. M. Abdulrahman, M. A. Omar, and A. A. Yazdeen "Performance Analysis of Enterprise Cloud Computing: A Review," in Journal of Applied Science and Technology Trends, vol. 4, Feb. 2023, doi: 10.38094/jastt401139.

[8] Y. Duan, J. S. Edwards, and Y. K. Dwivedi "Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda," in International Journal of Information Management, vol. 48, Oct. 2019, doi: 10.1016/j.ijinfomgt.2019.01.021.

[9] V. S. N. Murthy, R. Kumari, M. Goyal, P. Dubey, M. Manikandan, and S. P. Ramesh "Edge-AI in IoT: Leveraging Cloud Computing and Big Data for Intelligent Decision-Making," in Journal of Information Systems Engineering and Management, vol. 10, 2025, pp. 601-619, doi: 10.52783/jisem.v10i20s.3194.

[10] Y. Chen, "IoT, cloud, big data and AI in interdisciplinary domains," in Simulation Modelling Practice and Theory, vol. 102, Jul. 2020, doi: 10.1016/j.simpat.2020.102070.

[11] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," in Computers & Electrical Engineering, vol. 59, Apr. 2017, pp. 126-140, doi: 10.1016/j.compeleceng.2016.03.004.

[12] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," in Journal of Network and Computer Applications, vol. 160, Jun. 2020, doi: 10.1016/j.jnca.2020.102642.

[13] S. Ahmadi, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in Journal of Information Security, vol. 160, pp. 148-167, May. 2024, doi: 10.4236/jis.2024.152010.

[14] T. J. Akinbolaji, G. Nzeako, D. Akokodaripon, and A. V. Aderoju, "Proactive monitoring and security in cloud infrastructure: leveraging tools like Prometheus, Grafana, and HashiCorp Vault for Robust DevOps Practices," in World Journal of Advanced Engineering Technology and Sciences, vol. 13, issue. 2, 2024, pp. 74-89, doi: 10.30574/wjaets.2024.13.2.0543.

[15] D. Ajish, "The significance of artificial intelligence in zero trust technologies: a comprehensive review," in Journal of Electrical Systems and Information Technology, Aug. 2024, doi: 10.1186/s43067-024-00155-z.

[16] K. Chokkanathan, S. M. Karpagavalli, G. Priyanka, K. Vanitha, K. Anitha, and P. Shenbagavalli, "AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience," in 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS), Nov. 2024, doi: 10.1109/CSITSS64042.2024.10816746.

[17] Joint Task Force Transformation Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Mar. 2011, doi: 10.6028/NIST.SP.800-39.

[18] D. Hillman, Y. Harel, and E. Toch, "Evaluating organizational phishing awareness training on an enterprise scale," in Computers & Security, vol. 132, Sep. 2023, doi: 10.1016/j.cose.2023.103364.

[19] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches," in Egyptian Informatics Journal, vol. 27, Sep. 2023, doi: 10.1016/j.eij.2024.100517.

[20] V. B. Ayoola, U. U. James, I. P. Idoko, O. M. Ijiga, and T. M. Olola, "Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective," in Global Journal of Engineering and Technology Advances, vol. 20, issue. 3, 2024, pp. 94-117, doi: 10.30574/gjeta.2024.20.3.0164.

[21] R. Taib, K. Yu, S. Berkovsky, and P. Bayl-Smith, "Social Engineering and Organisational Dependencies in Phishing Attacks," in 17th IFIP Conference on Human-Computer Interaction (INTERACT), Sep. 2019, pp. 564-584, doi: 10.1007/978-3-030-29381-9_35.

[22] R. Sharma, and A. Singla, "Optimizing Cloud Security: A Study of Effective Cybersecurity Measures for Organizations," in International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Dec. 2024, doi: 10.1109/ICICNIS64247.2024.10823273.

[23] M. S. Krishnappa, P. K. Veerapaneni, B. M. Harve, V. Jayaram, D. M. Bidkar, and G. Mehta, "Cybersecurity in the Cloud Era: Protecting Virtualized Environments Against Evolving Threats," in International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Dec. 2024, doi: 10.1109/ICICYTA64807.2024.10913114.

[24] M. Z. Alam, A. A. Khan, A. Ahmad, H. Khan, M. R. Khan, and I. Budhiraja, "Investigation of Cloud Forensic Incidents in Cloud Architecture for 6G Networks," in IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Dec. 2023, doi: 10.1109/ANTS59832.2023.10469370.

[25] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing," in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, Sep. 2011, doi: 10.6028/NIST.SP.800-145.

[26] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Cloud Computing Reference Architecture," in National Institute of Standards and Technology (NIST) Special Publication (SP) 500-292, Sep. 2011, doi: 10.6028/NIST.SP.500-292.

[27] S. Sisodia, S. Sharma, D. Kumar, L. Biswas, and S. Aluvala, "Navigating the Cloud: Choosing the Right Cloud Computing Services for Your Business," in IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Jan. 2024, doi: 10.1109/KHI-HTC60760.2024.10481894.

[28] H. B. Patel, and N. Kansara, "Cloud Computing Deployment Models: A Comparative Study," in International Journal of Innovative Research in Computer Science & Technology (IJIRCST), vol. 9, issue. 2, Mar. 2021, pp. 45-50, doi: 10.21276/ijircst.2021.9.2.8.

[29] G. Coppola, A. S. Varde, and J. Shang, "Enhancing Cloud Security Posture for Ubiquitous Data Access with a Cybersecurity Framework Based Management Tool," in IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), Oct. 2023, doi: 10.1109/UEMCON59035.2023.10316003.

[30] M. P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," in National Institute of Standards and Technology (NIST), Apr. 2018, doi: 10.6028/NIST.CSWP.04162018.

[31] M. A. L. Moscosos, P. E. S. Anccori, and W. N. Choquehuayta "Hardening to Improve the Security of Financial Institutions," in IEEE XXXI International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Nov. 2024, doi: 10.1109/INTERCON63140.2024.10833467.

[32] X. Liang, and Y. Xu, "A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud," in Computers & Security, vol. 151, Jan. 2025, doi: 10.1016/j.cose.2025.104339.

[33] D. Saxena, S. R. Swain, J. Kumar, S. Patni, K. Gupta, A. Kumar, and V. Lindenstruth, "Secure Resource Management in Cloud Computing: Challenges, Strategies and Meta-Analysis," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 55, issue. 4, Jan. 2025, pp. 2897-2912, doi: 10.1109/TSMC.2025.3525956.

[34] R. Thaqi, B. Krasniqi, A. Mazrekaj, and B. Rexha, "Literature Review of Machine Learning and Threat Intelligence in Cloud Security," in IEEE Access, vol. 13, Jan. 2025, pp. 11663-11678, doi: 10.1109/ACCESS.2025.3529636.

[35] M. Lata, and V. Kumar, "Cyber security techniques in cloud environment: comparative analysis of public, private and hybrid cloud," in The EDP Audit, Control, and Security Newsletter (EDPACS), vol. 70, issue. 3, Jan. 2025, pp. 1-21, doi: 10.1080/07366981.2025.2449743.