Al-Farouk journal of sciences
Volume (2), Issue (4) (Spt, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) العدد 4 سبتمبر 2026
ردمد: 3135-2359

Cloud computing security: A systematic review of security threats, protection strategies, and future trends

Ismail Abouiqasim omar Abumilyana 1, Mustafa Abdulhadi Ben Hmaida [2], Salem.S.M Klifa [3]

[1]College of science and technology – alriyayna Department of IT project management Hammamm2012@gmail.com

[2] Higher Institute of Science and Technology Misrata, Department of Computer Technology, BOFA.benhmaida@gmail.com

[3] Higher Institute of Science and Technology- Bir Alghanam, Department of IT, Salemassaid@gmail.com

Received: 2/8/2026 Revised: 21/8/2026 Accepted: 30/8/2026 Publication: 15/9/2026

Abstract

This research addresses cloud computing security through a systematic review of the scientific literature. Its aim is to identify the most prominent security threats facing cloud environments, analyze the protection strategies and techniques used to mitigate these threats, and explore future trends and research gaps in this field. The study employed the Systematic Literature Review (SLR) methodology, based on PRISMA guidelines for organizing the search, screening, selection, and analysis phases. 25research papers were reviewed from various databases and scientific sources. Such as Google Scholar, Scopus and IEEE Access After examining titles and abstracts and reviewing the studies' compliance with inclusion and exclusion criteria, 17 studies were selected for the final analysis, while 8 were excluded for not aligning with the research topic or criteria. The analysis focused on a range of threats, most notably data breaches, cloud resource misconfiguration, account hijacking, distributed denial-of-service (DDoS) attacks, privacy risks, and vulnerabilities associated with multi-cloud and hybrid environments. The review also addressed key protection strategies, including encryption, identity and access management, multi-factor authentication, the zero-trust model, continuous monitoring, and leveraging artificial intelligence and machine learning technologies for attack detection and response. The research concluded that enhancing cloud computing security requires an integrated approach combining technical solutions, organizational policies, and human awareness, along with the development of flexible security mechanisms adaptable to evolving threats. The review also highlighted the need for further applied research on the security of multi-cloud environments, privacy protection, the use of artificial intelligence, and improving interoperability and compliance with security standards.

Keywords: Cloud computing security, security threats, protection strategies, cybersecurity, multi-cloud computing, future challenges and opportunities.

الملخص

يتناول هذا البحث أمن الحوسبة السحابية من خلال مراجعة منهجية للأدبيات العلمية. ويهدف إلى تحديد أبرز التهديدات الأمنية التي تواجه بيئات الحوسبة السحابية، وتحليل استراتيجيات وتقنيات الحماية المستخدمة للتخفيف من هذه التهديدات، واستكشاف التوجهات المستقبلية والفجوات البحثية في هذا المجال. استخدمت الدراسة منهجية المراجعة المنهجية للأدبيات (SLR)، استنادًا إلى إرشادات PRISMA لتنظيم مراحل البحث والفرز والاختيار والتحليل. تمت مراجعة 25 بحثًا علميًا من قواعد بيانات ومصادر علمية متنوعة مثل IEEE Access,Google Scholar, and Scopus بعد فحص العناوين والملخصات ومراجعة مدى توافق الدراسات مع معايير الإدراج والاستبعاد، تم اختيار 17 دراسة للتحليل النهائي، بينما تم استبعاد 8 دراسات لعدم توافقها مع موضوع البحث أو معاييره.

ركز التحليل على مجموعة من التهديدات، أبرزها اختراقات البيانات، وسوء تكوين موارد الحوسبة السحابية، واختراق الحسابات، وهجمات الحرمان من الخدمة الموزعة(DDoS) ، ومخاطر الخصوصية، والثغرات الأمنية المرتبطة ببيئات الحوسبة السحابية المتعددة والهجينة. تناولت المراجعة أيضًا استراتيجيات الحماية الرئيسية، بما في ذلك التشفير، وإدارة الهوية والوصول، والمصادقة متعددة العوامل، ونموذج انعدام الثقة، والمراقبة المستمرة، والاستفادة من تقنيات الذكاء الاصطناعي والتعلم الآلي للكشف عن الهجمات والاستجابة لها. وخلص البحث إلى أن تعزيز أمن الحوسبة السحابية يتطلب نهجًا متكاملًا يجمع بين الحلول التقنية والسياسات التنظيمية والوعي البشري، إلى جانب تطوير آليات أمنية مرنة قابلة للتكيف مع التهديدات المتطورة. كما سلطت المراجعة الضوء على الحاجة إلى مزيد من البحوث التطبيقية حول أمن بيئات الحوسبة السحابية المتعددة، وحماية الخصوصية، واستخدام الذكاء الاصطناعي، وتحسين قابلية التشغيل البيني والامتثال لمعايير الأمان.

الكلمات المفتاحية: أمن الحوسبة السحابية، التهديدات الأمنية، استراتيجيات الحماية، الأمن السيبراني، الحوسبة السحابية المتعددة، التحديات والفرص المستقبلية.

1. Introduction

In recent years, the world has witnessed rapid development in information and communication technology, leading to the emergence of new technologies that have transformed how data is stored, processed, and managed. Cloud computing is one of the most prominent technologies that has fundamentally transformed digital infrastructure. It allows organizations and individuals to access computing resources, such as servers, storage, databases, and software, via the internet without needing to own and directly manage the underlying infrastructure. This model has contributed to greater flexibility in the use of technological resources, reduced operational costs, and improved scalability and responsiveness to changing business requirements.

Cloud computing relies on a range of models and services that meet the diverse needs of users and organizations. Among the most prominent are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud deployment environments also vary, including public, private, and hybrid clouds, enabling the application of this technology in numerous fields, such as higher education, healthcare, banking, e-commerce, and government administration. With the increasing adoption of cloud computing, this technology has become essential for supporting digital transformation and enhancing the efficiency of e-services.

Despite the advantages offered by cloud computing, its growing reliance has led to a range of challenges related to information security and data protection. Organizations are increasingly dependent on technology environments that may include shared resources, public network connections, and third-party services, making it more critical to ensure data confidentiality, integrity, and availability. The most prominent potential security threats include account compromise, data leaks, misconfiguration of cloud resources, distributed denial-of-service (DDoS) attacks, malware, and risks associated with access control and permissions management.

Cloud computing security is a crucial research topic due to its direct link to protecting digital assets and ensuring the continuity of e-services. The diverse nature of cloud environments and the variety of service providers lead to multiple challenges that require integrated security strategies. These strategies should include encryption, multi-factor authentication, identity and access management, continuous monitoring, risk assessment, and the implementation of governance and compliance policies. Data protection is not solely the responsibility of the cloud service provider; it requires collaboration and a clear division of responsibilities between the service provider and the end user, according to the shared responsibility for security model.

With the rapid advancements in artificial intelligence, the Internet of Things, and edge computing, cloud computing environments have become increasingly complex and diverse. This necessitates the development of security solutions capable of addressing emerging threats. Reviewing published scientific studies is also crucial for identifying current research trends, analyzing key security risks, and evaluating the effectiveness of strategies and technologies used to mitigate these risks.

Therefore, this research aims to provide a systematic review of the scientific literature related to cloud computing security. This review examines the most common security threats, analyzes existing protection strategies, and identifies key future trends in the field. The review seeks to organize the available scientific knowledge and identify areas requiring further research, thereby supporting researchers and technology institutions in understanding the challenges of cloud computing security and developing more effective practices for protecting data and digital services.

2. Research Problem

Cloud computing has witnessed increasing adoption across various organizations and sectors due to its flexibility in accessing computing resources, ease of data storage and processing, and reduced reliance on traditional infrastructure. With this expansion, organizations have become increasingly dependent on cloud environments that host vast amounts of data, applications, and services. This has made information security and privacy protection among the most prominent challenges facing the adoption and continued use of cloud computing.

The research problem lies in the fact that migrating to cloud environments introduces a range of security risks related to data protection, access management, resource misconfiguration, account breaches, and cyberattacks. Furthermore, ensuring the confidentiality, integrity, and availability of

information while relying on cloud service providers is challenging. The multiplicity of cloud service models and the differing responsibilities of service providers compared to users further complicate the process of managing security risks.

Ahmadi's study (2024) demonstrated that cloud computing, despite its flexibility, scalability, and cost-effectiveness, faces multiple security threats, including distributed denial-of-service (DDoS) attacks, account hijacking, malware, and data breaches. The study also highlighted the importance of risk mitigation strategies such as identity and access management, encryption, vulnerability management, and continuous monitoring.

Similarly, Ukeje, Gutierrez, and Petrova (2024) conducted a systematic review of the information security and privacy challenges associated with cloud computing adoption in government institutions. Their findings revealed that information security and privacy represent significant barriers to cloud service adoption, underscoring the need to develop more effective frameworks and strategies to address these challenges.

In their systematic review, Soveizi, Turkmen, and Karastoyanova (2023) addressed security and privacy concerns in cloud-based scientific and commercial workflows. They highlighted gaps in monitoring, preventing, and responding to security breaches, as well as the need for integrated workflow management systems that consider security requirements.

Based on the above, the research problem lies in the need for a systematic analysis of scientific studies related to cloud computing security. This analysis aims to identify the most prominent security threats, understand the protection strategies employed, and evaluate current research trends and remaining research gaps. Therefore, this research seeks to answer the following main question:

What are the most prominent security threats facing cloud computing environments? What strategies and technologies are used to mitigate them? And what are the most important future trends in the field of cloud computing security?

3. Research Objectives

This research aims to achieve the following objectives:

1. To identify the most prominent security threats facing cloud computing environments and analyze the risks associated with data protection and privacy.
2. To analyze the protection strategies and technologies used to enhance cloud computing security and mitigate attacks and security breaches.
3. To identify future research trends in the field of cloud computing security and pinpoint scientific gaps that require further investigation.

4. Research Questions

This research seeks to answer the following main question:

1. What are the most prominent security threats and risks facing cloud computing environments, according to previous scientific studies?
2. What are the most important strategies and technologies used to protect data, enhance cloud computing security, and mitigate cyberattacks?
3. What are the most prominent future research trends and scientific gaps in the field of cloud computing security that need further study?

5. Research Methodology

This study employed the Systematic Literature Review (SLR) methodology to systematically and methodically analyze scientific studies related to cloud computing security. The review procedures were implemented according to the principles of PRISMA 2020 to ensure the organized selection of studies, the identification of relevant studies, and the clear and traceable analysis of their results.

The review process began by collecting relevant scientific studies on cloud computing security. These studies were then reviewed and assessed for their relevance to the study's topic and scope. Following this, inclusion and exclusion criteria were applied to the collected studies to arrive at a group of studies most relevant to the research topic.

During the review process, 25 studies were read and analyzed in detail. After examination and evaluation, 17 studies were included in the final analysis, while 8 studies were excluded for not adequately aligning with the study's scope or the established selection criteria.

After identifying the final studies, relevant information and results were extracted from each study and organized to facilitate comparison between them. The analysis primarily focused on the nature of security threats facing cloud computing, the protection strategies and techniques used to mitigate these threats, as well as emerging technologies, future trends, and research gaps.

The selected studies were analyzed using thematic and narrative synthesis. This involved grouping and classifying similar findings into main themes, then comparing the similarities and differences between the studies. Accordingly, the review results were organized into six main themes: characteristics of the included studies, security threats, protection strategies, emerging technologies, future trends, and research gaps.

The analysis also focused on identifying recurring themes and findings across the different studies, monitoring recent developments in cloud computing security, and comparing the protection methods used to address various threats. This approach provided a comprehensive picture of the current state of cloud computing security, while also identifying areas that still require further research and development.

Thus, the systematic review methodology used in this study enabled the construction of a structured analysis of the selected literature, linking the results of previous studies to the main research themes, leading to the extraction of general trends, the most prominent security challenges, protection strategies, modern technologies, and research gaps in the field of cloud computing security.

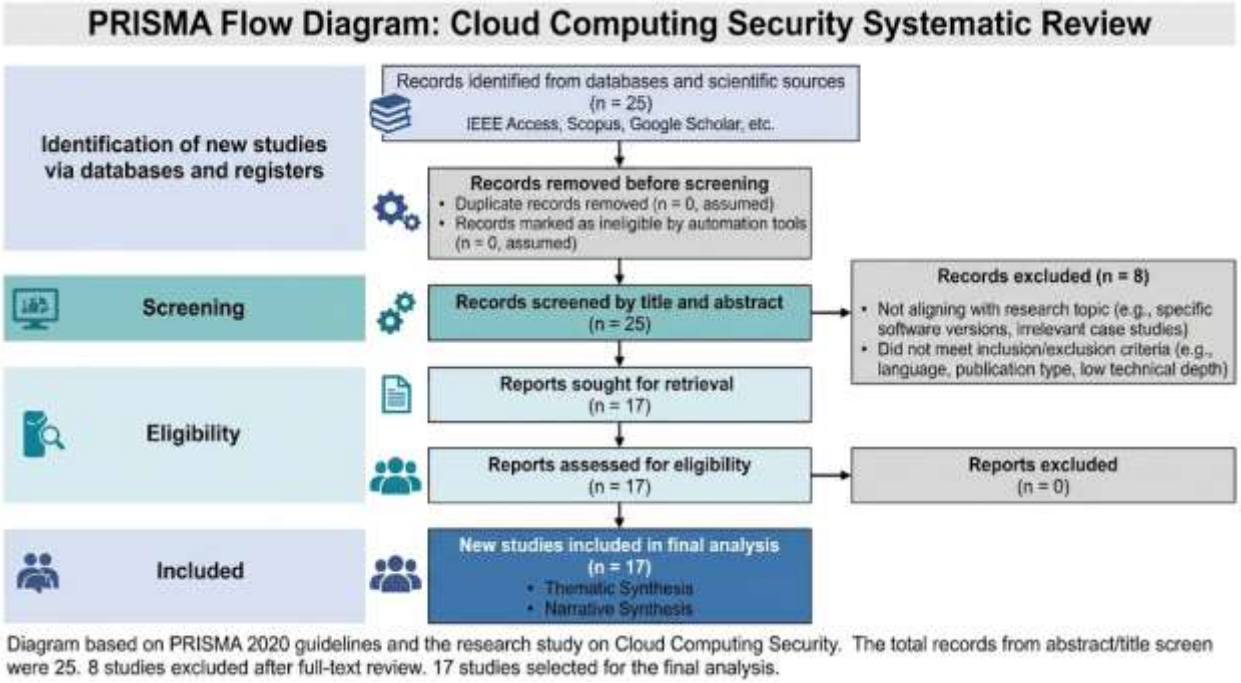

Figure 1 PRISMA Flow Diagram

6. Literature review

The study by Alouffi et al. (2021), titled "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," published in IEEE Access, addressed cloud computing security through a systematic review of the scientific literature related to security risks and challenges. The study aimed to review research published on cloud computing security between 2010 and 2020, analyzing the security threats facing cloud services and mitigation strategies. The researchers relied on examining studies published in digital libraries, selecting 80 research papers to answer the research questions. The results identified seven major security threats to cloud computing services and showed that data manipulation and leakage were among the most frequently addressed topics in the selected studies, along with the risks associated with data breaches and storage in cloud environments. The study also indicated that outsourcing user data storage presents a significant challenge for both cloud service providers and users. It suggested blockchain technology as a potential solution to mitigate security concerns. The study emphasized the need for continued research to develop solutions that ensure data confidentiality, integrity, and availability. This study aligns with current research in its reliance on a systematic literature review and analysis of security threats in cloud computing, while the current research focuses on threat analysis, protection strategies, and future research trends in light of recent scientific studies.

The study by Zanjiabadi Zadeh et al. (2023), titled "Cloud Computing Security: A Review of Basic Concepts, Security Challenges, Issues, Requirements, Security Standards, and Types of Attacks in Cloud Computing," published in the journal Computing and Distributed Systems, Volume 6, Issue 1, pages 137–153, addressed the topic of cloud computing security by reviewing

the basic concepts, security challenges and issues, and the requirements and standards related to protecting cloud environments. The study aimed to clarify the most important security aspects associated with cloud computing, identify the types of attacks that may target its resources and services, and highlight the importance of implementing appropriate security measures and standards to protect data. The study explained that while cloud computing provides dynamic and scalable virtual computing resources on demand via the internet, organizations face security concerns when migrating their services to the cloud, particularly regarding data privacy, the transparency of security procedures at service providers, and ensuring the protection of information and resources. The study also emphasized the importance of understanding security requirements and protection standards to mitigate potential risks. This study is consistent with current research in addressing cloud computing security and the security challenges and attacks associated with it, while the current research is distinguished by its reliance on a systematic review of scientific literature to analyze security threats, protection strategies and future trends in this field.

The study by Dawood ا‌et al. (2023), titled “Cyberattacks and Cloud Computing Security: A Comprehensive Guide,” addressed cloud computing security by reviewing various cloud computing models and services and analyzing associated security trends. The study focused on a wide range of security problems and threats facing cloud environments, most notably data breaches, data confidentiality, access control, authentication, inadequate due diligence, phishing, key disclosure, auditing, and privacy protection, in addition to the challenges associated with cloud-enabled Internet of Things (IoT) applications. The study also proposed a set of security attacks and countermeasures suitable for different cloud computing models, aiming to enhance their ability to withstand security threats. It concluded by identifying several future trends and implications related to the security of cloud computing models, emphasizing the importance of continued research and development to improve security in cloud environments. This study aligns with current research in its focus on security threats, protection strategies, and future trends. However, current research distinguishes itself by employing a systematic literature review (SLR) to collect and analyze previous studies in a structured manner and identify key trends and research gaps in the field of cloud computing security.

Barbara's 2023 thesis, "Assessing Future Development Needs in Cloud Computing Cybersecurity: A Systematic Review of Literature Reviews," addressed the topic of identifying future research needs to enhance the security and reliability of cloud computing. The thesis aimed to analyze a collection of literature reviews published in the Google Scholar and Scopus databases to uncover key research gaps that still require in-depth investigation. It also assessed the extent to which previous studies addressed the awareness of businesses and their employees regarding the importance of cybersecurity when using cloud computing services. Based on specific inclusion and exclusion criteria, the study selected eleven literature reviews for analysis in accordance with the research objectives. The results revealed several research gaps requiring further attention, along with suggestions on how to address these gaps to make cloud computing more secure and reliable for organizations. This thesis agrees with the current research in its reliance on a systematic methodology for analyzing the literature and identifying research gaps and future trends in cloud computing security, but it differs from it in its focus on reviewing literature reviews and on the

level of security awareness among institutions and employees, while the current research focuses on analyzing security threats, protection strategies and future trends through a systematic review of relevant studies.

Thatikonda's 2023 study, "Data Security in Cloud Computing: Challenges, Solutions, and Future Trends," addressed the importance of data security in cloud computing environments, given the increasing reliance of organizations on adaptable and customizable cloud resources. The study focused on the role of data security in maintaining digital trust and ensuring business continuity. It also discussed a range of technical and administrative challenges facing organizations and cloud service providers, most notably the need for encryption, the risks of data breaches, and the necessity of complying with data protection laws and regulations. The study also reviewed several solutions and best practices that can contribute to enhancing cloud data protection. Furthermore, it discussed the role of emerging technologies, particularly artificial intelligence and machine learning, in developing mechanisms for monitoring, detecting, and responding to cyber threats. The study emphasized the need for organizations and cloud service providers to continuously adapt to the rapidly changing cybersecurity landscape, focusing on continuous improvement and the development of data security mechanisms to safeguard the digital future. This study is consistent with the current research in its interest in cloud computing security and the analysis of security challenges, solutions and future trends, but the current research is distinguished by its reliance on the systematic literature review (SLR) methodology, with the aim of providing a more comprehensive and organized analysis of security threats, protection strategies and future research trends in the field of cloud computing security.

The study by Alhadi, Al-Shaibany, and Al-Homdyl (2024), titled "Survey on Cloud Computing Security," published in the Sana'a University Journal of Applied Sciences and Technology, addressed the topic of cloud computing security. Its aim was to review studies related to various attacks targeting cloud computing services and to provide a better understanding of security issues and related solutions. The study explained that cloud computing offers numerous advantages, including easy access to resources and modern technologies, reduced investment costs in technical infrastructure, and the ability to gradually increase resources according to service demand. Conversely, it emphasized that data security and privacy are among the most prominent challenges facing cloud environments, given their vulnerability to cyberattacks that exploit security weaknesses, potentially exposing data, resources, and digital assets to risk. The study also focused on the importance of identifying attacks targeting cloud services and understanding appropriate security solutions to mitigate these risks. This study is consistent with current research in its interest in cloud computing security and the cyber threats it faces, while the current study is distinguished by its systematic approach on conducting a systematic review of the literature to analyze security threats, protection strategies and future trends in this field.

A study by Singh Sanger and Johari (2024), titled "A Survey Study on Cloud Computing Security Issues," published in the AIP Proceedings, Volume 2919, Issue 1, Article 120006, addressed cloud computing security issues. Its aim was to review the fundamentals of cloud computing, its security challenges, cyberattacks, and strategies for mitigating them. The study explained that cloud computing provides ample storage capacity and on-demand online services,

while also reducing the need for investment in expensive hardware and lowering IT resource expenditures. However, it also pointed out that the migration of organizations from on-premises to cloud infrastructure introduces a range of security challenges, particularly since most cloud resources rely on online service providers, increasing the likelihood of additional security risks. The study further explored cloud infrastructure models, deployment frameworks and services, cloud computing platforms, and cloud security standards, along with security risks and attacks, and outlined future research directions in the field of cloud computing security. This study is consistent with current research in focusing on cloud computing security and the challenges and attacks associated with it, while the current research is distinguished by its reliance on a systematic review of scientific literature to analyze security threats, protection strategies and future trends.

Sina Ahmadi's (Ahmadi, 2024) study, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," published in the Journal of Information Security, Volume 15, Issue 2, pages 148–167, addressed the topic of cloud computing security through a systematic review of the scientific literature. The study aimed to identify the latest knowledge related to cloud computing security, focusing on the most prominent security threats and mitigation strategies. It explained that cloud computing offers organizations numerous advantages, including flexibility, scalability, and cost-effectiveness; however, its adoption necessitates ensuring the security of cloud applications, data, and networks. The study also addressed the most prominent security threats, such as distributed denial-of-service (DDoS) attacks, account hijacking, malware, and data breaches. Furthermore, it reviewed a range of protection strategies, including security awareness training, vulnerability management, security information and event management (SIEM), identity and access management (IAM), and encryption techniques. The study also discussed emerging trends in cloud computing security, such as artificial intelligence and machine learning, serverless computing, and containerization, in addition to the shared responsibility model and the challenges associated with its implementation. It emphasized the importance of continued research and innovation to address evolving threats and foster a strong security culture within organizations. This study aligns with current research in its reliance on a literature review and an examination of security threats and protection strategies, while the current research focuses on analyzing research trends and gaps in the field of cloud computing security.

Ahmed's 2024 study, "Trends and Challenges in Securing Cloud Computing Environments: An Overview of Current Technologies," addressed the latest trends and challenges related to the security of cloud computing environments, given the increasing use of cloud services and the accompanying security threats and complexities related to shared responsibility and compliance. The study focused on several emerging trends and technologies, most notably zero-trust architecture, the integration of artificial intelligence and machine learning for advanced threat detection, and the use of encryption, access controls, and security standards to protect data and systems in multi-tenant environments. The study also emphasized the importance of adopting a multi-layered security approach, clearly defining security responsibilities, and continuously developing security technologies to address evolving threats. It highlighted challenges requiring further research, particularly adversarial attacks, and the need to establish robust security standards for hybrid and multi-cloud environments. The study also advocated for enhanced collaboration among stakeholders and investment in privacy-preserving technologies. This study is consistent

with the current research in addressing the most prominent security threats, protection technologies, and future trends in cloud computing security, while the current research is distinguished by its reliance on a systematic literature review (SLR) with the aim of systematically collecting and analyzing the results of previous studies and identifying research gaps and future trends in the field.

The study by Khalifa and Al-Madani (2024), titled "Security in Cloud Computing: Threats, Mitigation Strategies, and Future Trends," published in the IET Conference proceedings, addressed cloud computing security by focusing on the most prominent security threats that organizations may face as a result of their increasing reliance on cloud infrastructure and services. The study aimed to identify the most common threats, including data loss and malware infection, and reviewed the controls and mitigation strategies that organizations can implement to reduce these risks, such as intrusion detection systems. The study also discussed future trends and defensive measures that can contribute to enhancing the security of cloud computing environments, emphasizing that achieving a higher level of protection requires understanding security threats, implementing effective mitigation controls, and keeping pace with modern technological developments. This study is consistent with the current research in its treatment of security threats, mitigation strategies, and future trends in cloud computing security, while the current research is distinguished by its reliance on the systematic literature review (SLR) to systematically analyze the results of previous studies, link threats to protection strategies, and identify gaps and future research trends.

The study by Mestry et al. (2024), titled "Cloud Security Risks and Mitigation Strategies: A Review of Current Trends and Future Directions.," addressed the security challenges arising from the increasing prevalence of cloud computing and its reliance on organizations for their IT infrastructure. The study focused on a range of risks associated with cloud environments, most notably misconfiguration, multi-tenant vulnerabilities, and insecure APIs. It also discussed advanced mitigation strategies, primarily Zero Trust Architecture (ZTA) and symmetric encryption. Furthermore, the study explored several emerging technological trends, such as confidential computing and post-quantum cryptography, along with future challenges related to cross-border data management and the ethical use of artificial intelligence. The study integrated findings, industry reports, and technical research published between 2019 and 2024 to provide practical recommendations for improving the security of cloud environments. This study aligns with current research in addressing security risks, protection strategies, and future trends in cloud computing. It also supports the importance of studying emerging technologies such as zero-trust and post-quantum cryptography. However, this research differs from previous studies in its reliance on a systematic literature review (SLR), employing a structured methodology to analyze existing studies and identify research trends and gaps in the field of cloud computing security.

The study by Ali et al. (2024), titled "Enhancing Cloud Computing Security: Unlocking the Preventive Potential of Symmetric Secret Sharing in Secure Cloud Computing," explored the development of a security approach combining secret sharing and symmetric encryption to protect sensitive data in cloud computing environments. The study relied on distributing data across multiple servers, which reduces the risk of relying on a single point of failure and enhances security

and privacy. It also employed symmetric encryption to allow computations to be performed on encrypted data without requiring direct access to the original data, thus minimizing the potential for unauthorized disclosure or misuse during processing. To evaluate the effectiveness of the proposed scheme, the study conducted a series of performance tests, including encryption and decryption times, processing load, and computational efficiency. The results demonstrated the possibility of achieving a balance between security and performance efficiency. This study agrees with the current research in its interest in data protection and enhancing privacy and security in cloud environments, but it focuses in a specialized technical way on a specific protection mechanism, which is the combination of secret sharing and symmetric encryption, while the current research deals with various threats, protection strategies and future trends through a systematic literature review (SLR).

The study by Chan et al. (2025), titled "Cloud Computing Security: Addressing Evolving Threats in the Digital Age," published on January 7, 2025, as a preprint, examines the evolution of cloud computing and its security paradigms. It focuses on the core components of a cloud computing environment, including data, applications, operating systems, virtualization, servers, storage, and networks. The study reviews the most prominent security threats facing cloud environments, such as account compromise, malware, data leaks, Denial-of-Service (DoS/DDoS) attacks, and social engineering, discussing the impact of these threats and the measures used to mitigate them. It also addresses several security technologies, most notably encryption, Identity and Access Management (IAM), cloud firewalls, and disaster recovery plans. Furthermore, the study highlights some limitations and challenges, such as bandwidth and redundancy issues and control constraints, as well as emerging trends in cloud computing security, including threat detection using artificial intelligence, zero-trust models, and multi-cloud security. The study proposed advanced countermeasures, such as the use of behavioral biometrics and adaptive deception systems, along with the application of neural networks and reinforcement learning in threat detection. While this study aligns with current research addressing security threats, protection technologies, and future trends in cloud computing security, it distinguishes itself by employing a systematic literature review (SLR) to analyze a range of previous studies in a structured manner, identifying research trends and gaps in the field. It is important to note that this study is a preliminary, non-peer-reviewed version and should therefore be used as a supporting source for current trends, not as a peer-reviewed study.

"Cloud Computing Security Trends" by Balboni et al. (2025), published in the fourth edition of the Computer and Information Security Handbook, addresses current trends in cloud computing security in light of the increasing reliance on cloud services and the accompanying risks and challenges, particularly those related to data security and compliance with data protection requirements. The chapter explains that cloud service providers are striving to enhance security and legitimacy guarantees by developing new technologies and mechanisms to protect cloud services. The authors focus on two main trends: the expanding use of data encryption and the emergence of self-regulatory frameworks that include codes of conduct and certification mechanisms. They also discuss in more detail the European Cloud Computing Services Scheme (EUCS) as a model of the proactive European approach to enhancing cybersecurity and establishing unified standards for cloud service security. This study is consistent with current

research in its treatment of cloud computing security trends, data protection technologies, and security compliance, while the current research differs from it in its broader focus on analyzing security threats, protection strategies, and future trends through a systematic literature review (SLR).

The study by Ali et al. (2025), titled "Security and Privacy in Multi-Cloud and Hybrid Computing Environments: Challenges, Strategies, and Future Trends," focused on analyzing the security and privacy aspects associated with the increasing reliance on multi-cloud and hybrid cloud environments, characterized by data distribution, diverse infrastructures, and complex intercloud communications. The study examined a range of security issues, including data confidentiality, access control, communications security, and regulatory compliance, as well as modern threats that may transcend the boundaries of a single cloud environment, such as cross-cloud threats and side-channel attacks. It also evaluated several security approaches, including encryption, identity and access management, AI-powered threat detection, and privacy protection techniques, comparing these approaches in terms of security effectiveness, computational cost, and applicability. The study further discussed emerging security technologies, such as post-quantum cryptography, zero-trust architectures, decentralized security frameworks, and AI-driven security automation. The study concluded that scalable security solutions are needed to adapt to the nature of multi-cloud and hybrid environments, while also considering regulatory and privacy requirements. This research contributes to the current discussion by clarifying the nature of risks and security strategies in complex cloud environments. It also supports future trends by highlighting emerging technologies that could shape the future of cloud computing security. Furthermore, the current research addresses cloud computing security more comprehensively through a systematic literature review (SLR) encompassing various cloud environments and models.

A study by Adeniji, S. A., Oke, F., Okolo, J., & Dubamu, O. (2025), titled "Cybersecurity in the Era of Cloud Computing and the Internet of Things: Emerging Threats and Advanced Protection Technologies," published as a preprint on TechRxiv on August 7, 2025, examines the convergence of cloud computing and the Internet of Things (IoT), and the resulting development of intelligent, interconnected, and scalable digital environments. The study focuses on analyzing emerging cyber threats in these environments, most notably data breaches, insecure APIs, hardware compromise, and multi-layered vulnerabilities, and the risks they pose to data confidentiality, integrity, system availability, and user privacy.

The study also reviews several advanced protection technologies, such as Zero Trust architecture, AI-powered threat detection, blockchain technology, and post-quantum cryptography. The study also addressed global cybersecurity standards and regulatory frameworks, along with the challenges of implementing these solutions, including scalability, the diversity of IoT devices, and the need for real-time threat detection. The study aimed to identify knowledge gaps and provide practical recommendations for enhancing the security of cloud environments connected to the Internet of Things.

The study by Ahmadipour and Ahmadipour (2026), titled "Cybersecurity in Cloud Energy Storage Systems: A Comprehensive Review of Challenges and Future Trends," examined the

security of cloud energy storage systems (CESS) as a critical component of modern energy infrastructure. It focused on the cyber risks arising from these systems' reliance on cloud technologies and their integration with renewable energy sources. The study categorized security threats according to operational architecture and attack vectors, highlighting advanced persistent threats (APTs), ransomware, IoT device exploitation, and systemic risks associated with cloud operations. It also reviewed various defense mechanisms, such as blockchain, AI-powered threat detection, and zero-trust architectures, assessing their role in enhancing data integrity, system reliability, and scalability. Furthermore, the study explored emerging technologies, including quantum computing-resistant encryption, federated learning, and differential privacy, and identified a range of future research directions aimed at developing more resilient and energy-efficient security frameworks. This study intersects with current research on cyber threats, protection technologies, and future trends in cloud computing, but it focuses specifically on cloud energy storage systems, while current research addresses cloud computing security in general through a systematic review of the literature, allowing for the compilation of results from studies related to various cloud environments and applications.

6.1 Comparing the Results of Previous Studies

Previous studies have shown a growing interest in cloud computing security, but they differ in their scope, the nature of the security threats, and the strategies they propose. The results of these studies can be compared through the following points:

First: Points of Agreement Among Previous Studies

Most studies agreed that data security and privacy are among the most prominent challenges associated with cloud computing. The studies by Thatikonda (2023), ALhadi et al. (2024), and Zanjiabadi Zadeh et al. (2023) focused on the risks of data breaches, information leaks, and weak privacy protection, and emphasized the importance of encryption, access controls, and compliance with data protection regulations.

The studies by Alouffi et al. (2021), Ahmadi (2024), and Mestri et al. also agreed on these points. (2024) states that cloud threats are not limited to data breaches, but also include misconfiguration, account hijacking, distributed denial-of-service attacks (DDoS), malware, weak APIs, and insider threats. This indicates that cloud security requires integrated protection encompassing data, infrastructure, applications, and users.

Most recent studies, such as Ahmad (2024), Ali et al. (2025), and Adeniji et al. (2025), agree on the importance of employing advanced technologies to enhance cloud security, particularly artificial intelligence and machine learning, zero-trust architecture, blockchain, advanced encryption, and post-quantum cryptography. These studies also emphasize the need for continuous development of early threat detection and response mechanisms.

Second: Differences Among Previous Studies

Previous studies differed in their subject scope. Some studies addressed cloud computing security in general, such as Singh Sanger and Johari (2024) and Ridwan et al. (2017), while other studies focused on more specialized aspects. For example, Ali et al. (2024) examined the use of symmetric

encryption and secret partitioning to protect cloud data, while Ahmadipour and Ahmadipour (2026) focused on cybersecurity in cloud energy storage systems.

Adeniji et al. (2025) focused on the convergence of cloud computing and the Internet of Things (IoT), and the resulting threats related to connected devices and their diversity. Ali et al. (2025) addressed the security and privacy of multi-cloud and hybrid environments, including the challenges related to data exchange, compliance, and cross-cloud threats.

Methodologically, some studies relied on general or exploratory reviews, while others used systematic literature reviews. Alouffi et al., for example, presented a comprehensive literature review. (2021) provided a systematic review of threats and mitigation strategies, while Ahmadi's (2024) study focused on analyzing the literature related to threats and mitigation methods. Barbara's (2023) study was distinguished by its focus on reviewing literature reviews to identify future development needs and gaps in the field of cloud cybersecurity.

Third: Comparison of security threats addressed by studies

Table 1 Comparison of Security Threats Addressed in the Reviewed Studies

Security Threat	Studies That Addressed the Threat	Key Findings
Data Breaches and Data Leakage	Thatikonda (2023); Alhadi et al. (2024); Alouffi et al. (2021); Ahmadi (2024); Dawood et al. (2023)	Emphasized the importance of encryption, secure data storage, access control, privacy protection, and mechanisms for preventing unauthorized disclosure of sensitive data.
Cloud Resource Misconfiguration	Ahmadi (2024); Dawood et al. (2023); Ahmad (2024); Mistry et al. (2024)	Highlighted the need for secure configuration, continuous monitoring, vulnerability assessment, and effective management of cloud resources and services.
Account Hijacking and Weak Authentication	Ahmadi (2024); Dawood et al. (2023); Singh Sanger and Johari (2024)	Emphasized Identity and Access Management (IAM), stronger authentication mechanisms, access control, and continuous monitoring of user activities.
Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) Attacks	Ahmadi (2024); Alhadi et al. (2024); Dawood et al. (2023); Adeniji et al. (2025)	Highlighted the importance of attack detection, continuous monitoring, appropriate mitigation mechanisms, and rapid incident response.
Malware and Ransomware	Ahmadi (2024); Khalifa and Al-Madani (2024);	Emphasized threat detection and response mechanisms, continuous monitoring, data

Security Threat	Studies That Addressed the Threat	Key Findings
	Ahmadipour and Ahmadipour (2026)	backup, and advanced security technologies to reduce the impact of malware-related attacks.
Insecure Application Programming Interfaces (APIs)	Dawood et al. (2023); Mistry et al. (2024); Adeniji et al. (2025)	Highlighted the need to strengthen API security, conduct vulnerability assessments, and protect interfaces connecting cloud services and applications.
Insider Threats	Dawood et al. (2023); Mistry et al. (2024)	Emphasized access control, privilege management, monitoring of user activities, and applying the principle of least privilege to reduce insider-related risks.
Privacy and Data Protection Risks	Alouffi et al. (2021); Thatikonda (2023); Dawood et al. (2023); Ali et al. (2025)	Emphasized encryption, privacy-preserving mechanisms, access control, regulatory compliance, and stronger data protection policies.
Multi-Cloud and Hybrid Cloud Security Risks	Ali et al. (2025); Ahmad (2024)	Highlighted the complexity of securing distributed environments and the need for unified security policies, identity management, compliance mechanisms, and scalable protection solutions.
Cloud–IoT Security Risks	Adeniji et al. (2025); Dawood et al. (2023)	Identified additional risks resulting from the integration of cloud computing with IoT, emphasizing real-time threat detection, Zero-Trust Architecture, and advanced protection technologies.
Advanced and Emerging Cybersecurity Threats	Ahmad (2024); Adeniji et al. (2025); Ahmadipour and Ahmadipour (2026)	Highlighted the growing importance of Artificial Intelligence, Machine Learning, Zero-Trust Architecture, blockchain, post-quantum cryptography, and privacy-preserving technologies.

Fourth: Comparing Protection Strategies

Studies have shown that encryption is one of the most frequently used solutions, but it is no longer sufficient on its own to counter all threats. Thatikonda (2023) focused on encryption and data protection, while Ali et al. (2024) proposed more specialized techniques, such as symmetric

encryption and secret partitioning, to reduce the risk of a single point of failure and protect data during processing.

In contrast, other studies have focused on identity and access management, such as those by Ahmadi (2024) and Dawood et al. (2023), while Ahmad (2024) and Ali et al. (2025) explored zero-trust architecture as a security framework that does not automatically grant trust to any user or device.

Artificial intelligence and machine learning have also emerged in recent studies as tools for improving attack detection and anomalous behavior analysis. However, some studies have indicated that these technologies may face challenges related to model accuracy, malicious attacks, privacy, and the need for reliable training data.

Fifth: Comparing Future Trends

Most recent studies emphasize the importance of:

1. Artificial intelligence and machine learning for early threat detection.
2. Zero-trust architectures for access management and continuous verification.
3. Post-quantum cryptography to counter future threats.
4. Blockchain to enhance integrity and traceability.
5. Privacy-preserving technologies, such as federated learning and differential privacy.
6. Developing security solutions tailored to multi-cloud and hybrid environments.
7. Improving compliance, regulatory standards, and governance frameworks.
8. Enhancing security in IoT and smart systems environments.

However, priorities vary among studies; some focus on technical aspects, while others emphasize governance, compliance, and security awareness. This indicates that the future of cloud computing security requires a combination of technical, regulatory, and human solutions.

Sixth: The Research Gap Revealed by Comparative Analysis

Despite the abundance of studies addressing cloud computing security, several research gaps remain, most notably:

1. The lack of a complete consensus on ranking security threats according to their severity and impact across different cloud models.
2. The focus of some studies on a single security technology without providing a comprehensive framework that integrates encryption, identity management, monitoring, and response.
3. The limited number of studies that comprehensively compare public, private, hybrid, and multi-cloud environments.
4. The need for more studies that measure the balance between security level, performance, cost, and scalability.
5. The weak connection between modern security solutions and the practical challenges related to compliance, privacy, and governance.
6. The need for a more accurate assessment of the role of artificial intelligence in threat detection, taking into account the risks of malicious attacks, bias, and privacy concerns.

7. The scarcity of studies that synthesize the findings of previous literature into a unified analytical framework linking threats, mitigation strategies, and future trends.

6.2 Comparison Summary

This comparison reveals that previous studies agree that cloud computing security presents a multidimensional challenge, encompassing data, applications, infrastructure, users, and compliance. They also concur on the importance of encryption, identity management, and continuous monitoring, with increasing interest in artificial intelligence, zero-trust, and post-quantum cryptography. However, these studies differ in scope, methodology, and targeted environments, justifying the current research as a comprehensive systematic review of security threats, protection strategies, and future trends in cloud computing.

7. Results

Based on the results of the systematic literature review, and after reviewing 25 research papers and selecting 17 studies for final analysis, the results were organized into six main categories: characteristics of the included studies, security threats, protection strategies, emerging technologies, future trends, and research gaps. This classification reflects the nature and diversity of the selected studies in terms of their scope, the threats they addressed, the protection mechanisms they proposed, and the emerging technologies they focused on.

7.1 Characteristics of the Included Studies

The review process revealed that the included studies differed in their scope, objectives, and methodologies. Some studies addressed cloud computing security in general, while others focused on specific aspects, such as data security and privacy, encryption, multi-cloud and hybrid cloud environments, and cloud computing security related to the Internet of Things (IoT).

The studies included systematic reviews, literature reviews, surveys, and specialized technical studies. For example, some studies focused on threat analysis and mitigation strategies, while others focused on specific protection technologies or on identifying future trends and research gaps.

The studies also showed a growing interest in the security of advanced cloud environments, including multi-cloud and hybrid environments, cloud computing connected to the Internet of Things (IoT), and specialized applications such as cloud energy storage systems.

Overall, the characteristics of the studies included indicate a shift in research focus from studying traditional threats to studying more complex cloud environments, with an emphasis on integrating modern security technologies with governance, privacy, and compliance.

7.2 Security Threats

The review results showed that data security and privacy were the most frequently recurring themes in the studies included. The results also revealed a wide range of threats facing cloud computing environments, the most prominent of which can be categorized as follows:

1. Data Breaches and Leaks: These represent one of the most prominent risks addressed in the studies, particularly regarding the unauthorized disclosure, manipulation, or loss of control over data.

2. Poor Cloud Resource Configuration: Incorrect configuration of cloud resources and services can expose data and services to unauthorized access.

3. Account Hijacking and Weak Authentication: Seizing user accounts and gaining unauthorized access to cloud resources is a recurring threat in the literature.

4. DoS/DDoS Attacks: Several studies have addressed attacks targeting the availability and continuity of cloud services.

5. Malware and Ransomware: These pose a threat to cloud data and systems and can lead to service disruptions or data loss.

6. Insecure APIs: Inadequately protected APIs represent a vulnerability that can be exploited to access services and data.

7. Insider Threats: These are related to the misuse of privileges or unauthorized access by users with privileges within the cloud environment.

8. Privacy and Data Protection Risks: These risks are related to data storage and processing at cloud service providers, in addition to data protection and regulatory compliance requirements.

9. Multi-Cloud and Hybrid Environment Risks: Security challenges increase as data and services are distributed across multiple environments or providers.

10. IoT Risks: Integrating IoT devices with cloud services increases the number of potential entry points and the complexity of the security environment.

These findings confirm that security threats in cloud computing are not limited to a single layer, but rather encompass data, infrastructure, applications, networks, accounts, and users. Studies have identified threats such as account compromise, malware, data leaks, DoS/DDoS attacks, and social engineering.

7.3 Protection Strategies

The studies included demonstrate that protecting cloud computing environments relies on a comprehensive set of technical and organizational mechanisms, not a single technology. Among the most prominent protection strategies repeatedly mentioned in studies are:

- Encryption: Encryption is one of the most widely used data protection mechanisms in the literature, especially for protecting data confidentiality during storage, transmission, and processing. Some studies have also addressed the use of symmetric encryption and secret-sharing techniques to reduce the risk of unauthorized disclosure.
- Identity and Access Management (IAM): Studies have demonstrated the importance of managing user identities and controlling permissions to limit unauthorized access. This

strategy includes defining user permissions, implementing the principle of least privilege, and strengthening authentication mechanisms.

- Multi-Factor Authentication: Multi-factor authentication is an important way to reduce the risk of account hijacking, especially when accessing cloud resources and services remotely.
- Continuous Monitoring and Vulnerability Management: Studies have emphasized the importance of continuous system monitoring, detecting abnormal activity, conducting periodic vulnerability assessments, and using Security Information and Event Management (SIEM) systems.
- Zero Trust Architecture: Zero Trust architecture has emerged as a modern strategy that relies on continuous verification of users, devices, and resources, rather than assuming trust simply because a user is present within the organizational environment.
- Artificial Intelligence and Machine Learning: Studies have shown increasing interest in using artificial intelligence and machine learning to detect anomalies, predict threats, and improve the speed of response to security incidents.
- Backup and Disaster Recovery: Backup and disaster recovery plans are a critical component of any data protection and business continuity strategy, especially in the face of malware, ransomware, and data loss.

Therefore, the findings indicate that the best approach to protecting cloud computing is a multi-layered approach that combines encryption, identity and access management, continuous monitoring, incident response, and security governance.

7.4 Emerging Technologies

The review revealed a growing interest in a range of emerging technologies that can contribute to the development of cloud computing security. These include:

1. Artificial Intelligence and Machine Learning: for threat detection, behavior analysis, and the detection of anomalous activity.
2. Zero Trust: for implementing continuous verification and reducing the risk of unauthorized access.
3. Blockchain: for supporting data integrity and mitigating some of the risks associated with centralized trust.
4. Confidential Computing: for protecting data during processing.
5. Post-Quantum Cryptography: for addressing future threats related to the development of quantum computing.
6. Federated Learning: for developing AI models while minimizing the need to share original data.
7. Differential Privacy: for enhancing privacy during data analysis.
8. Automation-based technologies: for improving the speed of threat detection and response.

Some recent studies have focused specifically on Zero Trust, artificial intelligence, and advanced cryptography, while others have addressed quantum computing-resistant cryptography, federated learning, and differential privacy.

These findings indicate that cloud security is gradually shifting towards smarter, more proactive solutions, rather than relying solely on traditional protection methods.

7.5 Future Trends

The results of the studies included reveal several key future trends in cloud security, which can be summarized as follows:

1. Increased reliance on artificial intelligence and machine learning for threat detection and automated incident response.
2. Expansion of Zero Trust as a suitable security model for distributed cloud environments.
3. Moving towards quantum-resistant encryption in preparation for future threats.
4. Developing privacy protection technologies that allow data to be used and analyzed while minimizing the risk of disclosure.
5. Increased focus on the security of multi-cloud and hybrid environments due to their increasing prevalence in enterprises.
6. Enhancing the security of cloud-IoT integration due to the growing number and diversity of connected devices.
7. Developing more automated and responsive real-time security mechanisms.
8. Strengthening security, compliance, and governance standards in cloud environments.
9. Developing integrated security models that combine technical protection, risk management, and governance. Achieving a balance between security, performance, cost, and scalability when implementing security solutions.
10. Recent studies indicate that the future trend is not limited to developing new defensive technologies, but rather focuses on building more flexible security frameworks capable of adapting to evolving threats.

7.6 Research Gaps

The systematic review revealed several gaps requiring further research, most notably:

1. Lack of Integrated Security Frameworks: Many studies focus on specific threats or technologies, while there is a need for integrated frameworks that link the type of threat, the protection mechanism, and the cloud environment used.

2. The Need for More Empirical Studies: There is a need for empirical studies that measure the effectiveness of security technologies in terms of protection level, performance, cost, and scalability.

3. Limited Comparative Studies Between Cloud Environments: There is a need for studies that systematically compare public, private, hybrid, and multi-cloud environments in terms of security risks and protection mechanisms.

4. Artificial Intelligence Challenges: Despite the significant potential of artificial intelligence in threat detection, issues such as malicious attacks, model accuracy, privacy, and computational cost still need to be addressed. Studies have indicated that malicious attacks represent a crucial area requiring further research.

5. Security of Multi-Cloud and Hybrid Environments: These environments require further research in areas such as data sharing, identity management, security policy standardization, and compliance across different service providers.

6. Cloud Computing and IoT Security: The proliferation and diversity of IoT devices present additional challenges, particularly regarding real-time threat detection and scalability.

7. Quantum-Resistant Cryptography: Further research is needed on how to integrate quantum-resistant cryptography into existing cloud architectures while maintaining performance and applicability.

8. Organizational and Human Aspects: The gaps are not limited to the technical aspect; Further research is needed on user security awareness, governance, accountability, and compliance with data protection laws and regulations. Some studies have highlighted the importance of security awareness and collaboration among different stakeholders.

Overall, research gaps indicate a need to move from studies addressing a single security problem to comprehensive, empirical studies capable of evaluating cloud computing security from an integrated perspective that encompasses threats, protection, performance, privacy, governance, and scalability.

8. Discussion

The results of this systematic review indicate that cloud computing security has become a multidimensional challenge that is not limited to protecting data or network infrastructure, but extends to technical, organizational, and operational aspects. This reflects the nature of modern cloud environments that depend on continuous interaction between users, applications, cloud services, and resource management mechanisms. Hence, achieving a high level of security requires an integrated approach rather than relying on a single security mechanism.

The review demonstrates that security threats in the cloud environment do not operate independently, but can be interconnected. A weak security component may increase the impact of other threats. For example, poor identity and permissions management can facilitate unauthorized access to resources, while cloud service setup errors can expose data even with some other protection mechanisms in place. This indicates that the security of the cloud environment should be treated as an interconnected system in which the effectiveness of each security mechanism is affected by its level of integration with the rest of the system components.

The results also reveal a gradual shift from the concept of traditional preventive protection to the concept of continuous and adaptive security. Although encryption, identity management, and multi-factor authentication remain important, the complexity of modern cloud environments requires continuous monitoring, detection, and response capabilities. In this context, the concept of **Zero Trust** and the use of **Artificial Intelligence and Machine Learning** emerge as two trends that reflect a change in the way risks are managed, through continuous verification of activities and authorizations and responding to changes in the threat level.

The review also notes that the expanding use of multi-cloud and hybrid cloud environments, along with the integration of IoT with cloud services, increases the complexity of protecting data and resources. The diversity of platforms and services poses challenges related to identity management, data transfer, consistent application of security policies, and compatibility between different service providers. Therefore, protection mechanisms designed for a single cloud environment may not be sufficient to handle distributed and multiple environments, which reinforces the need for security frameworks capable of working across different environments while maintaining a consistent level of protection.

On the other hand, the results show that emerging technologies hold important potential to enhance security and privacy, but at the same time they pose new challenges. The introduction of technologies such as artificial intelligence, block chain, confidential computing, federated learning, and privacy protection technologies may contribute to the development of protection, detection, and response capabilities, but their practical application is related to issues such as computational cost, scalability, compatibility between systems, transparency, and trust. Therefore, emerging technology should not be viewed as a standalone security solution, but rather as part of an integrated security architecture that should be evaluated according to the needs of the cloud environment.

The issue of balancing security with operational requirements also arises. Increased security controls and procedures may impact performance, cost, and scalability, especially in large-scale cloud environments. Hence, the effectiveness of a security solution should not be measured only by its ability to prevent threats, but rather its operational efficiency, cost, ability to expand, and suitability to the nature of the environment in which it is applied must be taken into account.

The review also indicates that technical solutions, although important, are not sufficient alone to ensure the security of cloud computing. The effectiveness of security measures is also related to institutional policies, authority management, user awareness, governance, and compliance with regulatory requirements. Therefore, the presence of advanced security technologies may not achieve the required level of protection if it is not accompanied by appropriate application of policies and procedures and a clear definition of security responsibilities within the organization.

Accordingly, it can be said that the future trend of cloud computing security is towards developing integrated, adaptive and scalable** security models, capable of dealing with changing threats in different cloud environments. There is also a need for more applied studies that test the effectiveness of these models in realistic environments, rather than being limited to theoretical and conceptual studies. This shows that future development in this field does not depend only on the innovation of new security technologies, but rather on the ability to integrate technologies, organizational and human procedures within a unified security framework that achieves a balance between security, performance, cost and scalability.

Thus, the main addition of this systematic review is to provide a coherent view of cloud computing security, by combining the nature of security threats, protection mechanisms, emerging

technologies, future trends, and research gaps, which helps to understand the development of the field and identify aspects that need further research and development.

9.Recommendations

1. Enhance data protection through encryption, privacy management, and adherence to security standards.
2. Implement multi-factor authentication, the principle of least privilege, and the zero-trust principle.
3. Conduct regular security configuration checks, update systems, and address vulnerabilities.
4. Enable continuous monitoring, early attack detection, and incident response plans.
5. Unify security policies across hybrid and multi-cloud environments and clearly define responsibilities.
6. Leverage artificial intelligence and emerging technologies to enhance protection, while evaluating their effectiveness and cost.
7. Organize awareness and training programs for employees and conduct regular penetration testing and security audits.
8. Support future research on post-quantum cryptography, confidential computing, and privacy protection.

10. Conclusion

This research concluded that cloud computing security is essential for protecting data and ensuring the continuity of digital services. The analyzed studies revealed that cloud environments face multiple threats, most notably data breaches, misconfiguration, account hijacking, malware, denial-of-service attacks, weak APIs, and privacy risks in hybrid and multi-cloud environments.

The findings also indicated that addressing these threats requires an integrated security strategy that combines encryption, identity and access management, multi-factor authentication, continuous monitoring, vulnerability management, and incident response, along with the implementation of a zero-trust principle and clear accountability between organizations and cloud service providers. The review further showed that artificial intelligence and machine learning, confidential computing, post-quantum cryptography, and privacy protection technologies represent promising trends for enhancing cloud security.

Therefore, achieving effective and sustainable cloud security requires the integration of technical, organizational, and human aspects, continuous updating of security policies, and the development of flexible solutions that adapt to evolving threats. The study also recommends continuing applied research to evaluate the effectiveness of modern technologies, achieving a balance between security, performance and cost, and bridging research gaps related to hybrid and multi-cloud environments and privacy protection.

11. References

1. Ahmad, W. (2024). Trends and Challenges in Securing Cloud Computing Environments: An Overview of Current Technologies. *Premier Journal of Computer Science*. https://doi.org/10.70389/PJCS.100004

2. Ahmadi, S. (2024). A Systematic Review of the Literature on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security, 15(2), 148–167. https://doi.org/10.4236/jis.2024.152010

3. Ahmadi Pour, M., & Ahmadi Pour, M. (2026). Cybersecurity in Cloud Energy Storage Systems: A Comprehensive Review of Challenges and Future Trends. *Computers & Security*. https://doi.org/10.1016/j.cose.2026.105090

4. Alhadi, F. E., Al-Shaibani, N. A., and Al-Hamdil, S. A. (2024). A survey on cloud computing security. *Sana'a University Journal of Applied Sciences and Technology, 2*(4), 381–390. https://doi.org/10.59628/jast.v2i4.1025

5. Ali, S., Wadu, S. A., Yishit, A., Ghan, M. L., and Li, S. K. (2024). Enhancing cloud computing security: Unveiling the preventative potential of symmetric secret sharing technology in secure cloud computing. *Egyptian Journal of Informatics, 27*, 100519. https://doi.org/10.1016/j.eij.2024.100519

6. Ali, S., et al. (2025). Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Trends. *Computers & Security*. https://doi.org/10.1016/j.cose.2025.104599

7. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic review of the literature on cloud computing security: threats and mitigation strategies. *IEEE Access, 9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

8. Adeniji, S. A., Oke, F., Okolo, J., and Dobamo, A. (2025). Cybersecurity in the Age of Cloud Computing and the Internet of Things: Emerging Threats and Advanced Protection Technologies [Preliminary Version]. *TechRxiv*. https://doi.org/10.36227/techrxiv.175459370.08259901

9. Balboni, B., Taborda Barata, M., Bella, J., & Caparelli, F. (2025). Cloud Security Trends. In *The Computer and Information Security Handbook* (4th ed., pp. 1093–1108). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00066-7

10. Barbara, T. (2023). *Assessing Future Development Needs in Cloud Computing Cybersecurity: A Systematic Review of the Literature* [Master's Thesis, University of Malta].

11. Chen et al. (2025). Cloud Computing Security: Addressing Evolving Threats in the Digital Age [Preliminary Edition].

12. Dawood et al, (2023). Cyberattacks and Cloud Security: A Comprehensive Review. *Symmetry, 15*(11), 1981. https://doi.org/10.3390/sym15111981

13. Khalifa, N., and Al-Madani, W. (2024). Security in Cloud Computing: Threats, Mitigation Strategies, and Future Trends. *IET Conference Proceedings*, 2023(44). https://doi.org/10.1049/icp.2024.0974

14. Mastry, H. K., Mavani, S., Patel, R., and Goswami, A. (2024). Cloud Security Risks and Mitigation Strategies: A Review of Current Trends and Future Directions. *Journal of Basic Science and Engineering, 21*(1). https://doi.org/10.10399/JBSE.2025295959

15. Singh Sanger, A. K., & Johari, R. (2024). A Survey on Cloud Computing Security Issues. *AIP Conference Proceedings, 2919*(1), 120006. https://doi.org/10.1063/5.0175034

16. Thatikonda, F. K. (2023). Data security in cloud computing: challenges, solutions, and future trends. *Journal of Modern Data Science and Technology, 2*, 1–6.

17. Zanjiabadi Zadeh, H., Ghasemi, M., Vazifeh Doost, F., Qadkhoda Dehkhani, S., & Rahmani, M. (2023). Cloud computing security: a review of basic concepts, challenges, issues, requirements, security standards, and types of attacks in cloud computing. *Computing and Distributed Systems, 6*(1), 137–153.