Emirates International University EIU

Research Article

Emirates International University Journal Issued. (5) .(2026)

(2026) . (5) مجلة الجامعة الإماراتية الدولية. العدد

Security Challenges and Solutions in Cloud Computing Environments: A Comprehensive Review.

Amat AL-latif H. Abo-Torkhoma*[1], Abd AL-latif H. Abo-Torkhoma [2] , Gameil S. H. Ali [3]

1. *Information Technology Department, Faculty of Education and Applied Science - Arhab, Sana'a University, Sana'a, Yemen. amatallatifhezam@gmail.com*
2. *Information Technology Department, Faculty of Education and Applied Science - Arhab, Sana'a University, Sana'a, Yemen , abdalaltifhezam2002@gmail.com .*
3. *Head of Artificial Intelligence and Data Science Department, 21 September University of Medical and Applied Sciences, Sana'a, Yemen , gameilsaad01@gmail.com .*

Abstract

Cloud computing has become a fundamental paradigm for delivering scalable, flexible, and cost-effective computing resources through Internet-based platforms. Its rapid adoption across various sectors has enhanced operational efficiency, resource utilization, and service delivery. Despite these advantages, cloud environments continue to face significant security challenges that threaten the confidentiality, integrity, and availability of data and services. This review examines the major security threats affecting cloud computing environments, including data breaches, account hijacking, insider threats, insecure application programming interfaces (APIs), cloud misconfigurations, distributed denial-of-service (DDoS) attacks, multi-tenancy risks, and regulatory compliance issues. The study also analyzes the security implications associated with different cloud services and deployment models. Furthermore, it reviews contemporary security mechanisms and mitigation strategies, including encryption techniques, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM), Artificial Intelligence-based security systems, DevSecOps practices, and Confidential Computing. In addition, the strengths and limitations of existing approaches are critically discussed, while emerging trends, research gaps, and future research directions are highlighted. By synthesizing recent developments in cloud security, this review provides researchers, practitioners, and decision-makers with a comprehensive understanding of current challenges and promising solutions for securing modern cloud computing environments.

Keywords

Cloud Computing, Cloud Security, Cybersecurity, Zero Trust Architecture, Identity and Access Management, Multi-Cloud Security.

Received	**01/01/2026**
Accepted	**01/01/2026**
Published	**31/07/2026**
Publisher	**Emirates International University**

ISSN	**3104-6142**
ISSN (Online)	**3104-6150**
DOI	10.64059/eiu.v3i1.227
Wikidata	Q137945151
ROR	03j6pc929

Citation:

Abo-Torkhoma, A. A.- latif H., Abo-torkhoma, A. A.-latif H., & Ali, G. S. H. (2026). Security Challenges and Solutions in Cloud Computing Environments: A Comprehensive Review. Emirates International University Journal, 3(1), 15. https://doi.org/10.64059/eiu.v3i1.227

Corresponding author

Amat AL-latif H. Abo-Torkhoma, Information Technology Department, Faculty of Education and Applied Science - Arhab, Sana'a University, Sana'a, Yemen. amatallatifhezam@gmail.com

Code:

9773104615005

التحديات والحلول الأمنية في بيئات الحوسبة السحابية: مراجعة شاملة

امة اللطيف حزام أبو ترخمة* [1] ، عبد اللطيف حزام أبو ترخمة[2] ، جميل سعد علي [3]

1. قسم تقنية المعلومات، كلية التربية والعلوم التطبيقية – أرحب، جامعة صنعاء، صنعاء، اليمن amatallatifhezam@gmail.com
2. قسم تقنية المعلومات، كلية التربية والعلوم التطبيقية – أرحب، جامعة صنعاء، صنعاء، اليمن ، abdalaltifhezam2002@gmail.com
3. رئيس قسم الذكاء الاصطناعي وعلوم البيانات، جامعة 21 سبتمبر للعلوم الطبية والتطبيقية، صنعاء، اليمن gameilsaad01@gmail.com

الملخص

أصبحت الحوسبة السحابية نموذجًا أساسيًا لتوفير موارد حوسبية قابلة للتوسع ومرنة وفعالة من حيث التكلفة، وذلك من خلال منصات تعتمد على الإنترنت. وقد أسهم الانتشار السريع للحوسبة السحابية في مختلف القطاعات في تعزيز الكفاءة التشغيلية، وتحسين استغلال الموارد، والارتقاء بمستوى تقديم الخدمات. وعلى الرغم من هذه المزايا، لا تزال البيئات السحابية تواجه تحديات أمنية جوهرية تهدد سرية البيانات وسلامتها وتوافرها، فضلًا عن تهديد الخدمات المستضافة عليها.

تستعرض هذه الدراسة أهم التهديدات الأمنية التي تؤثر في بيئات الحوسبة السحابية، بما في ذلك اختراقات البيانات، والاستيلاء على الحسابات، والتهديدات الداخلية، وعدم أمان واجهات برمجة التطبيقات (APIs)، وسوء تهيئة البيئات السحابية، وهجمات حجب الخدمة الموزعة (DDoS)، والمخاطر المرتبطة بتعدد المستأجرين، وقضايا الامتثال للمتطلبات واللوائح التنظيمية. كما تحلل الدراسة الآثار الأمنية المرتبطة بمختلف نماذج الخدمات السحابية ونماذج نشر الحوسبة السحابية.

وعلاوة على ذلك، تستعرض الدراسة آليات الأمن السيبراني الحديثة واستراتيجيات الحد من المخاطر، بما في ذلك تقنيات التشفير، وإدارة الهوية والوصول (IAM)، والمصادقة متعددة العوامل (MFA)، وبنية انعدام الثقة (ZTA)، وإدارة الوضع الأمني للحوسبة السحابية (CSPM)، وأنظمة الأمن القائمة على الذكاء الاصطناعي، وممارسات DevSecOps، والحوسبة السرية (Confidential Computing).

إضافة إلى ذلك، تناقش الدراسة بصورة نقدية نقاط القوة والقيود في الأساليب الأمنية الحالية، مع تسليط الضوء على الاتجاهات الناشئة، والفجوات البحثية، والمسارات المستقبلية للبحث العلمي في مجال أمن الحوسبة السحابية. ومن خلال تجميع وتحليل التطورات الحديثة في مجال الأمن السحابي، تقدم هذه المراجعة للباحثين والممارسين وصنّاع القرار فهمًا شاملًا للتحديات الأمنية الراهنة والحلول الواعدة لتعزيز أمن بيئات الحوسبة السحابية الحديثة.

الكلمات المفتاحية

الحوسبة السحابية، أمن الحوسبة السحابية، الأمن السيبراني، بنية انعدام الثقة، إدارة الهوية والوصول، أمن البيئات السحابية متعددة السحب.

Introduction

Cloud computing has become one of the most influential technological innovations in modern information systems. It enables organizations to access computing resources, storage services, and software applications through Internet-based platforms without the need for extensive physical infrastructure. The flexibility, scalability, and cost-effectiveness of cloud computing have contributed to its widespread adoption across sectors, such as healthcare, education, finance, government, and industry (Alouffi et al., 2021), (Soveizi et al., 2023), (Ahmadi, 2024). The rapid growth of digital transformation initiatives, big data analytics, artificial intelligence applications, and Internet of Things (IoT) technologies has further accelerated the adoption of cloud services. Organizations increasingly rely on cloud environments to improve operational efficiency, enhance service availability, and support business continuity. As a result, large volumes of sensitive information and critical applications are now hosted within cloud infrastructure (Ahmadi, 2024), (Cloud Security, 2024a), (Cloud Security, 2024b). Despite these advantages, cloud computing environments face numerous security challenges that may threaten the confidentiality, integrity, and availability of organizational data and services. Common security concerns include data breaches, account hijacking, insider threats, insecure application programming interfaces (APIs), cloud misconfigurations, distributed denial-of-service (DDoS) attacks, and regulatory compliance issues. The growing complexity of multi-cloud and hybrid-cloud environments has further increased the difficulty of managing security risks effectively (Alouffi et al., 2021), (Cloud Security, 2024a), (Chuka-Maduji & Anu, 2021), (Iqbal et al., 2024), (Khan & Zaidi, 2024). To address these challenges, researchers and industry practitioners have proposed various security mechanisms and protection strategies, including encryption technologies, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust

Architecture (ZTA), Cloud Security Posture Management (CSPM), Artificial Intelligence-based threat detection systems, and Confidential Computing technologies. However, the continuously evolving threat landscape requires ongoing research and evaluation of existing security approaches (Gambo & Almulhem, 2025), (Feng et al., 2024), (Ahmed, 2023), (Pratik, 2025).

This paper provides a comprehensive review of security challenges and solutions in cloud computing environments. It discusses major cloud security threats, examines current protection mechanisms, analyzes emerging security trends, identifies research gaps, and highlights future directions for improving cloud security and resilience.

Literature Review

Cloud computing has transformed how organizations manage, store, and process data by providing scalable, on-demand computing resources. Despite its advantages, cloud environments continue to face security challenges that require ongoing research and development. This section reviews cloud computing models, major security threats, and the security solutions proposed in recent literature.

2.1 Cloud Computing Models

Cloud service delivery is commonly organized into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each offering different levels of control and management responsibilities [1], [3], [29].

- Infrastructure as a Service (IaaS) provides virtualized computing resources, such as servers, storage, and networking services. Users maintain control over operating systems and applications while cloud providers manage the underlying physical infrastructure.
- Platform as a Service (PaaS) offers development environments and software platforms that enable developers to build, test, and deploy applications without managing infrastructure components.
- Software as a Service (SaaS) delivers complete software applications over the Internet. Users can access services through web browsers, while providers are responsible for maintaining both the infrastructure and the applications.

Each service model introduces different security responsibilities and challenges depending on the distribution of control between cloud providers and customers (Alouffi et al., 2021; Soveizi et al., 2023).

2.2Security Challenges in Cloud Computing

The increasing adoption of cloud computing has exposed organizations to various cybersecurity threats. These challenges can affect data confidentiality, integrity, and availability, making security a critical concern for cloud users and providers (Alouffi et al., 2021; Chuka-Maduji & Anu, 2021; Alharbi & Alenezi, 2024). Fig. 1 illustrates the major security challenges in cloud computing environments.

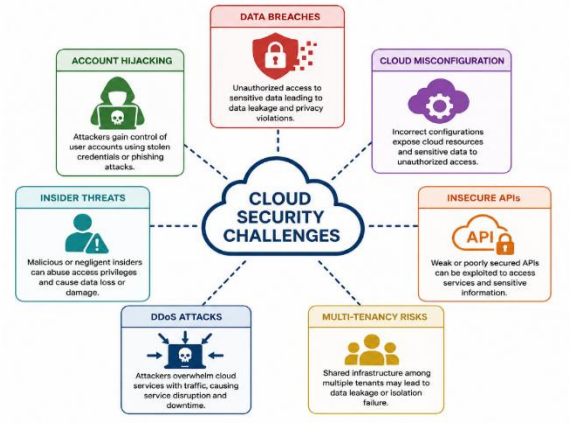

Figure 1:Major Security Challenges in Cloud Computing Environments

Cloud security challenges vary in their causes and impacts on organizations. Understanding these challenges is essential for designing effective protection mechanisms. The major security challenges and their impacts are summarized in Table 1.

Table 1:Major Security Challenges in Cloud Computing

Challenge	Description	Impact
Data Breaches	Unauthorized access to cloud data	Data loss and privacy violations (Alouffi et al., 2021; Cloud Security, 2024a).
Account Hijacking	Compromised user credentials	Unauthorized access violations (Alouffi et al., 2021; Cloud Security, 2024a).
Cloud Misconfiguration	Incorrect security settings	Information exposure (Khan & Zaidi, 2024)
Insider Threats	Malicious or negligent insiders	Data leakage (Alouffi et al., 2021; Chuka-Maduji & Anu, 2021).
Insecure APIs	Vulnerable service interfaces	System compromise violations (Alouffi et al., 2021; Cloud Security, 2024a).
DDoS Attacks	Service disruption attacks	Reduced availability (Cloud Security, 2024a, 2025a).
Multi-Tenancy Risks	Shared infrastructure concerns	Privacy issues (Chuka-Maduji & Anu, 2021; Soveizi et al., 2023).

2.2.1 Data Breaches

Data breaches occur when unauthorized individuals gain access to sensitive information stored in cloud environments. Such incidents may result in financial losses, legal consequences, and reputational damage. As cloud infrastructures store large volumes of valuable information, they remain attractive targets for cybercriminals (Alouffi et al., 2021; Cloud Security, 2024a; Alharbi & Alenezi, 2024).

2.2.2 Account Hijacking

Account hijacking involves the unauthorized acquisition of user credentials through phishing attacks, credential theft, or weak authentication mechanisms. Compromised accounts may provide attackers with direct access to sensitive cloud resources and services (Cloud Security, 2024a; Alshamrani & Bahattab, 2022).

2.2.3 Cloud Misconfiguration

Misconfiguration is one of the most common causes of cloud security incidents. Improperly configured storage services, databases, or access permissions may expose sensitive information to unauthorized users (Alharbi & Alenezi, 2024; Khan & Zaidi, 2024; Ahmed, 2023).

2.2.4 Insider Threats

Insider threats originate from employees, contractors, or trusted individuals who intentionally or unintentionally compromise cloud security. These threats are particularly challenging because insiders often possess legitimate access privileges (Alouffi et al., 2021; Chuka-Maduji & Anu, 2021; Abioye et al., 2021).

2.2.5 Insecure APIs

Application Programming Interfaces (APIs) play a vital role in cloud service integration. However, poorly secured APIs can introduce vulnerabilities that attackers may exploit to gain unauthorized access or manipulate cloud services (Cloud Security, 2024a; Chuka-Maduji & Anu, 2021; Abioye et al., 2021; Theodoropoulos et al., 2023).

2.2.6 Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks attempt to overwhelm cloud resources by generating excessive traffic. These attacks may disrupt service availability and negatively impact business operations (Cloud Security, 2024a, 2025a).

2.2.7 Multi-Tenancy Risks

Cloud providers often use multi-tenant architectures in which multiple customers share physical resources. Although logical isolation mechanisms are implemented, security concerns remain regarding data privacy and tenant isolation (Iqbal et al., 2024; Soveizi et al., 2023).

2.3 Security Solutions in Cloud Computing

To mitigate cloud security threats, researchers and practitioners have developed various protection mechanisms and security frameworks. Fig. 2 presents a comprehensive cloud security protection framework that illustrates the integration of multiple security mechanisms in cloud environments (Alouffi et al., 2021; Gambo & Almulhem, 2025; Feng et al., 2024; Alzoubi et al., 2024).

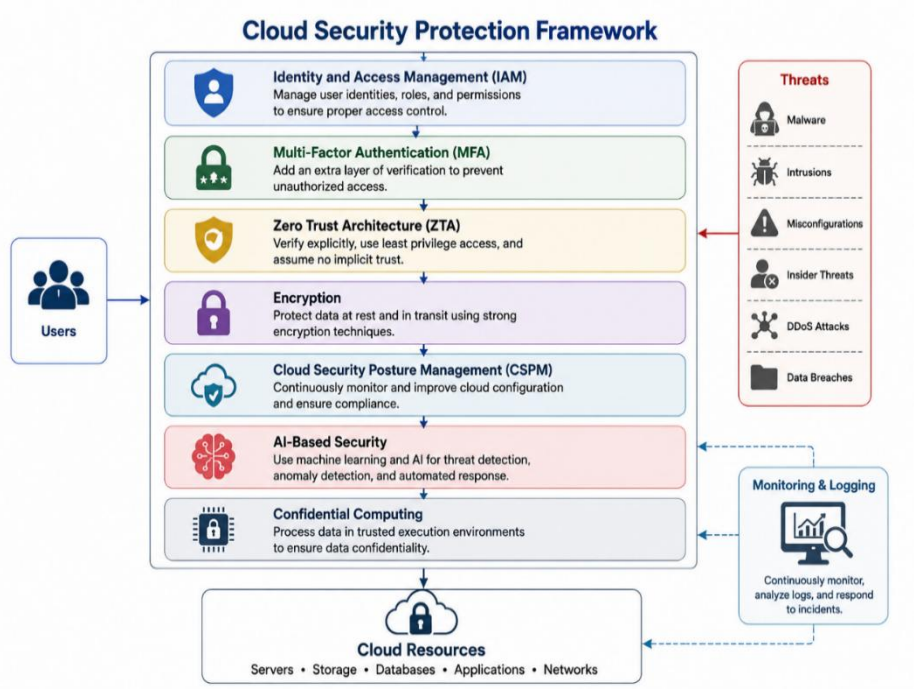

Figure 2 :Cloud Security Protection Framework

Table 2 summarizes the main cloud security solutions, their purposes, advantages, limitations, and publication years.

Table 2:Comparison of Cloud Security Solutions

Solution	Main Purpose	Advantages	**Limitations**	Year
Encryption	Data Protection	Strong confidentiality	Complex cryptographic key distribution and rotation across large-scale multi-cloud environments may increase operational overhead. (Singh & Bhushan, 2025; Albugmi et al., 2024).	2024
IAM	Access Control	Improved governance	Managing identities, roles, and permissions across multiple cloud providers increases administrative complexity and the risk of inconsistent access policies. (Alshamrani & Bahattab, 2022).	2023
MFA	User Authentication	Reduced credential attacks	Authentication fatigue, phishing-resistant implementation requirements, and reduced user convenience may affect adoption. (Mostafa et al., 2023)	2023
Zero Trust	Continuous Verification	Strong security posture	Requires significant architectural changes, continuous monitoring infrastructure, and higher deployment costs in large cloud	2024-2025

			environments. (Gambo & Almulhem, 2025; Godwin & Rahman Akorede, 2024).	
CSPM	Security Monitoring	Automated detection	It cannot prevent identity-based attacks and depends on accurate cloud configuration visibility for effective risk detection. (Khan & Zaidi, 2024; Ahmed, 2023).	2023
AI-Based Security	Threat Detection	Real-time analysis	Model accuracy depends on high-quality training data and may generate false alarms or biased security decisions. (Alzoubi et al., 2024; Uddoh et al., 2021).	2024–2025
Confidential Computing	Data-in-Use Protection	Enhanced privacy	Performance overhead, hardware dependency, and limited interoperability across heterogeneous cloud platforms may restrict large-scale adoption. (Feng et al., 2024), (Sinan et al., 2025).	2023–2024

2.3.1 Encryption Techniques

Encryption remains one of the fundamental security mechanisms for protecting sensitive information in cloud computing environments. It safeguards data both at rest and in transit by ensuring that only authorized entities possessing the appropriate cryptographic keys can access protected information (Singh & Bhushan, 2025; Albugmi et al., 2024; Arif et al., 2025).

Although encryption provides strong protection for data confidentiality, it does not eliminate all cloud security risks. Encryption alone cannot prevent attacks resulting from compromised user credentials, insecure application programming interfaces (APIs), insider threats, or cloud service misconfigurations. Furthermore, managing cryptographic keys across distributed and multi-cloud environments introduces significant operational complexity, particularly for organizations handling large-scale cloud infrastructures (Albugmi et al., 2024; Zhang & Zhang, 2024).

Compared with other security mechanisms such as Identity and Access Management (IAM) and Zero Trust Architecture (ZTA), encryption primarily protects the confidentiality of data, whereas IAM controls user identities and permissions, and ZTA continuously verifies every access request regardless of user location. Therefore, encryption is most effective when integrated with complementary security approaches rather than being deployed as a standalone protection mechanism.

2.3.2 Identity and Access Management (IAM)

Identity and Access Management (IAM) is a fundamental component of cloud security that ensures only authorized users can access cloud resources and services. IAM enables organizations to define user identities, assign roles and permissions, and enforce authentication and authorization policies, thereby reducing the risk of unauthorized access and privilege misuse (Pratik, 2025; Alshamrani & Bahattab, 2022; Mostafa et al., 2023).

Despite its critical role, traditional IAM solutions face several challenges in modern cloud environments. Managing identities across multiple cloud providers, hybrid infrastructures, and third-party applications increases administrative complexity and may lead to inconsistent access policies. In addition, static access control models may not effectively respond to evolving cyber threats or compromised user credentials, particularly in highly dynamic cloud environments (Pratik, 2025; Alshamrani & Bahattab, 2022).

Compared with encryption, IAM focuses on controlling access rather than protecting the confidentiality of stored data. Compared with Zero Trust Architecture (ZTA), IAM establishes user authentication and authorization policies, whereas ZTA continuously validates every user, device, and access request throughout the session. Consequently, IAM should be integrated with continuous verification mechanisms, multi-factor authentication (MFA), and Zero Trust principles to provide stronger protection against sophisticated cloud attacks.

2.3.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) has become one of the most widely adopted security mechanisms for protecting cloud accounts against unauthorized access. By requiring users to verify their identities using two or

more authentication factors, such as passwords, biometric verification, or one-time security codes, MFA significantly reduces the risk of credential theft and account compromise (Mostafa et al., 2023).

Despite its effectiveness, MFA is not a comprehensive solution against all cloud security threats. Sophisticated phishing attacks, session hijacking, and social engineering techniques can still bypass certain MFA implementations. Moreover, deploying MFA across large organizations may introduce additional administrative overhead, increase implementation costs, and affect user convenience, particularly when legacy systems do not fully support modern authentication protocols (Gambo & Almulhem, 2025; Mostafa et al., 2023).

Compared with Identity and Access Management (IAM), which defines user identities and access privileges, MFA strengthens the authentication process by providing additional identity verification. However, unlike Zero Trust Architecture (ZTA), which continuously validates user behavior and device trust throughout each session, MFA generally performs verification only during login. Therefore, integrating MFA with IAM and Zero Trust principles provides stronger protection against evolving cloud cyber threats than relying on MFA alone.

2.3.4 Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) has emerged as an advanced security paradigm that addresses the limitations of traditional perimeter-based security models. Instead of assuming that users or devices operating within a network are trustworthy, ZTA requires every access request to be continuously authenticated, authorized, and validated regardless of its origin (Gambo & Almulhem, 2025; Godwin & Rahman Akorede, 2024; Shin et al., 2025).

The adoption of ZTA significantly enhances cloud security by minimizing unauthorized access and reducing the potential impact of compromised credentials. However, implementing Zero Trust in large-scale cloud infrastructures is often associated with considerable technical and organizational challenges. Existing applications may require architectural modifications, while integrating identity management, continuous monitoring, and policy enforcement across heterogeneous cloud environments can increase deployment time and operational costs (Gambo & Almulhem, 2025; Mushtaq et al., 2025).

Compared with Cloud Security Posture Management (CSPM), which primarily focuses on detecting configuration weaknesses and compliance issues, ZTA provides a proactive approach by continuously evaluating trust before granting resource access. Although CSPM is generally easier to deploy in dynamic cloud environments, ZTA offers stronger protection against identity-based attacks and lateral movement within cloud infrastructures. Consequently, many organizations combine ZTA with CSPM and Identity and Access Management (IAM) to establish a more resilient and adaptive cloud security strategy (Gambo & Almulhem, 2025; Ahmed, 2023; Godwin & Rahman Akorede, 2024).

2.3.5 Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) has become an essential security solution for organizations operating in public, private, and multi-cloud environments. CSPM platforms continuously assess cloud resources, identify security misconfigurations, monitor compliance requirements, and provide automated recommendations to reduce vulnerabilities before they can be exploited (Khan & Zaidi, 2024; Ahmed, 2023).

Despite these advantages, CSPM should not be considered a complete security solution. Its effectiveness largely depends on the accuracy of cloud configuration data and the organization's ability to respond promptly to identified risks. Furthermore, CSPM primarily focuses on configuration management and compliance monitoring rather than on protecting against identity-based attacks, insider threats, or advanced persistent threats. Consequently, relying solely on CSPM may leave critical security gaps in complex cloud infrastructures (Khan & Zaidi, 2024; Ahmed, 2023).

Compared with Zero Trust Architecture (ZTA), CSPM is generally easier to deploy and requires fewer architectural changes, making it particularly suitable for organizations adopting multi-cloud services. However, while CSPM emphasizes continuous visibility into cloud configurations, ZTA focuses on continuously validating users, devices, and access requests before granting resource access. Therefore, combining CSPM with Zero Trust

principles enables organizations to achieve both proactive configuration management and stronger access control, resulting in a more comprehensive cloud security strategy.

2.3.6 Artificial Intelligence-Based Security

Artificial Intelligence (AI) has become an increasingly important component of modern cloud security by enabling intelligent threat detection, anomaly identification, and automated incident response. Unlike conventional rule-based security systems, AI-driven approaches analyze large volumes of cloud-generated data to identify complex attack patterns and previously unknown threats in near real time, thereby improving the efficiency of security monitoring (Alzoubi et al., 2024; Uddoh et al., 2021; Le et al., 2025).

Nevertheless, the effectiveness of AI-based security solutions depends heavily on the quality, diversity, and timeliness of the training data. Poor-quality datasets, adversarial attacks, and biased learning models may reduce detection accuracy and increase false-positive or false-negative rates. In addition, many AI models operate as black-box systems, making it difficult for security analysts to interpret or justify automated security decisions, particularly in critical cloud infrastructures (Alzoubi et al., 2024; Uddoh et al., 2021).

Compared with traditional signature-based detection mechanisms, AI-based security systems provide greater adaptability to emerging cyber threats and continuously evolving attack techniques. However, unlike Cloud Security Posture Management (CSPM), which focuses on identifying configuration weaknesses, AI-based security emphasizes behavioral analysis and predictive threat detection. Therefore, integrating AI with CSPM, Zero Trust Architecture, and Identity and Access Management can significantly strengthen cloud security by combining proactive monitoring, intelligent threat analysis, and continuous access verification.

2.3.7 Confidential Computing

Confidential Computing has emerged as an advanced security approach designed to protect sensitive data while it is being processed, addressing a security gap that conventional encryption techniques cannot fully eliminate. By utilizing Trusted Execution Environments (TEEs), Confidential Computing isolates applications and data from unauthorized access, including privileged users and system administrators, thereby strengthening data privacy during computation (Feng et al., 2024; Arif et al., 2025; Anasuri, 2023).

Despite its strong security capabilities, the adoption of Confidential Computing is still constrained by several practical limitations. Performance overhead, hardware dependency, interoperability issues, and limited support across heterogeneous cloud platforms remain significant challenges for organizations seeking large-scale deployment. These factors may increase implementation costs and complicate integration with existing cloud infrastructures (Feng et al., 2024; Anasuri, 2023).

Compared with encryption, which primarily secures data at rest and during transmission, Confidential Computing extends protection to data while it is actively processed. However, unlike Zero Trust Architecture (ZTA) and Identity and Access Management (IAM), which focus on controlling user access and identity verification, Confidential Computing focuses on safeguarding computational environments. Consequently, combining Confidential Computing with encryption, IAM, and Zero Trust principles enables organizations to achieve comprehensive protection across the entire data lifecycle, including storage, transmission, processing, and access control.

2.3.8 DevSecOps and Cloud-Native Security

DevSecOps has emerged as a modern software development paradigm that integrates security practices throughout the software development lifecycle rather than treating security as a final testing phase. By embedding automated security checks into Continuous Integration and Continuous Deployment (CI/CD) pipelines, organizations can identify vulnerabilities earlier, improve software quality, and reduce the likelihood of security incidents in cloud-native environments (Sinan et al., 2025; Mohammed et al., 2025; Saleh et al., 2024).

Recent research also emphasizes the use of quantitative security metrics and continuous security monitoring to evaluate the effectiveness of DevSecOps practices and support secure software delivery (Zhang & Zhang, 2024; Carlos Bautista Ramos & Yoo, 2025). Furthermore, cloud-native environments increasingly rely on automated

orchestration technologies that require security controls capable of adapting to dynamic workloads and containerized applications (Deng et al., 2024; Silverthorne, 2024).

Despite these advantages, DevSecOps implementation still faces several challenges, including tool integration complexity, organizational readiness, and maintaining security without slowing software delivery. Emerging technologies, such as automated security analytics, Zero Trust principles, and intelligent cloud-native security tools are expected to further strengthen DevSecOps adoption in future cloud computing environments (Shin et al., 2025; Carlos Bautista Ramos & Yoo, 2025).

2.4Comparative Analysis of Cloud Security Solutions

Although various cloud security solutions provide effective protection mechanisms, their suitability varies depending on the cloud service model and organizational requirements. Security solutions differ in terms of deployment complexity, implementation cost, scalability, and operational effectiveness. For example, Zero Trust Architecture (ZTA) provides continuous verification and strong access control but usually requires significant architectural modifications, making its implementation more complex and costly, particularly in large-scale IaaS environments. In contrast, Cloud Security Posture Management (CSPM) focuses on continuously monitoring cloud configurations and identifying security misconfigurations with relatively lower deployment complexity, making it particularly suitable for dynamic multi-cloud environments. Similarly, encryption techniques provide strong data confidentiality across all service models but require efficient cryptographic key management. Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) improve authentication and authorization processes while introducing administrative overhead. AI-based security mechanisms enhance real-time threat detection and adaptive response but require high-quality training data and computational resources. Table 3 presents a comparative analysis of the major cloud security solutions discussed in this review (Gambo & Almulhem, 2025; Ahmed, 2023; Pratik, 2025; Alzoubi et al., 2024; Albugmi et al., 2024; Mostafa et al., 2023; Uddoh et al., 2021; Arif et al., 2025; Shin et al., 2025; Cloud Security, 2025b).

Table 3 : Comparative Analysis of Cloud Security Solutions

Security Solution	Cost	Deployment Complexity	Scalability	Best Suitable Model	**Main Limitation**
Encryption	Low–Medium	Low	High	IaaS / PaaS / SaaS	Key management (Albugmi et al., 2024)
IAM	Medium	Medium	High	All Models	Administrative complexity (Pratik, 2025; Cloud Security, 2025b)
MFA	Low	Low	High	SaaS / PaaS	User inconvenience (Mostafa et al., 2023)
Zero Trust Architecture	High	High	High	IaaS	Complex deployment (Gambo & Almulhem, 2025; Godwin & Rahman Akorede, 2024; Mushtaq et al., 2025; Dhiman et al., 2024)
CSPM	Medium	Medium	Very High	Multi-Cloud / IaaS	Tool dependency (Ahmed, 2023)
AI-Based Security	High	High	High	Large Cloud Environments	False positives (Alzoubi et al., 2024; Uddoh et al., 2021)
Confidential Computing	High	Medium	Medium	Sensitive Workloads	Performance overhead (Feng et al., 2024; Anasuri, 2023)

Methodology of the Study

This study adopts a structured literature review methodology to provide a comprehensive analysis of security challenges and protection mechanisms in cloud computing environments. The review process followed a systematic approach involving literature identification, screening, eligibility assessment, and qualitative synthesis. Relevant studies were collected from major scientific databases using predefined search strategies and

selection criteria. The methodology was designed to ensure transparency, reproducibility, and comprehensive coverage of recent research on cloud computing security (Alouffi et al., 2021; Soveizi et al., 2023; Ahmadi, 2024).

3.1Data Collection

The reviewed literature was collected from well-known academic databases and digital libraries that publish research in cloud computing, cybersecurity, and information systems. These sources include IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Wiley Online Library, and Google Scholar (Alouffi et al., 2021; Soveizi et al., 2023; Ahmadi, 2024). The search process focused on studies addressing cloud security challenges, cloud threats, data protection, access control mechanisms, security frameworks, and emerging security technologies (Alouffi et al., 2021; Chuka-Maduji & Anu, 2021; Ahmadi, 2024). Various keywords were used during the search process, including Cloud Computing Security, Data Breaches, Identity and Access Management, Zero Trust Architecture, Cloud Security Posture Management, Artificial Intelligence for Cybersecurity, and Confidential Computing (Gambo & Almulhem, 2025; Feng et al., 2024; Alzoubi et al., 2024).

To ensure transparency and reproducibility, the literature selection process followed a structured screening procedure. An initial search identified 145 records across the selected databases. After removing 32 duplicate records, 113 studies remained for title and abstract screening. During the screening phase, 61 studies were excluded because they were unrelated to cloud security or did not satisfy the inclusion criteria. The remaining 52 full-text articles were assessed for eligibility. After detailed evaluation, 25 studies were excluded due to insufficient technical contribution, duplication of findings, or limited relevance to the scope of this review. Consequently, 27 high-quality studies were selected for the final analysis.

3.1.1 Search Strategy

The literature search employed predefined keywords combined with Boolean operators (AND, OR) to improve retrieval accuracy across different academic databases. The search strategy was designed to retrieve recent studies focusing on cloud computing security challenges, protection mechanisms, and emerging security technologies. Search strings were adapted according to the search capabilities of each database while maintaining the same search scope. Representative search strings used during the literature search are presented in Table 4 (Alouffi et al., 2021; Soveizi et al., 2023; Ahmadi, 2024).

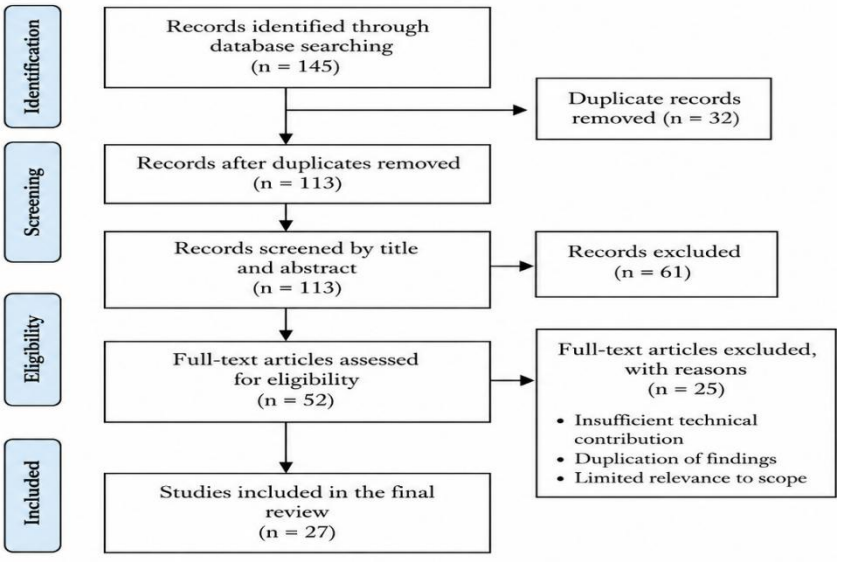

Figure 3 : PRISMA flow diagram illustrating the literature

Fig. 3 illustrates the literature identification, screening, eligibility assessment, and final study selection process adopted in this review.

Table 4 : Search Strategy Used for Literature Collection

Database	Search String
IEEE Xplore	("Cloud Computing Security" OR "Cloud Security") AND ("Security Challenges" OR "Cloud Threats")
ScienceDirect	("Cloud Computing Security") AND ("Security Solutions" OR "Mitigation Strategies")
SpringerLink	("Cloud Security") AND ("Zero Trust Architecture" OR "Identity and Access Management")
ACM Digital Library	("Cloud Computing") AND ("Artificial Intelligence" AND "Cybersecurity")
Wiley Online Library	("Cloud Security") AND ("Confidential Computing" OR "Data Protection")
Google Scholar	("Cloud Computing Security") AND ("Threats" OR "Solutions") AND ("Systematic Review")

3.2Study Selection Criteria

To ensure the relevance and quality of the reviewed literature, specific inclusion and exclusion criteria were considered. Inclusion Criteria:

- Studies related to cloud computing security.
- Peer-reviewed journal articles and conference papers.
- Research discussing cloud security threats, vulnerabilities, or mitigation strategies.
- Studies published in reputable scientific sources.
- Exclusion Criteria:
- Studies unrelated to cloud security.
- Duplicate publications.
- Articles lacking sufficient technical or scientific contributions.
- The selected studies were examined carefully to identify the most significant findings, trends, and security approaches discussed in the literature.

3.3Research Classification

The reviewed studies were classified into several categories based on their primary research focus. These categories include cloud security challenges, access control and authentication mechanisms, cloud security management frameworks, artificial intelligence-based security solutions, privacy-preserving technologies, and emerging cloud security trends (Gambo & Almulhem, 2025; Feng et al., 2024; Alzoubi et al., 2024). This classification facilitated a systematic analysis of existing research and enabled a clearer understanding of the relationships between security challenges and proposed solutions (Alouffi et al., 2021; Soveizi et al., 2023).

3.4 Analysis Approach

The collected studies were analyzed qualitatively by examining their objectives, methodologies, proposed solutions, advantages, limitations, and future recommendations. Comparative analysis was employed to identify common security challenges, evaluate existing protection mechanisms, and highlight areas that require further investigation.

The analysis also focused on identifying emerging technologies and innovative approaches that may contribute to improving security, privacy, and resilience in modern cloud computing environments(Alouffi et al., 2021; Soveizi et al., 2023; Ahmadi, 2024).

Research Gaps and Future Directions

Despite significant advancements in cloud security technologies, several challenges remain unresolved. These limitations continue to affect the effectiveness, scalability, and adaptability of existing security solutions. This section highlights the most important research gaps identified in the literature and discusses potential future directions for improving cloud security.

1.1.Multi-Cloud Security Challenges

The increasing adoption of multi-cloud environments has introduced new security concerns. Organizations often utilize services from multiple cloud providers to improve flexibility and reduce dependency on a single vendor. However, managing security policies, monitoring activities, and maintaining consistent protection mechanisms across heterogeneous cloud platforms remains a challenging task.

Future Work: Future research should focus on developing unified security frameworks capable of providing centralized visibility, automated threat detection, and consistent policy enforcement across multi-cloud environments (Chuka-Maduji & Anu, 2021; Iqbal et al., 2024; Theodoropoulos et al., 2023; Deng et al., 2024).

1.2.Zero Trust Implementation Challenges

Zero Trust Architecture has emerged as one of the most promising security approaches for cloud environments. However, implementing Zero Trust principles in large-scale cloud infrastructures remains complex due to integration difficulties, legacy systems, and operational constraints.

Future Work: Researchers should investigate lightweight and adaptive Zero Trust frameworks that simplify deployment while maintaining strong security controls. Automated policy generation and intelligent access control mechanisms also require further investigation (Gambo & Almulhem, 2025; Shin et al., 2025; Mushtaq et al., 2025).

1.3. Artificial Intelligence Security Limitations

Artificial Intelligence and Machine Learning technologies have demonstrated significant potential for cloud threat detection and security automation. Nevertheless, AI-based security systems remain vulnerable to adversarial attacks, biased training datasets, and false-positive predictions. In addition, the lack of explainability in many machine learning models limits trust and adoption in critical security applications.

Future Work: Future studies should focus on Explainable Artificial Intelligence (XAI), adversarially robust machine learning models, and adaptive security systems capable of responding to evolving cyber threats in real time (Alzoubi et al., 2024; Uddoh et al., 2021; Le et al., 2025).

1.4.Confidential Computing Challenges

Confidential Computing has recently emerged as an important technology for protecting sensitive data during processing. Although Trusted Execution Environments (TEEs) provide strong security guarantees, challenges related to performance overhead, scalability, and interoperability still limit widespread adoption.

Future Work: Further research is needed to improve the efficiency of Confidential Computing technologies and facilitate their integration into large-scale cloud infrastructures (Feng et al., 2024; Anasuri, 2023).

1.5.Regulatory Compliance and Data Privacy

Organizations operating in cloud environments must comply with various regulatory frameworks and data protection requirements. Ensuring compliance across distributed cloud infrastructures remains difficult, particularly for multinational organizations that operate under different legal jurisdictions.

Future Work: Future research should investigate automated compliance monitoring systems and intelligent governance frameworks capable of continuously evaluating cloud environments against evolving regulatory requirements (Cloud Security, 2024a; Alharbi & Alenezi, 2024).

1.6.Future Research Directions

Based on the reviewed literature, several promising research directions can contribute to the development of more secure cloud computing environments. These directions include AI-driven security analytics, autonomous security systems, advanced multi-cloud security frameworks, privacy-preserving technologies, and quantum-resistant cryptographic solutions. In addition, integrating Artificial Intelligence with Zero Trust principles may provide more adaptive and resilient security architectures capable of addressing future cybersecurity challenges

(Iqbal et al., 2024; Gambo & Almulhem, 2025; Feng et al., 2024; Alzoubi et al., 2024; Arif et al., 2025; Shin et al., 2025; Deng et al., 2024).

1.6.1. Quantum-Resistant Cryptography

The emergence of quantum computing presents significant challenges to existing cryptographic algorithms widely used in cloud computing environments. Many current encryption methods, including RSA and Elliptic Curve Cryptography (ECC), may become vulnerable to attacks performed by sufficiently powerful quantum computers. Consequently, future research should focus on the development and adoption of quantum-resistant cryptographic algorithms capable of protecting cloud data against emerging quantum threats. Integrating post-quantum cryptography into cloud security architectures is expected to become an important research direction for ensuring long-term data confidentiality and integrity (Feng et al., 2024). The continuous evolution of cloud technologies requires ongoing research efforts to enhance security, privacy, and trustworthiness while supporting the growing demand for scalable and reliable cloud services.

Conclusion

This review comprehensively examined recent security challenges and protection mechanisms in cloud computing by systematically analyzing studies published between 2023 and 2025. Unlike descriptive surveys that primarily summarize individual security technologies, this study critically compared widely adopted security approaches, including Encryption, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM), Artificial Intelligence (AI)-based security, and Confidential Computing. The comparative analysis highlights that no single solution can adequately address the diverse and evolving threat landscape of modern cloud environments.

The findings indicate that effective cloud security requires a multi-layered defense strategy in which complementary technologies operate together. Encryption and Confidential Computing protect sensitive data throughout its lifecycle; IAM and MFA strengthen identity verification and access control; ZTA minimizes trust-based vulnerabilities through continuous verification; CSPM improves cloud configuration visibility and compliance monitoring, while AI enhances proactive threat detection and response. Integrating these mechanisms provides stronger resilience against sophisticated cyberattacks than relying on any individual technology.

This review also identified several research gaps, including the sslimited integration of AI with Zero Trust frameworks, the operational challenges of securing multi-cloud environments, the scalability constraints of Confidential Computing, and the need for adaptive security models capable of responding to continuously evolving threats. Addressing these challenges represents an important direction for future research and practical cloud security deployments.

Overall, the study provides researchers and practitioners with a structured synthesis of current cloud security solutions, their strengths, limitations, and implementation trade-offs. The presented comparative analysis and identified research opportunities contribute to a clearer understanding of emerging security trends and support the development of more resilient and intelligent cloud computing environments.

References

Alouffi, Bader, Hasnain, Muhammad, Alharbi, Abdullah, Alosaimi, Wael, Alyami, Hashem, & Ayaz, Muhammad. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/access.2021.3073203

Cloud Security, Alliance. (2024a). *Top Threats to Cloud Computing 2024*.

Chuka-Maduji, N., & Anu, V. (2021). Cloud Computing Security Challenges and Related Defensive Measures: A Survey and Taxonomy. *SN Computer Science*, *2*(331).

Iqbal, S., Ahmad, Z., Naeem, W., & Ullah, M. O. (2024). Security Threats and Countermeasures in Cloud. *Kashf Journal of Multidisciplinary Research*, *1*(12), 280–300.

Alharbi, A., & Alenezi, M. (2024). Security and Privacy Challenges in Cloud Computing: A Comprehensive Survey. *Journal of Information Security and Applications*, *78*.

Soveizi, Nafiseh, Turkmen, Fatih, & Karastoyanova, Dimka. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Ahmadi, Sina. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, *15*(02), 148–167. https://doi.org/10.4236/jis.2024.152010

Cloud Security, Alliance. (2024b). Cloud Security in 2024: Addressing the Shifting Landscape. *Cloud Security Alliance Blog*.

Khan, Hamza Mehmood, & Zaidi, Syed Murtaza Haider. (2024). Detecting Security System Misconfiguration Threats in Cloud Computing Environments Using AI. *American Journal of Innovation in Science and Engineering*, *3*(3), 31–40. https://doi.org/10.54536/ajise.v3i3.3272

Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. *IEEE Access*. https://doi.org/10.48550/arXiv.2503.11659

Feng, Dengguo, Qin, Yu, Feng, Wei, Li, Wei, Shang, Ketong, & Ma, Hongzhan. (2024). Survey of research on confidential computing. *IET Communications*, *18*(9), 535–556. https://doi.org/10.1049/cmu2.12759

Ahmed, F. (2023). Cloud Security Posture Management (CSPM): Automating Security Policy Enforcement in Cloud Environments. *ESP International Journal of Advancements in Computational Technology*, *1*(3), 157–166. https://doi.org/10.56472/25838628/IJACT-V1I3P117

Pratik, Jain. (2025). Identity and Access Management in the Cloud. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(2), 1528–1535. https://doi.org/10.32628/cseit25112523

Cloud Security, Alliance. (2025a). *Top Threats to Cloud Computing - Deep Dive 2025*.

Alshamrani, A., & Bahattab, A. (2022). Identity and Access Management in Cloud Computing: A Systematic Review. *IEEE Access*, *10*.

Abioye, T. E., Kolo, A. K., Ahmed, A., Umoru, K., & Alarood, A. A. (2021). Cloud-Based Business Process Security Risk Management. *Applied Sciences*, *11*(12).

Theodoropoulos, Theodoros, Rosa, Luis, Benzaid, Chafika, Gray, Peter, Marin, Eduard, Makris, Antonios, Cordeiro, Luis, Diego, Ferran, Sorokin, Pavel, Girolamo, Marco Di, Barone, Paolo, Taleb, Tarik, & Tserpes, Konstantinos. (2023). Security in Cloud-Native Services: A Survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758–793. https://doi.org/10.3390/jcp3040034

Alzoubi, Yehia Ibrahim, Mishra, Alok, & Topcu, Ahmet Ercan. (2024). Research trends in deep learning and machine learning for cloud computing security. *Artificial Intelligence Review*, *57*(5). https://doi.org/10.1007/s10462-024-10776-5

Singh, Atul Kumar, & Bhushan, Kriti. (2025). In-Depth Literature Review of Cloud Computing Data Hazards and Mitigation Strategies. *Concurrency and Computation: Practice and Experience*, *37*(27-28). https://doi.org/10.1002/cpe.70393

Albugmi, H., Alassafi, M. O., Walters, R., & Wills, G. (2024). Data Security in Cloud Computing: A Systematic Review of Encryption and Access Control Techniques. *Future Internet*, *16*(4).

Mostafa, Ayman Mohamed, Ezz, Mohamed, Elbashir, Murtada K., Alruily, Meshrif, Hamouda, Eslam, Alsarhani, Mohamed, & Said, Wael. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied Sciences*, *13*(19). https://doi.org/10.3390/app131910871

Godwin, Nzeako, & Rahman Akorede, Shittu. (2024). Implementing zero trust security models in cloud computing environments. *World Journal of Advanced Research and Reviews*, *24*(3), 1647–1660. https://doi.org/10.30574/wjarr.2024.24.3.3500

Uddoh, Jeanette, Ajiga, Daniel, Okare, Babawale Patrick, & Aduloju, Tope David. (2021). AI-Based Threat Detection Systems for Cloud Infrastructure: Architecture, Challenges, and Opportunities. *Journal of Frontiers in Multidisciplinary Research*, *2*(2), 61–67. https://doi.org/10.54660/.Ijfmr.2021.2.2.61-67

Sinan, Maysa, Shahin, Mojtaba, & Gondal, Iqbal. (2025). Integrating Security Controls in DevSecOps: Challenges, Solutions, and Future Research Directions. *Journal of Software: Evolution and Process*, *37*(6). https://doi.org/10.1002/smr.70029

Arif, T., Jo, B., & Park, J. H. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors (Basel)*, *25*(8). https://doi.org/10.3390/s25082350

Zhang, J. Y., & Zhang, Y. (2024). Quantitative DevSecOps Metrics for Cloud-Based Web Microservices. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3864314

Shin, Daemin, Kim, Jiyoon, Pawana, I. Wayan Adi Juliawan, & You, Ilsun. (2025). Enhancing cloud-native DevSecOps: A Zero Trust approach for the financial sector. *Computer Standards & Interfaces*, *93*. https://doi.org/10.1016/j.csi.2025.103975

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors (Basel)*, *25*(19). https://doi.org/10.3390/s25196118

Le, Tran Duc, Le-Dinh, Thang, & Uwizeyemungu, Sylvestre. (2025). Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. *Electronics*, *14*(11). https://doi.org/10.3390/electronics14112252

Anasuri, S. (2023). Confidential Computing Using Trusted Execution Environments. *International Journal of AI, BigData, Computational and Management Studies*, *4*(2). https://doi.org/10.63282/3050-9416.Ijaibdcms-v4i2p111

Mohammed, Khwaja, Shanmugam, Bharanidharan, & El-Den, Jamal. (2025). Evolution of DevSecOps and Its Influence on Application Security: A Systematic Literature Review. *Technologies*, *13*(12). https://doi.org/10.3390/technologies13120548

Saleh, S. M., Madhavji, N., & Steinbacher, J. (2024). A Systematic Literature Review on Continuous Integration and Deployment (CI/CD) for Secure Cloud Computing.

Carlos Bautista Ramos, Roberto, & Yoo, Sang Guun. (2025). Cybersecurity in DevOps Environments: A Systematic Literature Review. *IEEE Access*, *13*, 191959–191979. https://doi.org/10.1109/access.2025.3582892

Deng, S., Zhao, H., Huang, B., Zhang, C., Chen, F., Deng, Y., Yin, J., Dustdar, S., & Zomaya, A. Y. (2024). Cloud-Native Computing: A Survey from the Perspective of Services.

Silverthorne, V. (2024). Cloud Native 2024: Approaching a Decade of Code. *Cloud*.

Cloud Security, Alliance. (2025b). *Top Threats Working Group Charter 2025*.

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel)*, *24*(4). https://doi.org/10.3390/s24041328

Index of Tables

Index of Figures