Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.090262

REVIEW

Zero Trust Architecture in Cloud Computing: A Scoping Review of Implementation Models, Security Benefits, Challenges, and Research Gaps

Darlington Chigozie Okeke*

Department of Computing and Engineering, University of Gloucestershire, Cheltenham, UK

*Corresponding Author: Darlington Chigozie Okeke. Email: okekechigozied2023@gmail.com

Received: 02 August 2026; Accepted: 09 October 2026; Published: 13 November 2026

ABSTRACT: Background: Traditional perimeter-centric cloud security approaches are increasingly challenged by distributed cloud environments and implicit trust. Zero Trust Architecture (ZTA) provides a "never trust, always verify" approach. This scoping review aims to provide an overview of ZTA implementation models, reported security benefits, and deployment challenges and research gaps in cloud computing environments. **Methods:** Based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR) reporting framework, a systematic search was conducted across six electronic databases: Scopus, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. Only peer-reviewed journal articles from January 2020 to May 2026 were included. **Findings:** Of 444 identified records, 42 studies met the eligibility criteria. The synthesis identified eight implementation themes, although the level of supporting evidence varied across themes, comprising identity-centric security frameworks, least-privilege access control, micro-segmentation, continuous monitoring and verification, policy-driven and automated enforcement, hybrid cloud frameworks, data-centric protection, and integrated multi-pillar models. Some themes were supported by fewer studies and are therefore interpreted as emerging or illustrative approaches. Key benefits included an improved cloud security posture, reduced lateral threat movement, and automated incident response, while technical complexity, legacy system incompatibility, scalability, and performance latency were major adoption challenges. **Conclusions:** While highly resilient, ZTA requires a long-term architectural shift to secure distributed cloud infrastructures. Future research should focus on moving beyond theoretical frameworks towards extensive experimental testing, more sophisticated AI-enabled automation, and interoperable, privacy-focused solutions.

KEYWORDS: Zero trust architecture; zero trust security; cloud computing; cloud security; implementation models; security benefits; challenges; research gaps

1 Introduction

Cloud computing has become a key computing paradigm, providing on-demand access to computing resources, storage, and applications through the Internet. Its scalability, flexibility, cost efficiency, and resource-sharing capabilities have contributed to widespread adoption [1,2]. Despite these benefits, cloud computing introduces security and privacy challenges because data and resources are distributed across geographically dispersed infrastructure, with some resources managed by cloud service providers [3]. These challenges include unauthorized access, data breaches, denial-of-service attacks, insider threats, privacy concerns, and compliance requirements, making confidentiality, integrity, and availability important security priorities [4].

Copyright © 2026 The Author. Published by Tech Science Press. This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Traditional security models were designed for centralized, on-premises environments in which users, devices, and applications operated within a defined network perimeter [5]. However, public, private, hybrid, and multi-cloud environments distribute users and workloads across heterogeneous infrastructures, making perimeter-based trust increasingly inadequate [6]. Third-party cloud providers, virtualization, multitenancy, insecure APIs, insider threats, and inconsistent security controls further complicate cloud security management [7]. Advanced threats, including malware, ransomware, denial-of-service attacks, account hijacking, and SQL injection, also pose challenges to consistent protection across heterogeneous cloud environments [8].

However, the challenges of perimeter-based security have given rise to a new framework, Zero Trust Architecture (ZTA). ZTA is a modern security framework for a highly distributed computing environment. Instead of trusting all users and devices on a network, ZTA adopts the motto "never trust, always verify," meaning that every access request, regardless of who it is from, must be authenticated, authorized, and continuously verified [9]. This is because the use of cloud computing, remote working, mobile devices, and Internet of Things (IoT) technologies has broken down traditional network barriers, and there is now increasing reliance on implicit trust, posing a major security risk.

The concept of Zero Trust was introduced in 2010 by Forrester Research's John Kindervag, who suggested that trust should not be regarded as a security assumption, but rather a security weakness [10]. He laid the groundwork for today's cybersecurity principles, including explicit verification, least-privilege access, and continuous monitoring. These concepts have since been proven in practice by Google's BeyondCorp program, which was designed to demonstrate that large organizations can securely operate without a traditional trusted network perimeter, based on user identity and device security posture, regardless of network location [11].

Since then, ZTA has expanded to be a full-fledged security strategy that focuses on securing users, devices, applications, data, and identity-centric security, micro-segmentation, continuous authentication, policy-based access control, and real-time monitoring [12]. ZTA takes a proactive approach to security, acknowledging that breaches can happen anytime and anywhere, and mitigates implicit re-entrustment, minimizes insider threats, and provides greater protection to organizations from the ever-changing nature of cyberattacks. This has made Zero Trust Architecture a growing favorite among cloud security solutions, as it shifts to a perimeter-less security approach that requires ongoing verification of resources rather than a single, fixed point of trust [13].

The past few years have seen a surge in research on ZTA and its significant role as a cybersecurity strategy for today's businesses. The proliferation of cloud computing, remote working, Bring Your Own Device (BYOD), and the growing threat from ever more complex cyber-attacks have placed traditional security models like Virtual Private Networks (VPNs) under immense strain, with many offerings providing significant network access after users have passed authentication checks [14]. As more research has emerged, it has become clear that these strategies are not enough to secure distributed cloud environments, as attackers who compromise a single endpoint can move around the organizational network to attack other endpoints. For this reason, ZTA has attracted considerable interest as an alternative security approach that continuously checks all access requests and restricts users and devices to only what they need to perform their activities [15]. It has spurred significant academic and industry research on the design, implementation, and effectiveness of ZTA across various organizational contexts [16].

Existing studies have examined ZTA implementation strategies, migration frameworks, security benefits, deployment challenges, and economic impacts [17]. However, the evidence remains fragmented, with studies often focusing on individual implementation approaches, tools, cost analyses, or organizational cases rather than providing a comprehensive synthesis of the field. Although research on ZTA in cloud computing

has increased, the evidence remains fragmented across cloud security, network security, identity and access management, and cybersecurity governance. Existing studies commonly address individual aspects such as implementation models, authentication, micro-segmentation, policy enforcement, migration strategies, benefits, or deployment challenges. Consequently, a comprehensive synthesis of implementation models, security benefits, challenges, and research gaps remains needed, particularly given the rapid evolution of cloud technologies and cyber threats.

A scoping review is therefore suitable because it can identify, classify, and describe evidence within a wide range of research and can reveal gaps and opportunities for future research. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR) is a scientific reporting guideline that can support this objective. It has a systematic approach that enables comprehensive identification of literature, study selection, systematic data charting, and clear reporting of findings. The use of PRISMA-ScR improves the methodological transparency, reproducibility, and reliability of the review, making it appropriate for mapping the literature on Zero Trust Architecture in cloud computing, given its diversity and evolution.

1.1 Objectives

Objective: To map and synthesize existing literature on Zero Trust Architecture (ZTA) in cloud computing, focusing on implementation models, security benefits, challenges, and research gaps.

The objective of this scoping review is to systematically map and synthesize the existing literature on Zero Trust Architecture (ZTA) in cloud computing environments. Specifically, the review aims to identify and categorize ZTA implementation models, examine the reported security benefits of ZTA adoption, explore implementation challenges and limitations, and highlight existing research gaps and future research opportunities in the field.

1.2 Research Questions

RQ1: What implementation models of Zero Trust Architecture have been proposed and applied in cloud computing environments?

RQ2: What security benefits are reported in the literature regarding the adoption of Zero Trust Architecture in cloud computing?

RQ3: What challenges and limitations are associated with implementing Zero Trust Architecture in cloud environments?

RQ4: What research gaps and future research opportunities exist in the current literature on Zero Trust Architecture in cloud computing?

2 Methods

2.1 Protocol and Registration

Prior to conducting this scoping review, no formal review protocol was created and registered. As such, there is no public protocol or registration number available for this review. A review protocol was considered during the planning of the study; however, the protocol was not prospectively registered in an external registry such as OSF. The review was instead conducted using predefined eligibility criteria, a structured search strategy, and a systematic screening and data-charting process established before the study selection and synthesis. However, the review was conducted according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR) guidelines. The

review methodology was developed before the literature search and applied consistently throughout the review to promote transparency, consistency, and reproducibility.

2.2 Eligibility Criteria

Studies were selected according to predetermined criteria that aligned with the aim of this scoping review, as listed in Table 1. The studies included in this review were peer-reviewed journal articles published in English between 2020 and 2026 that addressed ZTA in cloud computing environments. The studies that were included in this review addressed one or more of the following topics: ZTA models of implementation, security benefits, implementation challenges and limitations, and research gaps and future research opportunities associated with ZTA in cloud computing. Empirical and non-empirical studies, including qualitative, quantitative, mixed-methods, conceptual, review, survey, and framework-based articles, were included to reflect the wide range of available resources. Studies that addressed Zero Trust only in cloud computing, duplicate publications or book chapters, or editorials were not included. The publication period (2020–2026) was selected to capture the latest developments, as Zero Trust Architecture has been rapidly evolving and gaining traction in today's cloud computing landscape.

Table 1: Eligibility criteria for study selection.

Inclusion Criteria	Exclusion Criteria
Topic: Studies focusing on Zero Trust Architecture (ZTA) in cloud computing environments	Studies not focused on Zero Trust Architecture in cloud computing.
Publication type: Peer-reviewed journal articles	Conference abstracts, editorials, book chapters, commentaries, dissertations, and duplicate publications
Language: English	Non-English publications
Publication period: January 2020 to May 2026	Studies published before 2020
Study designs: Qualitative, quantitative, mixed-methods, conceptual, review, survey, framework-based, and empirical/non-empirical studies.	Publications that did not address one or more review domains
Review focus: Studies investigating ZTA implementation models, security benefits, implementation challenges and limitations, or research gaps and future research opportunities	Studies unrelated to ZTA implementation, benefits, challenges, or future directions in cloud computing

To ensure compliance with the eligibility criterion requiring peer-reviewed journal articles, the author verified the peer-review status of potentially eligible publications using the official journal websites and their stated editorial or peer-review policies. Journals were considered peer-reviewed when their official policies explicitly described external peer review of submitted manuscripts. For example, if a journal stated that manuscripts undergo preliminary editorial screening followed by review by two or more external experts using a double-blind peer-review process, the corresponding article was included. This verification process was applied to potentially eligible publications, particularly those published in less-established or less-well-indexed journals, to ensure consistency with the predefined eligibility criteria.

2.3 Information Sources

A thorough literature review was conducted to identify studies relevant to Zero Trust Architecture in cloud computing. Using electronic databases, including Scopus, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar, the literature was searched for peer-reviewed journal articles discussing the implementation, advantages, issues, and future trends of ZTA in cloud environments. The reference lists of eligible studies were also scanned to identify any other relevant publications not found in the database searches. The search strategy consisted of combinations of keywords and Boolean operators used to search the literature: "Zero Trust Architecture," "Zero Trust Security," "cloud computing," "cloud security," "implementation," "security benefits," "challenges," and "research gaps". All retrieved records were exported to a reference management tool before screening to identify and remove any duplication. The last database search was in May 2026, keeping the review up to date with the latest evidence on Zero Trust Architecture in cloud computing. Table 2 presents the information sources and search strategy used during the search.

Table 2: Information sources and search strategy.

Search Component	Description
Electronic databases	Scopus, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar
Main search concepts	"Zero Trust Architecture", "Zero Trust Security", "Zero Trust Network Access (ZTNA)", "Cloud Computing", "Cloud Security", "Cloud Environment", "Multi-cloud", and "Hybrid Cloud"
Implementation-related keywords	"Implementation", "Framework", "Model", "Identity and Access Management", "Micro-segmentation", "Policy Enforcement", "Adoption"
Outcome-related keywords	"Security Benefits", "Challenges", "Limitations", "Research Gaps", "Future Research"
Search operators	Boolean operators (AND/OR), phrase searching, and truncation (where supported)
Final search strategy	*(Zero Trust Architecture OR Zero Trust Security OR Zero Trust Network Access OR ZTA OR ZTNA) AND (Cloud Computing OR Cloud Security OR Cloud Environment OR Multi-cloud OR Hybrid Cloud OR Cloud-native) AND (Implementation OR Framework* OR Model OR Security Benefits OR Challenges OR Limitations OR Research Gaps OR Future Research)

2.4 Search

The electronic search strategy aimed to identify studies related to Zero Trust Architecture in cloud computing. The initial search was conducted in Scopus using a structured combination of terms relating to Zero Trust Architecture, cloud computing, and implementation, benefits, challenges, and research gaps. The initial search was conducted in Scopus, and the search strategy was subsequently adapted with minimal modifications for IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar to account for differences in database search functionality. Boolean (AND/OR) searching, phrase searching, and truncation, where supported, were used to combine search terms. The complete search strings for each

database, together with applicable search limits, are presented in Appendix A. The following search string was used in Scopus:

TITLE-ABS-KEY ("Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" OR ZTA OR ZTNA) AND ("cloud computing" OR "cloud security" OR "cloud environment" OR "multi-cloud" OR "hybrid cloud" OR "cloud-native") AND (implementation OR framework* OR model* OR adoption OR benefit* OR challenge* OR limitation* OR "security benefit*" OR "identity and access management" OR micro-segmentation OR "research gap*" OR "future research").*

Only peer-reviewed journal articles, English-language publications, and publications relevant to the review objectives were searched. Duplicate records were removed before screening for titles, abstracts, and full texts.

2.5 Selection of Sources of Evidence

Selection of evidence sources followed a structured screening process using the PRISMA-ScR guidelines. After completing the database searches, all records were downloaded into the reference management software, and duplicate records were deleted. As this was a single-author scoping review, the sole reviewer conducted all title and abstract screening. The full-text assessment of potentially eligible studies was also conducted by the same reviewer using the predetermined inclusion and exclusion criteria. As the review was designed and conducted as a single-author academic research project, no co-reviewer or independent screening team was available within the structure and resources of the project to undertake duplicate screening or an inter-rater reliability assessment. Studies were excluded if they were not about Zero Trust Architecture in cloud computing, did not include at least one of the review domains, or did not meet the eligibility criteria. Documentation of reasons for exclusion at the full-text stage was done for transparency and reproducibility. The final set of eligible studies was selected for data extraction and synthesis in the scoping review.

2.6 Data Charting Process

A data-charting form, followed by a structured data-extraction form, was developed for this scoping review. The charting form was developed to ensure that relevant information could be consistently extracted from all included studies and that it was consistent with the review objectives and research questions. The form was pretested on a small number of included studies to ensure that all necessary variables would be collected and to make any necessary changes.

Data from each eligible study were systematically collected in a Microsoft Excel tool. The information, which was charted, consisted of bibliographic details (author and year of publication), country or region of the study, study design, cloud computing environment, Zero Trust implementation model or framework, the security benefits reported, implementation challenges, datasets or technologies used, evaluation metrics, key findings, research gaps, and recommendations for future research.

Throughout the charting process, the extracted data were checked for completeness and consistency. When multiple implementation models, security outcomes, or challenges were reported in a study, all such data were captured to provide a fuller picture of the evidence. Any doubts encountered during data extraction were resolved by revisiting the original publication to ensure accuracy and consistency. Because the review was conducted by a single reviewer, consistency checks and revisiting the original publications were used to support the accuracy and consistency of the extracted data; however, independent duplicate data extraction was not performed.

Data charting tables were completed and used for descriptive analysis and thematic synthesis, as shown in Table 3. The extracted information was organized according to the review objectives, enabling the identification of common implementation models, reported security benefits, implementation challenges, evaluation methods, and gaps in emerging research studies. The structured approach provided greater transparency and consistency in the data-charting and evidence-synthesis process.

Table 3: Data charting framework used for extracting and organizing information from the included studies.

Category	Data Charted
Bibliographic information	Author(s), year of publication
Study characteristics	Study type, research design
Cloud characteristics	Cloud environment (public, private, hybrid, multi-cloud, cloud-native, edge)
Zero Trust implementation	ZTA model/framework, technologies used (IAM, MFA, micro-segmentation, SASE, AI, SDN, etc.)
Security benefits	Improved authentication, reduced insider threats, enhanced visibility, lateral movement prevention, compliance, etc.
Implementation challenges	Legacy systems, interoperability, scalability, performance, privacy, policy enforcement, cost, skills gap
Evaluation	Dataset/testbed, performance metrics (accuracy, precision, recall, F1-score, latency, etc.), validation approach
Key findings	Main conclusions
Research gaps	Future research directions identified by the authors

Note: Abbreviations: ZTA (Zero Trust Architecture), IAM (Identity and Access Management), MFA (Multi-Factor Authentication), SASE (Secure Access Service Edge), AI (Artificial Intelligence), SDN (Software-Defined Networking).

2.7 Data Items

A data extraction form developed for this review was used to extract data from each study included in the review. Other data on identity and access management, micro-segmentation, continuous authentication, AI integration, and policy enforcement were also collected when available. The applied framework for data extraction was kept consistent across all included studies, and data were synthesized narratively according to the four predefined review questions.

2.8 Synthesis of Results

The collected data were synthesized in a charted format, using a descriptive and thematic approach, consistent with the aims of the scoping review. Data extraction was followed by a summary of the included data based on publication characteristics (publication year, study type, cloud environment, primary focus, and research method). The findings were then classified into the four review questions: (1) Implementation models for Zero Trust Architecture in cloud computing, (2) reported security benefits offered by Zero Trust Architecture, (3) security challenges and limitations, and (4) research gaps and research opportunities. For each research question, studies were selected for comparison to identify recurring concepts, implementation strategies, and concepts that are agreed upon and those that are disputed in the literature. Common themes from the individual studies were combined thematically to synthesize findings on implementation models,

reported benefits, challenges, and future research directions across studies. Descriptive summary tables were created to describe the selected studies and summarize the themes identified for each review question. This review was not designed to assess the effectiveness of interventions, and so a quantitative synthesis or meta-analysis was not undertaken. The results are thus presented as a narrative, with summary tables that indicate the distribution of evidence and the main themes identified in the included studies.

3 Results

3.1 Selection of Sources of Evidence

A total of 444 records were identified through the literature search, including 400 records retrieved from the selected electronic databases and 44 additional records identified through other sources. After removal of duplicate records, 183 records remained for title and abstract screening. Thus, 261 duplicate records were removed before screening. Following title and abstract screening, 80 records were excluded, leaving 103 full-text articles for eligibility assessment. Of these, 61 full-text articles were excluded for the reasons presented in Fig. 1, including conference abstracts (n = 14), studies not focused on Zero Trust Architecture (n = 32), editorials and book chapters (n = 10), and dissertations and opinion papers (n = 5). A total of 42 studies fulfilled the eligibility criteria and were included in the final synthesis. The selection of articles is shown using the PRISMA-ScR flow chart in Fig. 1.

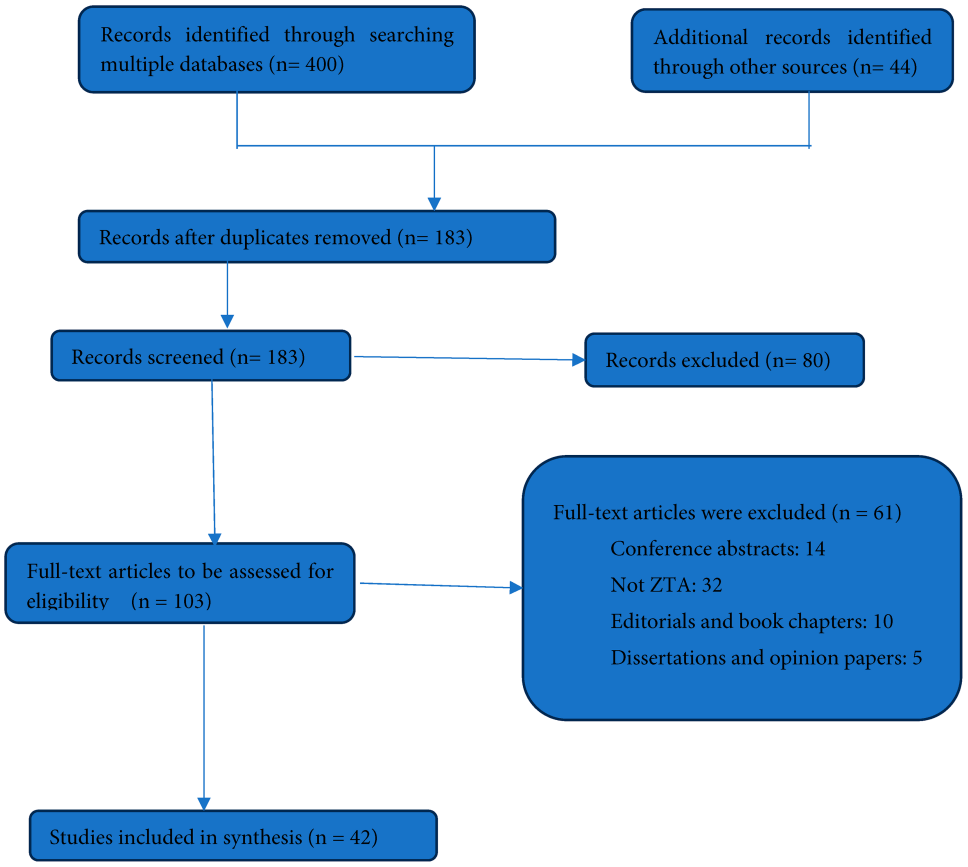


Figure 1: PRISMA-ScR (Preferred reporting items for systematic reviews and meta-analyses extension for scoping reviews) flow diagram. Note: n represents the number of records, articles, or studies at each stage of the review process. ZTA (Zero trust architecture).

3.2 Characteristics of Sources of Evidence

The characteristics of the included studies are summarized in Table 4, which gives a general overview of the evidence base, specifically the year of publication, study type, cloud environment, primary research focus, and the research methods employed. The literature reviewed shows an increase in research interest in ZTA over the last few years, with the majority of research published since 2024. As cloud computing becomes more widely adopted, cloud security models are increasingly seeking to be more robust. The evidence base comprised a variety of study designs, including research articles, review articles, survey articles, systematic literature reviews, and conceptual studies, demonstrating the multidisciplinary nature of ZTA research. The studies investigated a variety of cloud environments, such as public, private, hybrid, multi-cloud, cloud-native, distributed cloud, multi-tenant, and microservices platforms. The main areas of focus were ZTA implementation models, identity and access management, micro-segmentation, AI-driven security, dynamic access control, enterprise security frameworks, implementation challenges, security benefits, and future research directions—all of which were addressed with respect to the environments mentioned above. Similarly, the research methods employed were highly varied and included conceptual analysis, architectural analysis, literature reviews, systematic reviews, survey studies, case study analysis, framework development, algorithm design, mixed-methods research, and experimental performance testing.

3.3 Synthesis of Results

Implementation Models of Zero Trust Architecture in Cloud Computing

The included studies identified a variety of ZTA models applicable to cloud computing environments. Although there are differences in implementation contexts, such as hybrid cloud, multi-cloud, and enterprise cloud deployments, eight implementation themes emerged across the reviewed literature: (1) identity-centric security frameworks, (2) least-privilege access control, (3) micro-segmentation architectures, (4) continuous monitoring and verification models, (5) policy-driven and automated enforcement models, (6) hybrid cloud Zero Trust frameworks, (7) data-centric protection models, and (8) integrated multi-pillar Zero Trust models. These themes reflect recurring approaches to implementing ZTA across different cloud environments. The models were primarily identity-centric and grounded in continuous verification, least-privilege access, micro-segmentation, and continuous monitoring. The studies generally described a shift from perimeter-based security to adaptive, context-aware architectures that assume all access requests are potentially insecure.

An identity-based Zero Trust model was among the most frequently reported implementation strategies. Several studies have highlighted identity as the first line of defense in security, describing it as an alternative to reliance on traditional network boundaries. This approach relies on continuous verification of users, devices, workloads, and applications, rather than on a user's location within a network. However, Guntaka [18] proposed a cloud identity framework that incorporates concepts such as Zero Trust, Identity and Access Management (IAM), identity governance, role-based access control (RBAC), automated policy enforcement, and continuous authentication. With a similar approach, Poddar [19] introduced a multi-cloud unified identity management architecture that leverages multifactor authentication (MFA), risk-based authentication, identity governance, and centralized IAM platforms to maintain consistent security across a wide range of cloud services. Rehan [20] also noted that identity-centric security is the key element of Zero Trust in multi-cloud architectures, featuring adaptive authentication, identity federation, and Zero Trust Network Access (ZTNA) solutions. Solanke [21] emphasized the significance of centralized identity providers, such as Azure Active Directory and Okta, for achieving identity unification across multiple cloud providers.

Table 4: Summarizes publication years, research methods, studied cloud environments, and investigated types of ZTA approaches.

Study	Year	Study Type	Evidence Type	Cloud Environment	Primary Focus	Research Method
[18]	2025	Journal Research Article	Conceptual/ Framework	Cloud environments	Cloud identity and Zero Trust security framework	Standards-based conceptual analysis using NIST guidance and industry frameworks
[19]	2025	Journal Research Article	Conceptual/ Framework	Multi-cloud	Zero Trust network architecture for multi-cloud security	Conceptual architecture supported by implementation analysis
[20]	2022	Journal Research Article	Conceptual/ Framework	Multi-cloud	Zero Trust architecture for securing multi-cloud infrastructures	Conceptual framework supported by case study analysis
[21]	2021	Journal Research Article	Empirical/ Experimental	Multi-cloud (AWS, Azure, Google Cloud Platform)	Zero Trust implementation strategies and measurable outcomes	Architectural design with implementation guidelines and performance evaluation
[22]	2024	Journal Research Article	Case-Study/ Qualitative	Hybrid cloud	Implementing Zero Trust in hybrid cloud environments	Literature review and case study analysis
[23]	2024	Review Article	Conceptual/ Framework	Multi-cloud microservices platforms	Zero Trust implementation framework for multi-cloud microservices	Literature review and architectural framework development
[24]	2026	Journal Research Article	Conceptual/ Framework	Multi-tenant cloud (SaaS, Kubernetes)	Zero Trust architecture for multi-tenant cloud applications	Architectural design with experimental evaluation using enterprise workloads
[25]	2022	Journal Research Article	Conceptual/ Framework	Multi-cloud (AWS, Azure, GCP, IBM Cloud)	Zero Trust architecture for multi-cloud environments	Proposed architecture with performance evaluation and conceptual analysis
[26]	2024	Journal Research Article	Case-Study/ Qualitative	Cloud, hybrid cloud, and multi-cloud	Enterprise best practices for Zero Trust implementation	Literature review with case studies and practical examples
[27]	2025	Journal Article	Conceptual/ Framework	Multi-tenant cloud ecosystems (AWS, Azure, Kubernetes)	Zero Trust enforcement using microsegmentation, identity-aware proxies, and CARA	Reference model proposal and architectural implementation evaluation
[28]	2025	Journal Research Article	Empirical/ Experimental	Cloud computing	Dynamic Zero Trust-based access control	Algorithm development with experimental performance evaluation

(Continued)

Table 4 (continued)

Study	Year	Study Type	Evidence Type	Cloud Environment	Primary Focus	Research Method
[29]	2024	Journal Research Article	Conceptual/ Framework	Cloud and distributed cloud systems	Zero Trust framework for securing distributed cloud systems	Conceptual framework and architectural analysis
[30]	2024	Journal Research Article	Case-Study/ Qualitative	Enterprise multi-cloud	Enterprise implementation of Zero Trust across multi-cloud systems	Enterprise implementation analysis using practical case examples
[31]	2025	Journal Research Article	Conceptual/ Framework	Cloud computing	AI-driven Zero Trust for enhanced cloud security	Conceptual framework supported by AI use cases and illustrative case studies
[32]	2024	Journal Research Article	Conceptual/ Framework	Cloud-native, hybrid cloud, and platform engineering environments	Zero Trust architecture for platform engineering security	Conceptual analysis supported by industry reports and an implementation framework
[33]	2022	Journal Research Article	Case-Study/ Qualitative	Public, private, hybrid, and multi-cloud	Implementing Zero Trust architecture for enhanced cloud security	Literature review with conceptual implementation methodology
[34]	2025	Survey Article	Conceptual/ Framework	Cloud, hybrid cloud, and multi-cloud ecosystems	Survey of Zero Trust security architecture in cloud ecosystems	Systematic survey and comparative literature review
[35]	2025	Research Article	Case-Study/ Qualitative	Multi-cloud ecosystems (Big Data workloads)	Zero Trust implementation strategies and best practices for securing big data workloads	Literature review and analysis of implementation strategies, case studies, and future trends
[36]	2024	Journal Research Article	Case-Study/ Qualitative	Cloud computing environments	Implementing Zero Trust security models in cloud computing	Theoretical framework supported by technical analysis and real-world case studies
[37]	2025	Journal Research Article	Conceptual/ Framework	Enterprise cloud and distributed environments	Zero Trust architecture as the future of enterprise security	Conceptual review with phased implementation framework
[38]	2023	Review Paper	Conceptual/ Framework	Multi-cloud SaaS platforms	Scalable Zero Trust architectures for enhancing security in multi-cloud SaaS environments	Literature review and architectural analysis
[39]	2024	Journal Research Article	Conceptual/ Framework	Enterprise cloud environments	Zero Trust model for enterprise data protection	Conceptual framework with performance evaluation using KPIs and security metrics

(Continued)

Table 4 (continued)

Study	Year	Study Type	Evidence Type	Cloud Environment	Primary Focus	Research Method
[40]	2025	Journal Research Article	Conceptual/ Framework	Cloud-native applications (Microsoft Azure)	Zero Trust implementation for cloud applications	Conceptual analysis supported by Azure implementation example and industry evidence
[41]	2025	Journal Article	Empirical/ Experimental	Multi-cloud storage systems	Cryptographic zero-trust access challenges (online dependency and centralized CA bottlenecks)	Algorithm development (HIBE & CP-ABE) with experimental validation and limitation analysis
[42]	2025	Journal Research Article	Case-Study/ Qualitative	Distributed, hybrid, and multi-cloud architectures	Zero Trust security models in distributed cloud architectures	Conceptual framework supported by industry case studies
[43]	2024	Journal Article	Case-Study/ Qualitative	Cloud-native environments (microservices, containers, Kubernetes)	Implementation challenges, DevOps best practices, and emerging security trends	Framework mapping, practical strategy formulation, and quantitative benchmark evaluation
[44]	2025	Journal Research Article	Conceptual/ Framework	Multi-cloud cloud security environments	Identity and Access Management (IAM) challenges and solutions in Zero Trust Architecture	Conceptual analysis and literature-based review of IAM strategies
[45]	2026	Journal Research Article	Conceptual/ Framework	Cloud, hybrid cloud, edge computing, and multi-cloud	AI-enabled adaptive Zero Trust for dynamic cloud security	Conceptual perspective supported by architectural analysis and an AI integration framework
[46]	2025	Journal Research Article	Case-Study/ Qualitative	Cloud environments	AI-driven threat intelligence for enhancing Zero Trust Architecture	Conceptual framework supported by case study analysis
[47]	2020	Journal Research Article	Conceptual/ Framework	Multi-cloud environments	Challenges of achieving Zero Trust remote access in multi-cloud environments	Conceptual analysis and literature-based discussion
[48]	2020	Research Article	Conceptual/ Framework	Cloud computing environments	Establishing a conceptual Zero Trust strategy and trust management framework	Conceptual framework and analytical discussion of trust management challenges

(Continued)

Table 4 (continued)

Study	Year	Study Type	Evidence Type	Cloud Environment	Primary Focus	Research Method
[49]	2022	Journal Research Article	Conceptual/ Framework	Microsoft Azure financial services cloud	Implementing Zero Trust Architecture in financial cloud environments	Architectural implementation analysis with Microsoft Azure security framework
[50]	2024	Review Article	Conceptual/ Framework	Cloud networks	Zero Trust applications, implementation challenges, and future opportunities in cloud security	Systematic literature review with thematic and comparative analysis
[51]	2024	Journal Research Article	Empirical/ Experimental	Cloud, hybrid cloud, and multi-cloud environments	AI-reinforced Zero Trust Architecture for scalable cloud security	Mixed-methods approach combining architectural design, literature synthesis, and simulation-based experimental evaluation
[52]	2022	Survey Article	Conceptual/ Framework	Enterprise and cloud network environments	Survey of Zero Trust Architecture, implementation challenges, and future research trends	Comprehensive survey and comparative analysis of Zero Trust technologies
[53]	2025	Journal Research Article	Conceptual/ Framework	Cloud environments	Enhancing cloud security through Zero Trust Architecture, including implementation challenges and future research directions	Conceptual framework supported by literature synthesis
[54]	2025	Systematic Literature Review	Conceptual/ Framework	Cloud environments	Zero Trust micro-segmentation strategies, operational challenges, and future trends	Systematic literature review of 39 primary studies (2016–2025)
[55]	2025	Journal Research Article	Conceptual/ Framework	Cloud environments	Integrating Generative AI capabilities into Zero Trust Architecture for adaptive cloud security	Conceptual research with analytical discussion of AI-enabled Zero Trust frameworks
[56]	2022	Review Article	Conceptual/ Framework	Cloud computing networks	Comparative review of Zero Trust cloud network models, frameworks, and future research directions	Comparative literature review of Zero Trust cloud security models and frameworks
[57]	2026	Journal Research Article	Conceptual/ Framework	Cloud-native environments, including multi-cloud, serverless, and distributed cloud infrastructures	Development of a scalable Zero Trust Architecture framework that integrates identity-centric security, micro-segmentation, continuous verification, and real-time monitoring	Systematic literature review and thematic analysis

(Continued)

Table 4 (continued)

Study	Year	Study Type	Evidence Type	Cloud Environment	Primary Focus	Research Method
[58]	2021	Review Article	Conceptual/ Framework	Cloud networks	Dynamic and granular Zero Trust access control and policy enforcement for cloud security	Conceptual review proposing an adaptive Zero Trust framework
[59]	2025	Journal Research Article	Case-Study/ Qualitative	Multi-tenant cloud environments	Zero Trust security for multi-tenant cloud environments with AI-enhanced threat detection and adaptive access control	Conceptual analysis supported by a SaaS provider case study

Note: Abbreviations: NIST (National Institute of Standards and Technology), AWS (Amazon Web Services), GCP (Google Cloud Platform), SaaS (Software as a Service), IAM (Identity and Access Management), AI (Artificial Intelligence), IBM (International Business Machines), KPIs (Key Performance Indicators), HIBE (Hierarchical Identity-Based Encryption), CP-ABE (Ciphertext-Policy Attribute-Based Encryption).

A second implementation model identified across the literature was the least-privileged access control model. This approach implements the concept of "Zero Trust," which means granting minimal access needed to carry out authorized actions. Least privilege was identified as a key feature of the architecture in several studies, rather than merely an access control policy. Least-privilege access is an integral part of Zero Trust deployments in hybrid cloud environments and may help reduce unnecessary permissions and potentially limit the attack surface [22]. Additionally, least privilege is a key mechanism enforced at Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs), enabling dynamic, context-aware authorization decisions [23]. This model can be integrated with role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control (PBAC), enabling finer-grained, more flexible access decisions [24]. The implementation of least privilege was linked to the Just-in-Time (JIT) and Just-Enough-Access (JEA) paradigms, in which access rights or privileges are issued only on an *ad hoc* basis and for a limited period as needed.

Microsegmentation-based implementation models were also consistently cited as a crucial approach to implementing Zero Trust in cloud environments. Micro-segmentation is the process of segmenting cloud infrastructures into smaller, isolated security zones with explicit rules and policies governing communication [25]. Micro-segmentation is a mechanism for limiting lateral movement between network zones in hybrid cloud environments and for implementing access control between them. Similarly, micro-segmentation is a key element of enterprise Zero Trust deployments and may help restrict attacker mobility and contain the potential scope of a security incident [26]. To operationalize this, Kalejaiye and Shonubi [27] proposed a model utilizing granular, workload-level microsegmentation network policy controls across AWS, Azure, and Kubernetes-based architectures to isolate environments and enforce least-privilege access. Network isolation and micro-segmentation architectures rely on cloud-provider-specific resources, such as AWS Security Group, Azure Network Security Group, and Google Cloud Identity-Aware Proxy [21].

The other major implementation model in the literature was continuous monitoring and adaptive verification. This is not based on a single sign-on experience but rather continuously assesses user-, device-, network-, and context-related risk factors during an active session [22]. Ongoing monitoring and verification processes are crucial for maintaining trust assessments in a hybrid cloud environment. Nalla [26] noted that continuous monitoring is a core element of Zero Trust deployments, supported by platforms and tools for security information and event management (SIEM) and behavioral analytics. User and Entity Behavior Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), and Extended Detection and Response (XDR) technologies enable dynamic policy changes to better respond to emerging threats [20]. Also, activity monitoring and ongoing security assessments are key aspects of the Zero Trust approach to maintaining security in multi-cloud environments [19]. These results suggest that continuous monitoring is a dynamic feedback loop that facilitates security decisions and real-time decision-making.

The review also revealed that policy-driven, automated Zero Trust models are emerging as implementation approaches. These models focus on policy enforcement and automation to deliver uniform security policies across the complex cloud environment. Guntaka [18] defined the NIST Zero Trust framework as implemented using Policy Engines, Policy Administrators, and Policy Enforcement Points. Policy-based access control mechanisms can be enhanced through machine-learning-based behavioural analysis and adaptive security policies [20]. To incorporate Zero Trust controls into Infrastructure-as-Code (IaC) workflows and continuous integration/continuous deployment (CI/CD) pipelines, a Policy-as-Code (PaC) approach can be introduced [21]. Such approaches may support automation, scaling, and the consistent deployment of multi-cloud security policies. The emergence of Policy-as-Code therefore, represents a reported trend toward automation in implementing Zero Trust.

Some studies then focused on cloud-specific implementation frameworks that address the distributed nature of today's cloud infrastructures and apply to both hybrid and multi-cloud environments. Emmanni [22] proposed a hybrid cloud Zero Trust model that combines IAM, MFA, microsegmentation, encryption, continuous monitoring, and policy enforcement mechanisms. Specifically, multi-cloud entails adopting centralized identity management, unified policy enforcement, and cloud-agnostic security controls to address the challenge of managing inconsistent access across cloud providers' identity fragments [28]. Vodapally [29] also created a multi-cloud Zero Trust architecture that integrates cloud-native IAM capabilities, segments workloads at the workload level, and applies adaptive threat detection. Finally, one study presented an integrated multi-pillar Zero Trust model that combined multiple architectural aspects into a single framework. The conceptual framework integrated identity-centric security, least-privilege access, microsegmentation, continuous monitoring and telemetry, and data-centric protection [30]. The model was based on a continuous feedback loop intended to support dynamic trust assessment and adaptive security enforcement. Because this implementation theme was identified in only one study, it should be interpreted as an illustrative or emerging approach rather than as an established pattern across the reviewed literature. Table 5 summarizes the ZTA implementation models reviewed.

Table 5: Summary of zero trust architecture implementation models identified in the included studies.

Implementation Model/Theme	Description	Studies Reporting the Model	Number of Supporting Studies (n)	Evidence Type
Identity-Centric Security Frameworks	Security decisions are based on continuous verification of users, devices, applications, and workloads rather than network location. Common components include IAM, MFA, identity federation, SSO, adaptive authentication, and identity governance.	[18–20]	3	Conceptual/ Framework
Least-Privilege Access Control (PoLP)	Access is restricted to the minimum permissions necessary to perform authorized tasks. Often implemented through RBAC, ABAC, PBAC, Just-in-Time (JIT) access, and dynamic authorization mechanisms.	[22–24]	3	Conceptual/ Framework; Case-Study/ Qualitative
Micro-Segmentation Architectures	Cloud environments are divided into granular security zones or workload-level segments to restrict lateral movement and isolate potential breaches. Policies are enforced at the application, workload, or service level.	[21,25–27]	4	Empirical/experimental; Conceptual/ Framework; Case-Study/ Qualitative
Continuous Monitoring and Verification Models	Continuous assessment of user behavior, device posture, network traffic, and contextual risk factors through telemetry, SIEM, UEBA, XDR, and behavioral analytics.	[19,20,22,26]	4	Conceptual/Framework; Case-Study/ Qualitative
Policy-Driven and Automated Enforcement Models	Centralized policy engines and automated policy enforcement mechanisms support dynamic access decisions and security orchestration. Includes Policy-as-Code (PaC), Policy Decision Points (PDPs), and Policy Enforcement Points (PEPs).	[18,20,21]	3	Conceptual/ Framework

(Continued)

Table 5 (continued)

Implementation Model/Theme	Description	Studies Reporting the Model	Number of Supporting Studies (n)	Evidence Type
Hybrid Cloud Zero Trust Frameworks	ZTA implementations are designed for environments combining on-premises infrastructure with public and private cloud resources. Emphasize IAM integration, MFA, encryption, continuous monitoring, and adaptive access control.	[22,28,29]	3	Empirical/experimental; Conceptual/ Framework; Case-Study/ Qualitative
Data-Centric Protection Models	Security controls are applied directly to data through classification, encryption, governance policies, and data loss prevention mechanisms, ensuring protection regardless of location.	[28–30]	3	Empirical/experimental; Conceptual/ Framework; Case-Study/ Qualitative
Integrated Multi-Pillar Zero Trust Models	Comprehensive architectures combining identity verification, least privilege, micro-segmentation, continuous monitoring, and data-centric protection into a unified security framework.	[30]	1	Case-Study/ Qualitative

Note: Abbreviations: ZTA (Zero Trust Architecture), IAM (Identity and Access Management), MFA (Multi-Factor Authentication), SSO (Single Sign-On), RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), PBAC (Policy-Based Access Control), JIT (Just-in-Time), SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), XDR (Extended Detection and Response), PaC (Policy-as-Code), PDPs (Policy Decision Points), PEPs (Policy Enforcement Points).

Across the eight implementation themes identified in Table 5, although the reviewed studies generally converged on identity-centric security, least-privilege access, micro-segmentation, continuous monitoring, and adaptive policy enforcement as core implementation principles, the number of studies supporting individual themes varied, as shown in Table 5. The most frequently represented themes were micro-segmentation and continuous monitoring, each reported in four studies, whereas the integrated multi-pillar model was identified in only one study. Some differences also emerged regarding implementation feasibility, operational trade-offs, and the strength of empirical support. For example, Solanke [21] reported a substantial reduction in security breaches following the implementation of Zero Trust, indicating a indicating a reported positive outcome. In contrast, Segun Adanigbo et al. [23] acknowledged limitations in empirical validation and variability in implementation outcomes. Similarly, Emmanni [22] identified technical complexity and organizational resistance as important barriers to implementing ZTA in hybrid cloud environments, suggesting that adopting the model may be more difficult than the architectural benefits alone imply. Anasuri [25] also reported security improvements while acknowledging trade-offs involving resource utilization and latency. These differences suggest that the literature does not necessarily disagree about the underlying principles of Zero Trust. Still, it does differ in its assessment of how readily those principles can be implemented and evaluated across heterogeneous cloud environments. In addition, several studies primarily propose architectural frameworks or implementation strategies rather than providing longitudinal empirical evaluations [18–20,29]. Consequently, the convergence observed in the literature should be interpreted primarily as convergence around proposed implementation models and expected security benefits rather than definitive evidence that the same implementation approach will produce equivalent outcomes across hybrid, multi-cloud, and multi-tenant environments.

3.4 Security Benefits of Zero Trust Architecture

The reviewed literature generally associates ZTA with a range of potential security benefits in cloud computing environments. As indicated in Table 6, the commonly reported benefits included improved security posture, reduced attack surfaces, enhanced identity and access management, improved threat detection and response, greater visibility and monitoring, stronger regulatory compliance, increased cyber resilience, and support for secure cloud transformation. Although these themes were broadly consistent across the reviewed studies, the level of support varied across individual benefits, with some themes reported in four studies and others in only two. Importantly, the evidence should not be interpreted as uniformly empirically validated. Much of the literature was conceptual, framework-based, or review-oriented, meaning that the benefits described in these studies represent proposed or expected effects of ZTA mechanisms, whereas empirical or case-based studies provide evidence based on observed outcomes. Because empirical validation was limited, the findings are therefore presented primarily as reported or proposed security benefits rather than as consistently demonstrated effects across all cloud environments.

Table 6: Security benefits of zero trust architecture in cloud computing.

Security Benefit Theme	Description	Studies Reporting	Number of Supporting Studies (n)	Evidence Type
Enhanced Security Posture	May strengthen overall cloud security through continuous verification, least-privilege access, and elimination of implicit trust.	[31–33]	3	Conceptual/Framework; Case-Study/ Qualitative
Reduced Attack Surface	May restrict unauthorized access and minimize exposure of cloud resources through micro-segmentation and access controls.	[31,32,34]	3	Conceptual/ Framework
Improved Identity and Access Management	May enhance authentication, authorization, MFA implementation, RBAC/ABAC controls, and identity governance.	[33–36]	4	Conceptual/Framework; Case-Study/ Qualitative
Improved Threat Detection and Response	May enable faster identification and mitigation of suspicious activities through behavioral analytics and continuous monitoring.	[31–33,36]	4	Conceptual/Framework; Case-Study/ Qualitative
Insider Threat Mitigation	May reduce risks posed by malicious or compromised insiders through continuous verification and least-privilege enforcement.	[32,37]	2	Conceptual/ Framework
Regulatory Compliance and Governance	May support compliance with regulations through audit logging, monitoring, access controls, and data protection measures.	[33,34,37]	3	Conceptual/Framework; Case-Study/ Qualitative
Cyber Resilience and Breach Containment	May improve the ability to contain, isolate, and recover from cyberattacks while minimizing damage.	[38,39]	2	Conceptual/ Framework
Support for Secure Remote Work and Cloud Adoption	May facilitate secure access for distributed users and cloud-native environments without reliance on network perimeters.	[38–40]	3	Conceptual/ Framework

Note: Abbreviations: MFA (Multi-Factor Authentication), RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control).

A recurring theme in the literature was the potential for ZTA to enhance the overall security of cloud infrastructure. Some studies even highlighted the need to remove the implicit trust assumption and to verify access continuously before accessing any resource (Kodi, 2025) [31]. This was described as a

mechanism to mitigate the risks of unauthorized access and insider threats. One study proposed that granular access controls, continuous monitoring, and microsegmentation could improve security posture among organisations adopting Zero Trust [32]. Similarly, Sharma [33] contended that the "never trust, always verify" principle would be a potentially more effective cyber defense than perimeter-based security models against modern cyber threats.

The other commonly reported advantage was reducing the attack surface and limiting lateral movement in cloud environments. According to several studies, micro-segmentation was identified as an important mechanism, enabling smaller security zones to separate workloads and network resources, thereby limiting attackers' movement after a compromise [31]. The literature indicates that limiting communication between cloud resources and implementing least-privilege access policies may reduce opportunities for privilege escalation and unauthorized access. Across the reviewed evidence, some studies reported decreased attack exposure and improved containment of security incidents in organizations that implemented micro-segmentation [32,34].

Another recurring area identified across the literature was improving IAM. Several studies have highlighted the importance of Zero Trust in enhancing access control, including the incorporation of multifactor authentication (MFA), role-based access control (RBAC), attribute-based access control (ABAC), and continuous authentication mechanisms [35]. The reviewed literature described ZTA as potentially enhancing IAM by granting users access only to the extent needed to fulfill their roles, thereby reducing the risk of unauthorized access [33]. Additionally, IAM was described as a core component of Zero Trust implementation, as it continuously verifies user identity and implements dynamic access control [36]. Kuwari [34] described identity-based Zero Trust controls as a mechanism that could reduce unauthorized access incidents, highlighting the importance of ongoing identity validation in cloud environments.

The reviewed studies also frequently highlighted that enhanced threat detection and incident response capabilities are key security benefits of adopting ZTA. Some of the most common ways organizations were described as supporting faster detection of suspicious activity than traditional security methods included continuous monitoring, behavioral analytics, and real-time security assessment [31–33,36]. Sharma [33] highlighted the growing significance of combining AI and machine learning with Zero Trust strategies, as AI tools can detect anomalies and unusual user activities in real time, helping identify potential security breaches. In addition, automated incident response functions enable organizations to respond immediately to any detected threat, such as locking down accounts, redirecting traffic, or automatically encrypting sensitive data [31]. These features may support more timely incident response to security breaches and strengthen the company's resistance to cyberattacks.

A recurring theme across the reviewed literature was greater visibility and monitoring. To ensure the successful implementation of Zero Trust, organizations need to monitor, log, and collect large volumes of data on user activity, resource usage, network traffic, and system interactions [37]. By implementing Zero Trust, organizations often found they had greater visibility into their digital environments, enabling them to make more informed decisions about their operations and better manage security. Prasad [37] found that organizations that adopted Zero Trust typically gained a more comprehensive understanding of their digital environments, which was described as supporting security and operational decision-making. Similarly, Yerramsetty [32] noted that continuous monitoring can provide in-depth information on user actions and application activities, helping enhance security and streamline operations. The literature suggests that increased visibility may support security operations, detect inefficiencies and anomalies, and enable proactive response to new threats.

Another potential benefit identified in the reviewed literature is regulatory compliance and governance. Several authors highlighted the similarities between Zero Trust and other regulations, such as GDPR,

HIPAA, and PCI-DSS, that focus on least-privilege access, continuous monitoring, auditing logs, and data protection [33,34,37]. Kuwari [34] claimed that Zero Trust was described as providing mechanisms that may support organisational compliance through robust access controls, encryption, and monitoring. Sharma [33] noted that Zero Trust can aid in regulatory compliance by creating comprehensive audit trails and implementing fine-grained security policies. Prasad [37] pointed out that the robust authentication, authorization, and monitoring capabilities built into Zero Trust architectures may support compliance activities and audit processes.

The Zero Trust approach was associated with potential improvements in organizational resilience. These combine to make an organization more resilient in detecting, containing, and recovering from attacks. Bishukarma [38] characterized Zero Trust as potentially effective in addressing advanced threats such as phishing, ransomware, malware, and credential attacks because it continuously monitors user activity and network traffic, rather than relying solely on traditional defenses. Continual verification mechanisms may help limit attacker dwell time and potentially reduce the impact of breaches by quickly identifying and containing threats [39].

Finally, several studies also highlighted the role of Zero Trust in supporting secure cloud migration, hybrid cloud operations, and remote work environments [38]. Because Zero Trust security controls are identity-driven rather than location-dependent, organizations may be able to support geographically distributed users, cloud-native applications, and hybrid or multi-cloud infrastructures. Joy [39] noted that Zero Trust may support secure cloud migration by maintaining consistent security policies across different cloud providers and deployment environments. Gangina [40] observed that the location-independent nature of Zero Trust may support business agility by allowing organizations to adopt remote work models and cloud services while maintaining security controls.

Despite the overall convergence regarding the potential security benefits of ZTA, the reviewed studies differed in the strength and nature of the evidence supporting these benefits. Bishukarma [38] and Joy [39] primarily emphasize the protective value of Zero Trust mechanisms for multi-cloud SaaS and enterprise data environments, respectively, whereas Gangina [40], Kuwari [34], and Yerramsetty [32] provide largely conceptual, review-based, or framework-oriented accounts of how Zero Trust can strengthen cloud security. Thus, the literature more consistently demonstrates agreement about the expected mechanisms of benefit than about their empirically measured effectiveness. Where studies reported observed organizational or security outcomes, these findings are distinguished from benefits proposed primarily on theoretical or architectural grounds. In addition, the security advantages described in the literature are accompanied by potential operational trade-offs. Continuous monitoring and behavioral analytics can improve visibility and threat detection but may heighten privacy concerns due to extensive data collection, while broader implementation may entail trade-offs among security effectiveness, operational efficiency, and cost [36,37]. Therefore, no included study directly reported that ZTA provides no security benefit; however, the evidence does not establish that its benefits are uniform, cost-free, or equally demonstrated across all cloud environments.

3.5 Challenges and Limitations of Implementing ZTA

Several challenges and limitations were identified in the reviewed literature on the implementation of ZTA in cloud environments. Key implementation issues reported included complexity, integration with legacy systems, scalability, IAM challenges, performance issues, resource needs, user experience concerns, multi-cloud heterogeneity, and regulatory considerations, as shown in Table 7. Implementation complexity emerged as a frequently reported challenge across the reviewed literature. Another notable challenge identified in the reviewed studies concerns systemic operational constraints and vulnerabilities to centralization within zero-trust frameworks. For instance, implementing an anonymous cryptographic access

control model requires overcoming architectural dependencies that can impact practical deployment [41]. In cloud-native environments, these conditions add even more complexity, as organizations now need to manage distributed microservices and containerized workloads that require identity verification, continuous authentication, least-privilege enforcement, and policy orchestration. Implementing Zero Trust will be technically and organizationally challenging, as it requires significant coordination among network administrators, the security team, developers, and cloud architects [42]. The reviewed literature suggests that ZTA implementation complexity may extend beyond technological considerations to include organizational processes, governance structures, and workforce capabilities.

Table 7: Challenges and limitations associated with implementing zero trust architecture in cloud environments.

Challenge Theme	Description	Studies Reporting	Number of Supporting Studies (n)	Evidence Type
Implementation Complexity	Complexity associated with redesigning security architectures, deploying Zero Trust controls, and coordinating organizational change.	[41,42]	2	Empirical/experimental; Case-Study/Qualitative
Legacy System Integration	Difficulties integrating Zero Trust principles with existing applications, infrastructure, and legacy IAM systems.	[43,44]	2	Conceptual/Framework; Case-Study/Qualitative
Scalability Constraints	Challenges associated with scaling continuous authentication, monitoring, and policy enforcement across large cloud environments.	[46]	1	Case-Study/Qualitative
Performance Degradation	Challenges related to latency, CPU utilization, authentication overhead, and the performance impact of continuous verification, monitoring, encryption, and access-control processes.	[47–49]	3	Conceptual/Framework;
User Experience and Organizational Resistance	User friction due to repeated authentication requirements and resistance to organizational change.	[42,49,50]	3	Empirical/experimental; Conceptual/Framework; Case-Study/Qualitative
Multi-Cloud and Hybrid Cloud Complexity	Difficulty maintaining consistent policies across heterogeneous cloud platforms and environments.	[43,45]	2	Conceptual/Framework; Case-Study/Qualitative
Privacy and Regulatory Compliance Issues	Challenges balancing continuous monitoring with privacy requirements and regulatory obligations.	[43,46,48]	3	Conceptual/Framework; Case-Study/Qualitative

Note: Abbreviations: IAM (Identity and Access Management) and CPU (Central Processing Unit).

Another key challenge identified in the literature was integrating Zero Trust principles into legacy systems. Distributed cloud-native elements could not naturally integrate continuous authentication, least-privilege access, and micro-segmentation out of the box due to the fluid boundaries of microservices and ephemeral container environments. Volatile containers and default-exposed Kubernetes API servers often lack native runtime security configurations, making the enforcement of zero-trust controls complex and dynamic during auto-scaling events [43]. Similarly, current Identity and Access Management systems may not be compatible with new Zero Trust approaches and may require rewiring the entire architecture [44]. Prajapati [44] also pointed to this challenge–legacy system integration–as it is a common issue that companies must deal with when deciding to upgrade their current systems or replace them entirely. The reviewed

literature identifies the integration of legacy technology as a recurring challenge that may complicate Zero Trust adoption.

The literature also discussed scalability and integration within automated DevOps pipelines. As the volume of distributed microservices expands, maintaining continuous contextual verification, centralized secret rotation, and granular pod-to-pod traffic control across rapid release cycles becomes significantly harder to manage manually [43]. However, Zero Trust mechanisms can consume more CPU and memory resources, potentially impacting their efficiency and suitability for high-performance cloud setups [43]. A centralized policy engine can pose challenges in highly distributed systems, such as edge computing and the Internet of Things (IoT) [45]. These findings suggest that security performance and scalability are important considerations when implementing ZTA in distributed cloud environments.

Another common thread across the studies examined was the complexity of identity and access management. Specifically, Tian [41] exposed these underlying infrastructure challenges as data-owner online dependency and the risks of certificate authority (CA) centralization. Under such models, data owners must maintain constant online availability to manage dynamic user and attribute revocations, while relying on a single CA creates a centralized operational bottleneck and a single point of failure. The challenge was further identified as the complexity of identity management, in which organizations are required to constantly validate identities and devices, oversee permissions, audit access rights, and maintain accountability [41]. Also, cloud-native architectures demand advanced IAM solutions that can handle the evolving needs and dynamics of access and usage [46]. IAM implementation has been reported as cumbersome and demanding, requiring specific skills to be effective.

Other challenges reported by several studies include performance degradation. Several studies associated the use of continuous verification, monitoring, encryption, and access-control processes with potential increases in latency and CPU utilization [47–49]. Another study reported an initial performance loss during Zero Trust implementation, despite subsequent security enhancements [47]. Similarly, unnecessary authentication procedures and network segmentation can adversely affect system productivity and user interaction [48]. Ongoing authentication and encryption processes were described as potentially increasing latency, particularly in real-time or resource-constrained systems [49].

Financial and resource-related constraints were also commonly reported. Several studies identified investments in technology, infrastructure, personnel, training, and maintenance as factors that may be required to support Zero Trust deployment [42,49,50]. Zero Trust implementation may involve substantial initial costs, particularly for small and medium-sized businesses [50]. Investments in new technologies, security expertise, and network redesign may be necessary for organizations [49]. Singh [42] noted the need for significant computing power, expertise, and data handling infrastructure for AI-powered Zero Trust solutions.

Additionally, the stringent authentication and verification requirements of Zero Trust can create friction for end users, affecting productivity and acceptance [49,50]. Perumal et al. [49] found that repeated verification procedures could lead to negative user experiences and decreased operational efficiency. Singh [42] added that strict security measures can prompt users to find workarounds or sidestep security processes, thereby jeopardizing security goals. The reviewed literature suggests that security controls should be considered alongside usability and operational requirements when implementing ZTA.

Finally, several studies mentioned governance, privacy, and compliance issues. Several studies identified potential privacy and governance concerns associated with continuous monitoring, behavioral analytics, and the collection of large volumes of user and system data [46,48]. The issues of bias, explainability, and data governance in the context of AI were highlighted [46]. Also, the use of service meshes and policy-as-code was

described as supporting the measurement of defense-related security metrics [43]. Challenges in evaluating, assessing, and aggregating trust-related information in a distributed cloud environment were also noted [48]. The reviewed literature suggests that ZTA implementation may require organizations to balance security objectives with privacy, governance, and ethical considerations.

The reviewed studies did not provide direct evidence that ZTA is ineffective or that its security benefits are absent; rather, they reported divergent findings regarding the conditions under which those benefits can be achieved. However, the evidence supporting individual challenge themes was uneven, with some themes represented by only one or two studies. Perumal et al. [49] associated ZTA with improved security, regulatory compliance, and data protection, while also identifying implementation complexity and user experience concerns. Prajapati [44] similarly described IAM as fundamental to Zero Trust security but highlighted the challenges of legacy system integration, staffing requirements, identity complexity, and multi-cloud scalability. Singh [42] reported substantial security benefits while acknowledging significant technical, organizational, scalability, and usability barriers. Conversely, Tian [41] demonstrated that a specifically designed Zero Trust anonymous-access algorithm could improve encryption and decryption efficiency and reduce storage overhead compared with conventional approaches, suggesting that performance degradation is not an inevitable consequence of all Zero Trust implementations. Verma [43] also emphasized a gradual implementation through identity-first security and progressive micro-segmentation rather than an immediate, comprehensive deployment.

3.6 Research Gaps and Future Research Opportunities

The reviewed literature suggests that ZTA remains a developing security paradigm for cloud computing, with research gaps identified in implementation, optimization, scalability, interoperability, and the evaluation of longer-term effectiveness. As indicated in Table 8, the future research directions identified in the reviewed literature primarily concern dynamic policy enforcement, the use of Artificial Intelligence, trust assessment methods, interoperability between cloud-based platforms, privacy-related technologies, quantum-resistant security, and decentralized identity management, as well as the empirical testing of proposed models. The level of support for these research directions varied, with some themes identified across three studies and others reported in only two studies.

Table 8: Research gaps and future research opportunities in zero trust architecture for cloud computing.

Research Gap/Future Direction	Description	Reporting Studies	Number of Supporting Studies (n)	Evidence Type
Dynamic and Adaptive Policy Enforcement	Development of context-aware and risk-based access control mechanisms capable of continuously adjusting authorization decisions based on user behavior, device posture, and environmental conditions.	[51–53]	3	Empirical/experimental; Conceptual/ Framework
Artificial Intelligence and Machine Learning Integration	Use of AI, ML, Generative AI, and automation to enhance threat detection, behavioral analytics, adaptive access control, and automated incident response.	[51,54,55]	3	Empirical/experimental; Conceptual/ Framework
Advanced Trust Assessment Models	Improvement of trust evaluation mechanisms to increase accuracy, adaptability, context awareness, and computational efficiency across diverse cloud environments.	[52,56]	2	Conceptual/ Framework

(Continued)

Table 8 (continued)

Research Gap/Future Direction	Description	Reporting Studies	Number of Supporting Studies (n)	Evidence Type
Privacy-Preserving Zero Trust Technologies	Exploration of privacy-enhancing technologies such as homomorphic encryption, secure multi-party computation, and privacy-aware monitoring mechanisms.	[55,57]	2	Conceptual/ Framework
Quantum-Resistant Security Mechanisms	Investigation of post-quantum cryptography, quantum-resistant authentication, and quantum key distribution to protect future cloud infrastructures.	[58,59]	2	Conceptual/Framework; Case-Study/ Qualitative
Empirical Validation and Real-World Deployment Studies	Need for large-scale case studies, longitudinal evaluations, comparative analyses, and real-world implementation evidence.	[58,59]	2	Conceptual/Framework; Case-Study/ Qualitative

Note: Abbreviations: AI (Artificial Intelligence) and ML (Machine Learning).

A recurring research gap identified in the reviewed literature concerns the development of more dynamic and adaptive Zero Trust environments. Several studies have noted that existing or proposed Zero Trust implementations may rely on static security policies and predefined security rules, which some authors consider less suitable for highly dynamic cloud environments [51–53]. Another study identified a need for further development of fine-grained, context-aware access control mechanisms that can adapt their policies in real time to new user behaviors, device posture, application context, and environment [51]. It is also emphasized that there is a need for more complex dynamic authorization mechanisms that can adjust trust levels and access privileges as risk conditions change [52]. The reviewed literature suggests that future Zero Trust systems could benefit from a shift from the traditional static Authorization approach to an adaptive Security approach that can make continuous decisions [53].

Another noteworthy research opportunity is the role of artificial intelligence (AI), machine learning (ML), and automation in Zero Trust settings. AI-driven security analytics emerged as a recurring research focus for potentially supporting and enhancing threat detection, behavioral analysis, policy enforcement, and automated incident response [51,54,55]. Ibiyeye et al. [51] suggested using AI and machine learning to facilitate ongoing risk assessment and the flexible application of policies. Similarly, AI-based adaptive micro-segmentation and intelligent policy engines were identified as emerging research directions that may support cloud security [54]. Kadar [55] identified continued research in Generative AI, explainable AI, and hybrid AI as potential directions to improve transparency and support Zero Trust decision-making.

In the review, Trust assessment was also identified as an emerging research gap in two studies. Some studies suggested limitations in current trust evaluation mechanisms for assessing trustworthiness across various cloud environments for user, device, and workload trustworthiness [52,56]. The reviewed literature suggests that future trust-assessment models could place greater emphasis on accuracy, adaptability, contextual information, and additional trust factors [52]. Sarkar et al. [56] noted that more sophisticated trust-evaluation mechanisms were identified as a potential area for further development to enable ongoing verification and dynamic access control.

Two studies identified opportunities for privacy-preserving Zero Trust research. While continuous monitoring and behavioral analytics provide valuable security benefits, they can also be viewed as a privacy risk, raise privacy concerns about data collection, and uncover issues with regulatory compliance [55,57].

In particular, privacy-enhancing technologies such as homomorphic encryption and secure multi-party computation were identified as potential approaches to support verification while addressing user privacy concerns [57]. Robust ethical governance policies for AI in supporting transparency, accountability, and responsible data handling within the framework of an AI-powered Zero Trust system [55].

Two studies identified quantum-resistant security mechanisms as emerging research opportunities. Adaptation to post-quantum security challenges is a potential future research direction for Zero Trust systems, as advances in quantum computing threaten traditional cryptographic systems [58,59]. In maintaining the integrity of Zero Trust authentication and authorization systems, there is a potential investigation for quantum-resistant cryptography, such as lattice-based cryptography and quantum key distribution [58]. Similarly, Hariharan [59] highlighted post-quantum cryptography as an emerging research direction for strengthening security in multi-tenant cloud environments against potential future computational threats.

Finally, two of the reviewed studies identified limited empirical evidence as an important research gap concerning proposed Zero Trust frameworks. While many concepts and theoretical models have been proposed, relatively few studies in the reviewed literature evaluated their effectiveness in real-world enterprise cloud environments [59]. The reviewed literature remains substantially conceptual, with relatively limited empirical evaluation of proposed approaches. Additionally, the need to study the trade-offs among security effectiveness, operational efficiency, and implementation costs was highlighted [58]. Further empirical, longitudinal, and industry-based case studies could provide additional evidence regarding the effectiveness and practical implementation of ZTA deployments.

Although the reviewed studies broadly agree that further research is required to improve the adaptability, scalability, and practical effectiveness of Zero Trust Architecture, they differ on which specific problems are most important. Ike et al. [58] emphasize granular and dynamic access control and policy enforcement, whereas He et al. [52] identify more fundamental limitations in identity authentication, access control, and trust assessment, noting that Zero Trust remains at an early stage of practical development. Sarkar et al. [56] similarly demonstrate that existing Zero Trust models and frameworks offer different combinations of capabilities, and that implementation must be tailored to domain-specific cloud requirements. In contrast, Ibiyeye et al. [51] place greater emphasis on artificial intelligence and machine learning as mechanisms for adaptive threat detection and policy enforcement, while Cicek and Shafae [54] focus more specifically on micro-segmentation strategies and their operational challenges. Hariharan [59] extends the research agenda toward multi-tenant cloud environments, emphasizing tenant isolation, decentralized identity, and post-quantum security. These differences indicate that the literature does not converge on a single research priority or universally applicable ZTA model. Instead, future research priorities appear to be strongly influenced by the architectural context, with general cloud environments, micro-segmented infrastructures, AI-enabled systems, and multi-tenant platforms presenting different unresolved problems.

4 Discussion

4.1 Summary of Evidence

This scoping review aimed to map and synthesize the existing body of evidence on ZTA in cloud computing, with a particular focus on implementation models, security advantages, implementation barriers, and research gaps. The results demonstrated an overall increase in Zero Trust research over the past few years, highlighting the growing need for security approaches capable of addressing the security needs of increasingly distributed, cloud-native, hybrid, and multi-cloud environments. A recurring theme in the reviewed literature is that traditional perimeter-based security models may be insufficient for addressing the security of cloud infrastructure, especially in remote access environments, virtualization, microservices, and

the constantly changing threat landscape. Rather, the reviewed studies generally described the Zero Trust paradigm as being based on continuous verification, least-privilege principles, identity-based access control, and continuous monitoring.

The results directly contribute to the goal of this review: mapping and synthesizing implementation models, reported security benefits, implementation challenges, and research gaps of Zero Trust Architecture in cloud computing. This study was unable to identify a single predominant implementation strategy but rather a set of complementary architectural strategies that organizations select based on their operational needs. The reviewed literature identified several potential security benefits associated with Zero Trust, while also highlighting significant implementation challenges and several areas requiring further research to support its application across different cloud environments.

Regarding RQ1, the reviewed literature indicates that Zero Trust is increasingly identity-centric and policy-driven in the context of cloud computing. The need for identity verification has become the basic security perimeter in nearly every framework, rather than network boundaries. Key components of proposed and reported Zero Trust implementations were frequently highlighted in the reviewed studies: IAM, multi-factor authentication, continuous authentication, least-privilege access, and adaptive authorization. This pattern suggests that identity has become a central mechanism for establishing and continually evaluating trust in the cloud.

In addition to identity-centric approaches, micro-segmentation is one of the most widely adopted implementation strategies. Several studies reported or proposed that micro-segmentation may reduce opportunities for lateral movement following a security incident when cloud infrastructure is divided into smaller security zones, and that, at the same time, workload isolation and access control are enhanced. These implementation models were further supported by continuous monitoring, behavioral analytics, and automated policy enforcement, which may support the analysis of users' behavior, devices' posture, and contextual risks for each access session. In reality, the adoption of Zero Trust requires a multi-layered architecture that utilizes multiple security capabilities and is adaptable and constantly evolving.

Another key takeaway from the implementation models is the growing focus on hybrid and multi-cloud deployments. Several studies developed frameworks tailored to provide uniform identity management, policy enforcement, and governance across multiple cloud providers. This discovery mirrors the changing landscape of enterprise cloud adoption, as enterprises continue to operate across multiple cloud platforms rather than a single provider. This has led to a shift in focus from single clouds to architectures that support interoperability and uniform security governance across distributed infrastructures.

Regarding RQ2, the reviewed literature showed broad thematic agreement regarding the potential security benefits of Zero Trust adoption. A frequently reported benefit was improved security posture associated with ongoing verification and reduced reliance on implicit trust. Unlike perimeter-based methods, Zero Trust constantly verifies users, devices, applications, and workloads as it allows or maintains access, limiting the chances of unauthorized access and credential misuse. The overall pattern of findings supports the view that continuous verification is a central principle of Zero Trust security, although the strength of evidence supporting specific security outcomes varied across studies.

Additionally, several studies suggested that Zero Trust can reduce the attack surface in cloud environments. By combining least-privilege access controls and micro-segmentation, organisations may limit the flow of unwanted traffic between workloads and reduce an attacker's ability to move laterally after gaining access to a target system. These findings are relevant to security contexts involving ransomware, insider attacks, and advanced persistent threats that exploit excessive privileges and free movement across the

network. With granular authorization policies and workload isolation, Zero Trust can provide multiple layers of defense that may help mitigate the impact of a successful attack.

Another advantage reported in the literature that emerged in the review is the enhancement of identity and access management. The reviewed literature suggests that organisations may gain greater control over cloud resources through continuous authentication, multifactor authentication, adaptive authorization, and policy-based access control. This capability can be amplified with continuous monitoring, which may support the identification of anomalous behavior and suspicious activity in near real time. Additionally, the use of AI and behavioural analytics in Zero Trust deployments was mentioned in a few studies, suggesting potential opportunities for greater automation and context-awareness in the future.

The reviewed literature also conceptualizes Zero Trust as extending beyond a narrowly technical cybersecurity initiative to support an organization's overall goals. The benefits shown here illustrate that Zero Trust is not just a technical security solution, but a broader governance approach that may support digital transformation and security objectives. These are increasingly important organizational benefits as organizations keep moving more and more workloads to hybrid and multi-cloud.

Results from RQ3 indicate that the deployment of Zero Trust goes far beyond deploying individual security technologies and entails significant changes to the organization's security architecture, governance processes, and access management practices. However, the reviewed literature also identified several challenges in implementing Zero Trust effectively. The Zero Trust approach differs from traditional perimeter-centric security strategies by mandating that organizations reimagine their security architectures with continuous verification, identity-centric access control, policy-based authorization, and continuous monitoring. This transformation often requires the integration of multiple security technologies, as well as changes to organizational processes and governance. Implementation complexity is a recurring theme throughout the literature, suggesting that Zero Trust is better understood as an ongoing security transformation rather than a one-time technology deployment.

The results also highlight that legacy systems remain one of the main challenges to Zero Trust implementation. Perimeter-based security models were adopted when many existing enterprise applications and infrastructure were created, and they lack the capabilities to enable continuous authentication, adaptive authorization, or micro-segmentation. This mismatch may require substantial redesign, modernization, or adaptation of existing systems before some Zero Trust capabilities can be implemented effectively. The shift to cloud-based environments and the need to maintain legacy systems will remain a major implementation challenge as more organizations move towards cloud-native environments.

Scalability and performance were other common issues identified in the reviewed literature. Zero Trust demands continual authentication, policy assessment, monitoring, and telemetry gathering for all access requests, adding to the compute and network burden. Although these mechanisms are intended to strengthen security, several studies identified potential trade-offs involving latency, resource utilization, and operational complexity, particularly in large-scale deployments. These findings point to a potential trade-off between security controls and operational efficiency that warrants further empirical evaluation. In the future, more efforts should focus on optimizing Zero Trust architectures to ensure organizations can continue implementing strong security measures without sacrificing system performance or user productivity.

Additionally, user resistance, administrative hassles, staff competency issues, and budget limitations were identified as important potential barriers to adoption in several studies. The findings suggest that successful implementation may depend on both technological readiness and organizational preparedness. But organizational commitment, executive buy-in, employee training, and effective change management are also essential to the implementation process. The implementation of Zero Trust should be considered as a

technology effort and as part of an organization's transformational process, involving security professionals, IT administrators, business leaders, and end users.

The results of RQ4 showed that although research on Zero Trust is rapidly increasing, there are still many opportunities for further research. Adaptive and intelligent Zero Trust systems are one of the key research gaps identified during this review. Current solutions still rely heavily on predefined security policies, despite the ever-changing nature of cloud computing environments. Several of the reviewed studies proposed using AI, machine learning, and behavioral analytics to support ongoing risk assessment, automated policy adjustment, and threat response. These technologies may enhance adaptive security capabilities and operational efficiency, although their effectiveness, transparency, and implementation costs require further empirical evaluation. However, more research is needed to develop a more trustworthy, transparent, and explainable AI-based security model that organizations can adopt with confidence.

Interoperability was also identified as an important area for further study in the literature. The overall cloud infrastructure landscape is increasingly hybrid and multi-cloud, encompassing multiple cloud providers, each with distinct cloud-based identity management systems, security services, and policy frameworks. Implementing these Zero Trust policies consistently across diverse environments is challenging because there is no standardized approach. To this end, further work needs to focus on creating interoperable frameworks and protocols and cloud-agnostic policy management systems that enable secure operation in distributed cloud environments.

A further direction emerging from the performance and scalability challenges identified in this review concerns the integration of Zero Trust with green cloud multimedia networking and SDN-based task scheduling and load balancing. SDN-based resource management can dynamically distribute workloads and network traffic to improve resource utilization, reduce response or flow-completion times, and lower energy consumption, suggesting potential opportunities to make security enforcement more performance-aware [60]. In the context of ZTA, such mechanisms could be investigated for dynamically coordinating policy enforcement, continuous authentication, and micro-segmentation with available computing and network resources. This may be particularly relevant to cloud and edge environments supporting multimedia applications, where latency, bandwidth, workload variability, and energy efficiency are important operational considerations [61]. Future research could therefore examine whether SDN-enabled scheduling and load balancing can reduce the computational and communication overhead associated with continuous Zero Trust controls while maintaining appropriate security requirements. Green multimedia networking could similarly provide a useful context for evaluating how ZTA deployment can balance security, service quality, resource utilization, and energy efficiency.

Overall, the literature provides a generally favorable but qualified view of Zero Trust Architecture in cloud computing. No consistent body of evidence within the reviewed studies directly indicated that ZTA lacks potential security value; however, the available evidence is not sufficiently uniform or empirically developed to support claims of universal effectiveness. The findings are therefore best understood as demonstrating recurring evidence-informed themes and promising implementation approaches, rather than establishing that ZTA produces equivalent or consistently measurable security outcomes across all cloud environments.

4.2 Implications

The findings of this scoping review have significant implications in technological, organizational, regulatory, and practical aspects. The transition to cloud systems introduces disruptive technological paradigms, such as decentralised identity management, blockchain-based trust models, edge computing, the IoT, and next-generation communication networks. Current Zero Trust solutions need to adapt to the

distinct security challenges that arise in these new environments. More importantly, quantum-resistant cryptography needs to be actively investigated in research to ensure that fundamental authentication and encryption methods remain secure against future computational attacks.

Organisationally, the evidence suggests that it is very difficult to change the architecture physically, as it is not a practical approach to achieve overnight and entails too much operational risk. Rather, a step-by-step (phased) approach to implementation is recommended for enterprises. This step-by-step strategy enables organizations to modernize their aging infrastructure over time, regularly review security metrics, and continuously develop an internal technical skills base, as well as improve data governance and models. There is a phased rollout that helps to reduce the downside of operating the system, limits the capital risk, and helps manage user friction and ease into the culture.

The adoption of ZTA underscores a key policy and regulatory challenge: it involves a new, widespread, and rapidly growing technology. The widespread adoption of ZTA represents a critical policy and regulatory challenge, one that involves a new, broad, and emerging technology. The only way to ensure interoperability and avoid vendor lock-in across public, private, and hybrid cloud environments is through regulatory intervention and the adoption of uniform security frameworks. Moreover, as Zero Trust deployments become more sophisticated, incorporating advanced AI-driven automation and logging more behaviors, regulators will need to provide comprehensive guidelines that strike the right balance between stringent security monitoring and privacy and ethical data governance.

Finally, for cloud security practitioners, the study reinforces that Zero Trust is not simply about product deployment, but is a governance journey. To become publication-grade resilient, practitioners must continually evaluate the technical security aspects of the systems they design while also considering their usability and operational efficiency. Maintaining a stable posture is an ongoing task that involves continuous workforce upgrades, continual policy improvements, and the continuous integration of technology in rapidly evolving cloud environments.

4.3 Limitations

Although this scoping review provides an extensive and structured overview of the concept of ZTA in cloud computing, there are some limitations to consider. The search syntax and criteria for item structure were very narrowly targeted at peer-reviewed journal articles in English. Conference abstracts, conference proceedings, white papers, book chapters, dissertations, and grey literature have been excluded from the review. They may have been overlooked, even though they are highly relevant and might contain cutting-edge technical frameworks or practical deployment case studies. This is especially evident in a field like ZTA, which is very fast-moving and industry-driven, so important developments are often first released in technical white papers from vendors, vendor documentation, or the proceedings of specialized security conferences. Additionally, although all included studies met the predefined peer-reviewed journal eligibility criterion, the evidence base varied in publication venue, methodological approach, and empirical depth. Of the 42 included studies, 10 (23.8%) were published in established or widely indexed scholarly venues, while 32 (76.2%) were published in less-established or less-well-indexed venues. This variation was considered when interpreting the synthesized findings, particularly because a substantial proportion of the literature was conceptual or framework-based.

Second, the time period was limited to January 2020 to May 2026. This range highlighted recent interest in cloud-based Zero Trust research but restricted the scope to papers published after the last database search, thereby excluding earlier foundational papers and very recent paradigm shifts that emerged after the database search. Thirdly, a review protocol was considered during the planning of the study but was not prospectively registered in an external registry such as OSF. The review was conducted using predefined

eligibility criteria, a structured search strategy, and a consistent screening and data-charting process aligned with the PRISMA-ScR framework. Nevertheless, the absence of prospective protocol registration limits independent verification of the review procedures.

Fourth, scoping reviews cannot be used to appraise the methodological quality and/or risk of bias of individual studies. The scope of a scoping review is to map the breadth and structural features of an existing body of literature, not to appraise the methodological quality and/or risk of bias of individual studies. For this reason, this review does not assess the empirical validity, performance metrics, or rigor of the model simulations proposed in the 42 included papers. Fifth, because a high percentage of the included literature was conceptual, the results of the synthesis are largely theory-laden and do not yield firm, quantifiable evidence of operational efficiency in the real world for the various configurations used. Finally, the review was conducted by a single reviewer who performed title and abstract screening, full-text assessment, and data charting. Although predefined eligibility criteria and a structured data-charting process were used to promote consistency, the absence of an independent second reviewer or inter-rater reliability check may have introduced potential selection and data-extraction bias. This limitation should be considered when interpreting the included evidence and synthesized findings.

5 Conclusions

This scoping review successfully maps and synthesizes the ever-growing literature on ZTA in the context of cloud computing, addressing the key research questions and objectives. The structural analysis of the included studies finds an urgent need to move beyond traditional perimeter-based network security approaches and adopt a more adaptive (Identity-centric, Context-aware) approach to network security. ZTA is designed to reduce reliance on implicit trust that comes with network location and may support a more resilient security environment specifically designed for the dynamic, distributed nature of today's cloud-native, hybrid, and multi-cloud environments. Today, the four key elements of continuous identity verification with unified IAM, strict enforcement of granular least-privilege access, network-level and workload-level micro-segmentation, and continuous telemetry monitoring are strong pillars for current cloud-based ZTA implementations. These architectural principles are associated in the reviewed literature with potential security benefits, including a potential reduction in the attack surface of the organization, potentially improved containment of lateral threat movement after a compromise, increased visibility of access to the data, potential mitigation of insider threats, and potential support for compliance and governance for stringent regulatory data frameworks like GDPR, HIPAA, and PCI-DSS.

The review, however, makes it evident that it is not software or technology that needs to be deployed, but rather a multi-layered, long-term, cross-functional organizational shift towards a Zero Trust state. Organisations have to deal with deployment challenges of a very severe nature in many aspects. They range from significant (or massive) technical and architectural complexity to compatibility friction at the level of integration with legacy systems and older architectural designs. Additionally, policy enforcement scalability issues in highly distributed architectures lead to significant performance latencies due to continuous cryptographic processes, continuous authentication checks, and intensive logging requirements. Moreover, organisational friction, skills shortages in the workforce, high initial capital investment costs, and user experience challenges resulting from multiple verification hurdles are important barriers to organisational uptake. Balancing tight security constraints with usability and operational efficiency is the primary challenge faced by modern practitioners.

The key future research and practice opportunities should be directed towards closing these important gaps. First, there is a pressing demand for large-scale empirical validation of rigor rather than conceptual, framework-based, and theoretical papers. Further studies are needed to support the proposed ZTA models

with empirical evidence, longitudinal evaluation techniques, and specific real-world case studies that challenge and test them in diverse enterprise cloud environments. Second, research efforts need to focus on the more sophisticated integration of Artificial Intelligence (AI), Machine Learning (ML), and Generative AI into existing static, rule-based policy engines to transform them into fully autonomous, context-aware policy models capable of making real-time policy changes. Thirdly, it is crucial to establish standardized, cloud-agnostic protocols that enable seamless structural interoperability and consistent security governance across the intricate multi-cloud landscape. Finally, future frameworks need to accommodate privacy-preserving solutions, such as homomorphic encryption, that enable continuous monitoring without compromising user privacy rights, and build security solutions for the underlying authentication systems that address emerging threats in quantum computing.

Acknowledgement: Not applicable.

Funding Statement: The author received no specific funding for this study.

Availability of Data and Materials: The data that support the findings of this study are available from the Corresponding Author, [Darlington Chigozie Okeke], upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A: Database-specific search strategies.

Database	Search Strategy	Filters
IEEE Xplore	("Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" OR ZTA OR ZTNA) AND ("cloud computing" OR "cloud security" OR "cloud environment*" OR "multi-cloud" OR "hybrid cloud" OR "cloud-native") AND (implementation OR framework* OR model* OR adoption OR benefit* OR challenge* OR limitation* OR "security benefit*" OR "identity and access management" OR micro-segmentation OR "research gap*" OR "future research")	**Content type:** Journals **Year range:** 2020–2026
ACM Digital Library	("Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" OR ZTA OR ZTNA) AND ("cloud computing" OR "cloud security" OR "cloud environment*" OR "multi-cloud" OR "hybrid cloud" OR "cloud-native") AND (implementation OR framework* OR model* OR adoption OR benefit* OR challenge* OR limitation* OR "security benefit*" OR "identity and access management" OR micro-segmentation OR "research gap*" OR "future research")	**Publication date**: 2020–2026 **Publications:** Journal

(Continued)

Appendix A (continued)

Database	Search Strategy	Filters
SpringerLink	("Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" OR ZTA OR ZTNA) AND ("cloud computing" OR "cloud security" OR "cloud environment*" OR "multi-cloud" OR "hybrid cloud" OR "cloud-native") AND (implementation OR framework* OR model* OR adoption OR benefit* OR challenge* OR limitation* OR "security benefit*" OR "identity and access management" OR micro-segmentation OR "research gap*" OR "future research")	**Content type:** Research article **Publishing model:** open access **Date published:** 2020–2026 **Languages:** English
ScienceDirect	("Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" OR ZTA OR ZTNA) AND ("cloud computing" OR "cloud security" OR "cloud environment*" OR "multi-cloud" OR "hybrid cloud" OR "cloud-native") AND (implementation OR framework* OR model* OR adoption OR benefit* OR challenge* OR limitation* OR "security benefit*" OR "identity and access management" OR micro-segmentation OR "research gap*" OR "future research")	**Years:** 2020–2026 **Article type:** research articles and review articles **Languages:** English
Google Scholar	"Zero Trust Architecture" OR "Zero Trust Security" OR "Zero Trust Network Access" AND "cloud computing" OR "cloud security" AND implementation OR framework OR model OR challenges	**Years (Custom range):** 2020–2026 **Any type**: Review articles

References

1. Alzide S. Cloud computing: evolution, challenges, and future prospects. J IT Cybersecur AI. 2024;1(1):52–63. doi:10.70715/jitcai.2024.v1.i1.007.
2. Mell P, Grance T. The NIST definition of cloud computing. Gaithersburg, MD, USA: NIST Special Publication; 2011.
3. Akhtar DN, Kerim DB, Perwej DY, Tiwari DA, Praveen DS. A comprehensive overview of privacy and data security for cloud storage. IJSRSET. 2021:113–52. doi:10.32628/ijsrset21852.
4. Shah V. Managing security and privacy in cloud frameworks: a risk with compliance perspective for enterprises. Int J Curr Eng Technol. 2022;12:606–18.
5. Narendra R, Sr T, Mustafa SS. Cloud computing security challenges. SSRN Electron J. 2020;7(6):1–6. doi:10.17148/iarjset.2020.7817.
6. Umakor MF. Enhancing cloud security postures: a multi-layered framework for detecting and mitigating emerging cyber threats in hybrid cloud environments. IJCATR. 2025;9(12):438–51. doi:10.7753/ijcatr0912.1012.
7. Dawood M, Tu S, Xiao C, Alasmary H, Waqas M, Rehman SU. Cyberattacks and security of cloud computing: a complete guideline. Symmetry. 2023;15(11):1981. doi:10.3390/sym15111981.
8. Potla S. Securing multi-cloud environments: challenges and solutions. JCSTS. 2025;7(4):780–5. doi:10.32996/jcsts.2025.7.4.90.

9. Santucci F, Oliva G, Gonnella MT, Briga ME, Leanza M, Massenzi M, et al. Implementing zero trust: expert insights on key security pillars and prioritization in digital transformation. Information. 2025;16(8):667. doi:10.3390/info16080667.
10. Nasiruzzaman M, Ali M, Salam I, Miraz MH. The evolution of zero trust architecture (ZTA) from concept to implementation. In: Proceedings of the 2025 29th International Conference on Information Technology (IT); 2025 Feb 19–22; Zabljak, Montenegro. p. 1–8. doi:10.1109/it64745.2025.10930254.
11. Lindemulder G, Kosinski M, Chrystal. What is zero trust? 2024 [cited 2026 Jul 28]. Available from: https://www.ibm.com/think/topics/zero-trust.
12. Muhammad Z. Zero trust architecture (ZTA) design and implementation, a comprehensive review. Am J Innov Sci Eng. 2026;5(1):18–25. doi:10.54536/ajise.v5i1.5905.
13. Mushtaq S, Mohsin M, Mushtaq MM. A systematic literature review on the implementation and challenges of zero trust architecture across domains. Sensors. 2025;25(19):6118. doi:10.3390/s25196118.
14. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput Secur. 2022;122:102911. doi:10.1016/j.cose.2022.102911.
15. Gambo ML, Almulhem A. Zero trust architecture: a systematic literature review. arXiv:2503.11659. 2025.
16. Dakić V, Morić Z, Kapulica A, Regvart D. Analysis of azure zero trust architecture implementation for mid-size organizations. J Cybersecur Priv. 2025;5(1):2. doi:10.3390/jcp5010002.
17. Ashogbon A, Okpere O. Evaluating the application of zero trust architecture (ZTA) implementation in Nigeria's banking industry. JEEE. 2025;13(3):131–42. doi:10.11648/j.jeee.20251303.12.
18. Guntaka NYR. Zero trust and cloud identity: building a resilient security framework. Int J Sci Res Comput Sci Eng Inf Technol. 2025;11(1):3450–60. doi:10.32628/cseit251112368.
19. Poddar S. Zero trust network architectures in multi-cloud environments. J Inf Syst Eng Manage. 2025;10:1085–92. doi:10.52783/jisem.v10i58s.12771.
20. Rehan H. Zero-trust architecture for securing multi-cloud environments. Sarcouncil J Eng Comput Sci. 2025;4(7):1161–9. doi:10.21275/sr25047220126.
21. Solanke AA. Zero trust security architectures for multi-cloud environments: implementation strategies and measurable outcomes. World J Adv Eng Technol Sci. 2021;3(2):122–34. doi:10.30574/wjaets.2021.3.2.0054.
22. Emmanni PS. Implementing a zero trust architecture in hybrid cloud environments. IJCTT. 2024;72(5):33–9. doi:10.14445/22312803/ijctt-v72i5p104.
23. Segun Adanigbo O, Iyanu Adekunle B, Ogbuefi E, Timothy Odofin O, Aderemi Agboola O, Kisina D. Implementing zero trust security in multi-cloud microservices platforms: a review and architectural framework. IJAMRS. 2024;4(6):2402–9. doi:10.62225/2583049x.2024.4.6.4357.
24. Akavaram S. Zero-trust security architecture for multi-tenant cloud applications. J Inf Syst Eng Manage. 2026;11(1s):944–52. doi:10.52783/jisem.v11i1s.14213.
25. Anasuri S. Zero-trust architectures for multi-cloud environments. IJETCSIT. 2022;3(4):64–76. doi:10.63282/3050-9246.ijetcsit-v3i4p107.
26. Nalla KK. Building zero-trust security models in cloud environments: best practices for enterprises. World J Adv Eng Technol Sci. 2024;11(1):424–36. doi:10.30574/wjaets.2024.11.1.0009.
27. Kalejaiye AN, Shonubi JA. Zero trust enforcement using microsegmentation, identity-aware proxies, and continuous adaptive risk assessment in multi-tenant cloud environments. IJCATR. 2025;14(7):61–77. doi:10.7753/ijcatr1407.1006.
28. Wang R, Li C, Zhang K, Tu B. Zero-trust based dynamic access control for cloud computing. Cybersecurity. 2025;8(1):12. doi:10.1186/s42400-024-00320-x.
29. Vodapally R, Vodapally R. Zero trust architecture in cloud environments: a framework for securing distributed systems. IRE J. 2024;8(3):818–29. doi:10.36227/techrxiv.176591845.57793075/v1.
30. Thambireddy S, Reddy Bussu VR, Anbalagan B, Pasumarthi A. Zero trust in practice: how enterprises are implementing zero trust architectures across multi-cloud system. Res Analy Jour. 2024;7(12):36–46. doi:10.18535/raj.v7i12.542.

31. Kodi D. Zero trust in cloud computing: an AI-driven approach to enhanced security. SSRG-IJCSE. 2025;12(4):1–8. doi:10.14445/23488387/ijcse-v12i4p101.
32. Yerramsetty H. Zero trust architecture in cloud computing: a paradigm shift in platform engineering security. IJFMR. 2024;6(6):29765. doi:10.36948/ijfmr.2024.v06i06.29765.
33. Sharma H. Zero trust in the cloud: implementing zero trust architecture for enhanced cloud security. ESP J Eng Technol Adv. 2022;2(2):78–91. doi:10.56472/25832646/JETA-V2I2P110.
34. Kuwari L. A survey on zero trust security architecture in cloud ecosystems. Int J Cloud Comput Database Manage. 2025;6(1):23–8. doi:10.33545/27075907.2025.v6.i1a.81.
35. Thallam NS. Implementing zero trust security in multi-cloud ecosystems: strategies and best practices for securing big data workloads. Eur J Adv Eng Technol. 2025;12(7):11–8. doi:10.5281/zenodo.16418233.
36. Nzeako G, Shittu RA. Implementing zero trust security models in cloud computing environments. World J Adv Res Rev. 2024;24(3):1647–60. doi:10.30574/wjarr.2024.24.3.3500.
37. Prasad SV. Zero trust architecture: the future of enterprise security. World J Adv Eng Technol Sci. 2025;15(1):660–6. doi:10.30574/wjaets.2025.15.1.0247.
38. Bishukarma R. Scalable zero-trust architectures for enhancing security in multi-cloud SaaS platforms. IJARSCT. 2023:1308–19. doi:10.48175/ijarsct-14000s.
39. Joy N. Zero-trust architecture in cloud security: a model for enterprise data protection. IJERET. 2024;5:29–39. doi:10.63282/3050-922x.ijeret-v5i4p104.
40. Gangina P. Demystifying zero-trust architecture for cloud applications. JCSTS. 2025;7(9):542–8. doi:10.32996/jcsts.2025.7.9.62.
41. Tian J. Zero trust anonymous access algorithm for multi cloud storage system based on CP-ABE. Egypt Inform J. 2025;30:100681. doi:10.1016/j.eij.2025.100681.
42. Singh HP. Beyond perimeters: zero trust security models in distributed cloud architectures. World J Adv Res Rev. 2025;26(2):3545–53. doi:10.30574/wjarr.2025.26.2.1909.
43. Verma S. Zero trust architecture in cloud-native environments: implementation strategies & best practices. IJCTT. 2025;73(4):102–7. doi:10.14445/22312803/ijctt-v73i4p114.
44. Prajapati V. Role of identity and access management in zero trust architecture for cloud security: challenges and solutions. IJARSCT. 2025:6–18. doi:10.48175/ijarsct-23902.
45. Simhadri S. Adaptive zero trust security: integrating artificial intelligence for dynamic cloud security. IJCESEN. 2026;12(1):735–41. doi:10.22399/ijcesen.4901.
46. Kommera S. Enhancing zero trust architecture with AI-driven threat intelligence in cloud environments. Int J Sci Res Comput Sci Eng Inf Technol. 2025;11(1):1524–33. doi:10.32628/cseit251112163.
47. Chimakurthi VNSS. The challenge of achieving zero trust remote access in multi-cloud environment. ABC J Adv Res. 2020;9(2):89–102. doi:10.18034/abcjar.v9i2.608.
48. Mehraj S, Banday MT. Establishing a zero trust strategy in cloud computing environment. In: Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI); 2020 Jan 22–24; Coimbatore, India. p. 1–6. doi:10.1109/ICCCI48352.2020.9104214.
49. Perumal AP, Deshmukh H, Chintale P, Desaboyina G, Najana M. Implementing zero trust architecture in financial services cloud environments in Microsoft azure security framework. Int J Circ Comput Netw. 2022;3(2):75–80. doi:10.33545/27075923.2022.v3.i2a.70.
50. Ahmadi S. Zero trust architecture in cloud networks: application, challenges and future opportunities. JERR. 2024;26(2):215–28. doi:10.9734/jerr/2024/v26i21083.
51. Ibiyeye S, Olajide TD, Onwuegbuchi O, Amoran SO, Ibiyeye AO. Zero-trust architecture reinforced by artificial intelligence in cloud computing. Int J Cloud Comput Database Manage. 2024;5(2):143–54. doi:10.33545/27075907.2024.v5.i2b.124.
52. He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: challenges and future trends. Wirel Commun Mob Comput. 2022;2022:6476274. doi:10.1155/2022/6476274.
53. Juremi J, Tonny NT, Ishraq KF. Zero trust architecture in cloud security: enhancing security posture in the cloud era. JATI. 2025;9(1):51–6. doi:10.65136/jati.v9i1.3.

54. Cicek NE, Shafae N. Zero Trust micro-segmentation in cloud environments: a systematic literature review of strategies, challenges, and future trends. 2025 [cited 2026 Jul 28]. Available from: https://ju.diva-portal.org/smash/get/diva2:2022391/FULLTEXT01.pdf.
55. Kadar A. Redefining zero trust architecture with generative AI capabilities in the cloud 2025. In: IEEE Conference Publication. New York, NY, USA: IEEE; 2025.
56. Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: a comparative review. Sustainability. 2022;14(18):11213. doi:10.3390/su141811213.
57. Khan RI, Bin Habib MQ, Hasan MM, Shad KWU. Zero trust architecture in cloud-native environments: a scalable framework for cybersecurity. Int J Sci Res Arch. 2026;18(1):296–305. doi:10.30574/ijsra.2026.18.1.0063.
58. Ike CC, Ige AB, Oladosu SA, Adepoju PA, Amoo OO, Afolabi AI. Redefining zero trust architecture in cloud networks: a conceptual shift towards granular, dynamic access control and policy enforcement. Magna Sci Adv Res Rev. 2021;2(1):74–86. doi:10.30574/msarr.2021.2.1.0032.
59. Hariharan R. Zero trust security in multi-tenant cloud environments. JISEM. 2025;10(45s):623–44. doi:10.52783/jisem.v10i45s.8899.
60. Mahdizadeh M, Montazerolghaem A, Jamshidi K. Task scheduling and load balancing in SDN-based cloud computing: a review of relevant research. J Eng Res. 2025;13(4):3132–46. doi:10.1016/j.jer.2024.11.002.
61. Alnaim AK, Alwakeel AM. Zero-trust mechanisms for securing distributed edge and fog computing in 6G networks. Mathematics. 2025;13(8):1239. doi:10.3390/math13081239.