ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

Modernizing IT Audit Function to Support to Support Zero Trust and Cloud Security – A Systematic Review

Whenume O. Hundeyin[1]

Publication Date: 2025/10/08

Abstract:

- ***Aim:***

This study aims to examine how IT audit functions can be modernised to effectively support Zero Trust and cloud security frameworks in contemporary organisations.

- ***Methods:***

A systematic review was conducted following the PRISMA 2020 guidelines. Peer-reviewed studies published between 2015 and 2024 were retrieved from databases including Google Scholar, OpenAlex, Crossref, and Semantic Scholar. The review included qualitative, quantitative, and mixed-method studies that focused on Zero Trust and cloud security implementation within IT audit functions. Thematic analysis was used to synthesise data from twelve included studies.

- ***Results (Findings/Discussion):***

The findings highlight major challenges such as integration complexity, lack of centralised visibility, compliance burdens, and high implementation costs. Core implementation strategies include robust Identity and Access Management (IAM) practices—such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), and federated identity protocols—alongside micro-segmentation, continuous monitoring using SIEM and UEBA, and automation through Policy-as-Code. Cloud-agnostic architectures and phased deployment approaches were found to enhance adaptability and audit alignment across single-cloud, hybrid, and multi-cloud environments.

- ***Conclusion:***

The review reveals that despite persistent technical and organisational challenges, a set of consistent, security-aligned audit practices can serve as a strategic foundation for modernising IT audit functions. These findings provide a basis for developing resilient audit frameworks aligned with evolving cloud infrastructures.

Keywords: *IT Audit, Zero Trust, Cloud Security, Continuous Assurance, Policy-as-Code, Identity and Access Management.*

How to Cite: Whenume O. Hundeyin (2025) Modernizing IT Audit Function to Support to Support Zero Trust and Cloud Security – A Systematic Review. *International Journal of Innovative Science and Research Technology*, 10(10), 249-259. https://doi.org/10.38124/ijisrt/25oct056

I. INTRODUCTION

In today's digital landscape, characterized by cloud and hybrid infrastructures, as well as sophisticated cyber threats, traditional IT audit functions based on periodic checks and fixed control lists are becoming increasingly outdated. Organisations now demand audit systems that are continuous, adaptive, and integrated with advanced security models such as Zero Trust Architecture (ZTA) and cloud-native frameworks. Sharma (2022) argues that IT auditing should go beyond compliance, incorporating active policy enforcement, incident readiness, and dynamic risk assessment. Syed et al., (2022) support this by demonstrating how real-time session monitoring and access control within Zero Trust VPNs transform audit processes into live components of security enforcement. Similarly, Aldossary and Allen (2016) emphasise the importance of remote auditability and data integrity in distributed, cloud-based environments.

These developments reveal that perimeter-centric audit models, based on implicit trust of internal users and static network boundaries, can no longer meet modern security and assurance demands. Bell *et al.* (2024) advocated for a Zero Trust approach, where trust is never assumed and all access is continuously verified through identity management, encryption, and network segmentation. Yeoh *et al.* (2023) describe Zero Trust as a data-focused framework well-suited to cloud and mobile ecosystems, while Sarkar *et al.* (2022) highlight its role in detecting threats through continuous behavioural monitoring. Taken together, these perspectives

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

underline the urgent need to modernise IT audit functions. Adopting Zero Trust and cloud security frameworks not only fortifies technical controls but also enhances the strategic value of IT audit, supporting continuous assurance, rapid risk adaptation, and alignment with today's dynamic, cloud-driven threat landscape.

➢ *Justification of Study*

Traditional IT audit models, often reliant on static controls and periodic reviews, face significant limitations in cloud-based, decentralized environments, including reduced control visibility and real-time assurance gaps (Aldossary & Allen, 2016; Lund et al., 2024). Therefore, perimeter-based security is no longer effective, and weak visibility in virtual systems increases risk (Aljohani, 2023; Bell et al., 2024; Sarkar et al., 2022). Integrating Zero Trust and cloud security offers continuous verification and strict access control (Ghasemshirazi et al., 2023; Yeoh et al., 2023). This review helps researchers and IT audit professionals modernise audit practices for contemporary organisational needs by providing a foundation for developing adaptive audit strategies, refining implementation practices, and supporting more resilient security frameworks in evolving digital ecosystems.

➢ *Main Research Question*

How can IT audit functions be mordernized to effectively support Zero Trust and cloud security frameworks in contemporary organizations?

➢ *Research Aim*

To review how IT audit functions can be enhanced to achieve zero trust and cloud security frameworks in modern organizations.

➢ *Research Objectives*

- To highlight the key challenges/limitations in the application of IT audit functions in achieving Zero Trust and cloud security in organizations.
- To analyse the best IT audit functions, practices, and technologies that ensure Zero Trust and cloud security can be achieved in modern organizations.
- To recommend a new framework for IT audit functions that ensures Zero Trust and cloud security initiatives.

II. RESEARCH DESIGN AND METHODS

The systematic review and meta-analysis utilise the research question to identify, select, and synthesise all high-quality research evidence relevant to the study(Khedkar, 2014). Although popular in medicine, the authors use it to collect relevant data sufficient for quality methodological assessment of the subject discussed in this review. It follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guideline, which ensures a more precise and quality result via its checklist during the systematic and meta-analysis process(Kahale et al., 2021).

Systematic review is a structured review approach that offers guidelines and checklists to ensure that the best evidence available for a study from different sources is synthesized to minimize biases and errors, and to present results and conclusions that are reproducible (Brignardello-Petersen et al., 2024) In this study, an appropriate systematic review would help gather the best available evidence and assess, from the included papers, a quality study outcome via a statistical meta-analysis. Meta-analysis is a statistical method that combines and synthesizes results from multiple independent studies to produce a single, more precise estimate of an effect (Dommari & Khan, 2023)

➢ *Research Ethics*

A meticulous procedure was followed to ensure that the review's ethics were observed, in order to avoid future implications regarding the procedure and outcome of the study (Suri, 2019) The authors conducted a detailed study of the topic, sourcing relevant papers from different databases to validate the integrity and reliability of the reviewed results. A predefined criterion was followed for the selection process to avoid bias. The authors ensured accountability and reproducibility of the methodology by following predefined guidelines in the design adopted to improve the credibility of the review. There were no conflicts of interest or funding before, during, or after the review.

➢ *Search Strategy*

Developing an adequate search strategy is significant to obtaining the best evidence available for a study. It narrows down the search to items or terms relevant to the study topic and ensures efficient utilization of different databases. The authors used Google Scholar, OpenAlex, Crossref, and Semantic Scholar databases to source papers via appropriate utilization of key search words or terms, quotes, and Boolean operators such as "AND" and "OR" in these databases. Multiple databases were consulted to ensure authenticity and credibility of the review, and to eliminate bias in the selection process. "Cloud security," "Zero Trust," "Implementing Zero Trust," "IT audit," "IT risk assessment," "IT control operation," and "Contemporary Organization" are the search terms and keywords used by the authors for the search process. Also, quotes and Boolean operators like "AND" and "OR" were used to generate a precise result during the search.

Table 1 Search Strategy

Key Terms	Alternative Search keywords
Cloud Security	Cloud environment, Cloud network, Cybersecurity
Zero Trust	Zero Trust Architecture, Zero Trust framework
IT audit Function	IT risk assessment, IT governance, IT control operation
Contemporary Organization	Adaptive organization, modern Organization
Implementing Zero Trust	Integrating Zero Trust Architecture

Source: Author's Compilations

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

- *Inclusion Criteria for Systematic Review*

The structured format adhered to in a systematic review sets it apart from other types of reviews. Predefined eligibility criteria, as shown in Table 2, were followed in the search and review process. The inclusion criteria include studies that report effective implementation of Zero Trust and Cloud Security architecture in IT audit functions and in modern organizations; studies that use qualitative, quantitative, or mixed methods; and studies published in English between 2015 and 2024.

- *Exclusion Criteria for Systematic Review*

The exclusion criteria include studies that do not focus on implementing IT audit functions with Zero Trust and Cloud Security frameworks but instead use other methods; studies that are not peer-reviewed; studies that adopt methodologies other than quantitative, qualitative, or mixed methods; and studies not published in English or published before 2015.

Table 2 Exclusion Criteria for Systematic Review

Criteria for Inclusion	Criteria for Exclusion
Studies that report implementing IT audit Function with Zero Trust and Cloud Security, Cloud Network, Cloud Environment Framework in modern organization	Studies that do not report implementing IT audit Function: IT risk assessment, IT control Operation with Zero Trust and Cloud Security, Cloud Network, Cloud Environment in modern or adaptive organization.
Studies carried out from 2015-2024	Studies before 2015
Journals/article that uses any of qualitative, quantitative and mixed method	Systematic reviews, books, conference proceeding and journals/articles that use neither of qualitative, quantitative and mixed method
Publications typed in English and peer-reviewed journal	Publications in other languages and studies not peer-reviewed

Source: Author's Compilations

➢ *Study Selection for Systematic Review*

A strategic search was implemented using Harzing's Publish or Perish to search multiple e-databases—Google Scholar, OpenAlex, Crossref, and Semantic Scholar—for relevant papers published between 2015 and 2024 (Harzing, 2010) The software keeps a record of every search conducted in each database. Search operations varied across the databases, as some do not support Boolean operators. This helped the authors ensure that no journals or articles were left out during the search.

The authors saved the retrieved journal/article results in BibTeX format and uploaded them into Mendeley Reference Manager to sort duplicates and correct other errors. Mendeley was used in this systematic review to organise sources, remove duplicates, and streamline the review process (Elston, 2019). The authors further filtered the remaining papers by meticulously reviewing the titles and abstracts, excluding irrelevant ones based on some of the criteria stated in Table 2. The remaining papers were then assessed against the eligibility criteria in Table 2 to select those that would be included in the systematic review.

- *The PRISMA Flowchart*

The PRISMA flowchart outlines each step of the study selection process, from identification to final inclusion, providing a transparent overview that enhances the review's credibility and reproducibility (Kahale et al., 2021). From the search process, a total of 453 records were identified from the electronic databases. The authors checked for duplicates, books, and conference proceedings, and used an automation tool to eliminate ineligible materials due to erroneous metadata. The remaining 143 papers were screened by title and abstract against the predefined inclusion criteria outlined in Table 2, resulting in the exclusion of 102 papers. Of the remaining 41, 11 could not be retrieved due to inaccessible full texts. Thus, 30 full-text papers were reviewed and screened for methodology, context, and scope in relation to the predefined criteria in Table 2. Out of the 30 papers, 18 were excluded for not meeting the minimum inclusion criteria, leaving 12 journal articles included in the final systematic review.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

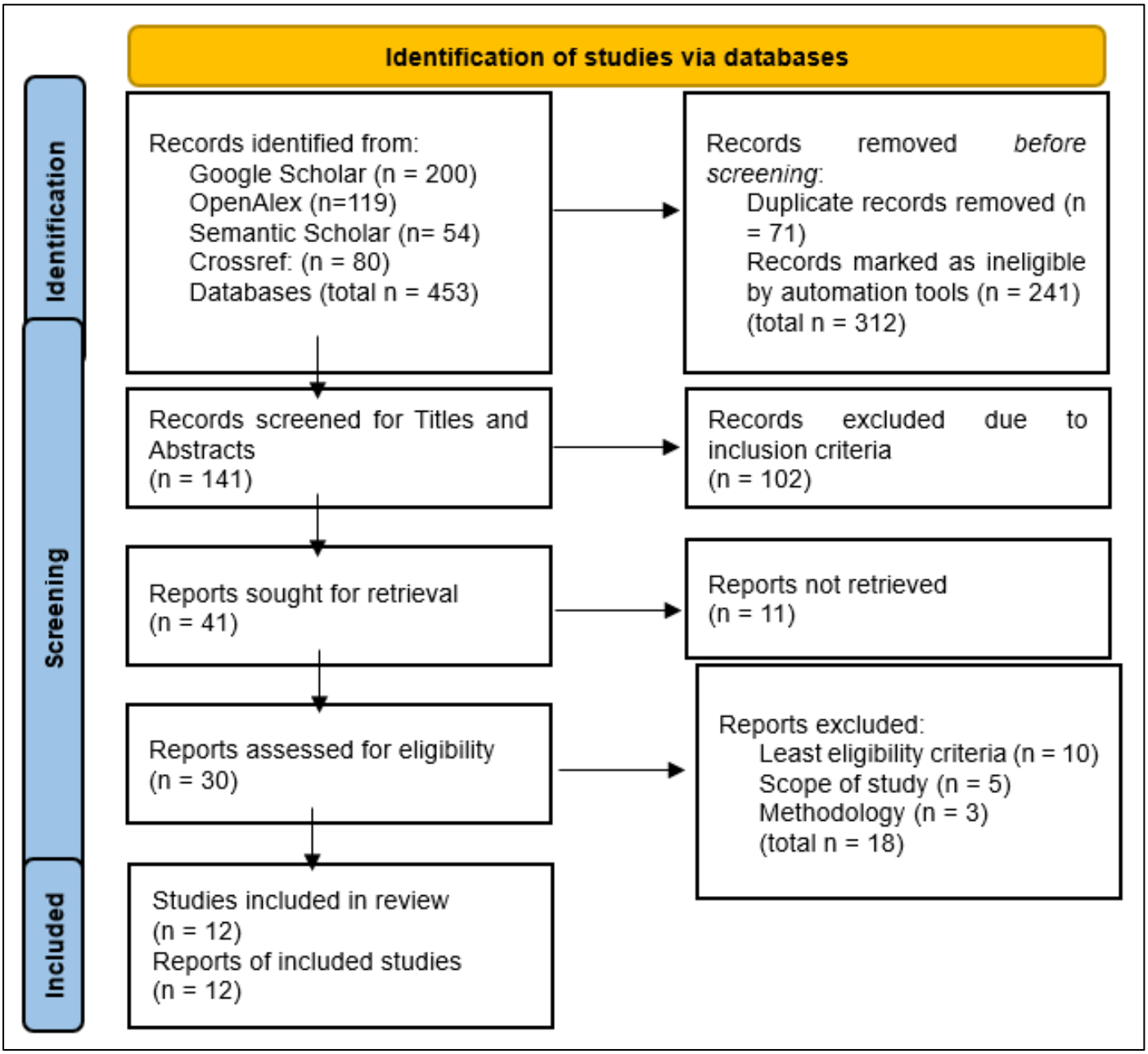

Fig 1 PRISMA Flow Chart
Source: Page et al., 2021

➢ *Data Analysis*

The study adopted an inductive qualitative approach to analyse the information obtained through the systematic review process. The reporting of the review was guided by the PRISMA 2020 framework, which supports transparency and standardisation in systematic evidence synthesis (Page et al., 2021). Due to the potential for conflicting interpretations across studies, thematic analysis was fully adopted, allowing for the identification of recurring themes relevant to the research focus (Khedkar, 2014). (Page et al., 2021) presented the PRISMA 2020 checklist in their work. In this review, Items 9, 10, 13, 19, and 23 were applied to support the thematic synthesis of qualitative data. Specifically, data were extracted as key quotes, conceptual themes, and applied frameworks (Items 9–10), then systematically coded and grouped using thematic synthesis (Item 13), with results presented narratively and in table to illustrate theme development (Item 19). The findings were further interpreted in relation to their practical significance, while also reflecting on the strengths and limitations of the synthesis process (Item 23). This approach aimed to reduce bias, strengthen the interpretation of findings, and integrate the evidence from the included studies to derive an effective method for implementing Zero Trust and cloud security frameworks within the IT audit functions of modern organisations, based on shared best practices.

- *Thematic Analysis*

Thematic analysis allows the authors to synthesise the results from all included papers, thereby reducing author bias and increasing the study's validity by identifying recurring patterns across the literature (Brooks et al., 2015) This

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

analytical approach was employed to verify the reliability and credibility of the findings by examining their consistency across time and contextual variations, which were subsequently classified into themes. (Brooks et al., 2015) define a theme as a cluster of linked categories conveying similar meaning, emerging through an inductive analytical process and characterising a qualitative research paradigm.

The authors also employed the Grading of Recommendations Assessment, Development, and Evaluation (GRADE) framework, which classifies evidence as high, moderate, low, or very low, as outlined by (Brignardello-Petersen et al., 2024) to appraise the strength of the findings from the included literature.

- *Thematic Analysis Process*

✓ *Familiarisation and Initial Interpretation*

The researcher engaged in repeated reading of the included studies to identify early themes *(Bee et al., 2015; Cree et al., 2015)*. Guiding prompts, such as "What challenge or practice is being described?" and "How does this relate to IT audit, Zero Trust, or cloud security frameworks?", were used to support systematic interpretation.

✓ *Comparative and Selective Coding*

Codes were continuously compared across studies to refine the framework. Selective coding ensured that final themes were grounded in the data and represented core concepts related to IT audit, Zero Trust, and cloud security (Brooks et al., 2015; Coker, 2021; Cree et al., 2015)

✓ *Narrative Synthesis and Visualisation*

Themes were synthesised narratively and illustrated with visual charts to communicate key findings. This ensured that interpretations remained data-driven and applicable across varied organisational contexts ((Nicholson et al., 2016).

✓ *Reflexivity, Audit Trail, and Trustworthiness*

Analytic decisions and interpretations were documented through reflexive memos. Trustworthiness was reinforced through transparency, acknowledgment of limitations, and attention to alternative interpretations (Bee et al., 2015; Cree et al., 2015)

➢ *Data Extraction and Synthesis*

The data from the included papers were extracted systematically, capturing relevant information as shown in Table 3 below. This information includes: the author(s)' names, year, and location (country), research aim, research design and methodology, type of organizational infrastructure, and key findings. The extracted information was further reviewed to assess arguments related to adoption, outcomes, and challenges. This synthesis was conducted to develop a unified strategy that addresses the research question.

Table 3 Data Extraction and Synthesis

Author(s) name, year, and place	Key Aim(s)	Research Design	Research Methodology	Infrastructure Type	Key Findings
Yeoh et al. (2023) Deakin University, Geelong, Victoria, Australia	To develop a maturity framework and identify critical success factors for effective Zero Trust implementation	Delphi Study	Qualitative method	On-premises and Cloud architecture	Zero Trust implementation requires a structured approach guided by critical success factors and maturity models, highlighting the need for IT audit functions to adapt to continuous verification and dynamic access controls
Muralidhara & Janardhan (2016), University of Southern California, Los Angeles, USA	To propose Zero Trust as a security model for multi-cloud environments and outline its key implementation components	Conceptual/ Narrative Review	Qualitative (Theoretical) method	Multi-Cloud architecture	Zero Trust is the optimal model for securing multi-cloud environments, where IT audits must assess interoperability, access governance, and the effectiveness of identity and policy enforcement mechanisms.
Ajani et al. (2024), Ramdeobaba University (RBU), Nagpur, India	To design Zero Trust models for distributed cloud systems and explore identity-based security and real-time access controls	Technical/Analytical study	Quantitative / Mixed method	Hybrid and multi-cloud	Implementing Zero Trust in hybrid and multi-cloud infrastructures demands identity-based models, behavioural analytics, and audit functions capable of evaluating real-time, algorithm-driven access decisions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

Adanigbo et al (2024), Delaware, USA	The study aims to review Zero Trust literature and propose a framework for securing multi-cloud microservices environments	Architectural Synthesis	Qualitative	Multi-Cloud Microservices	The study proposes a Zero Trust framework to address fragmented security in multi-cloud microservices by integrating identity management, continuous verification, and service segmentation.
Manne (2023), Eden Prairie, Minnesota, USA	The aim is to explore how Zero Trust can be implemented in multi-cloud setups and address related security challenges	Analytical/Descriptive Review	Qualitative	Multi-Cloud	Zero Trust enhances multi-cloud security by reducing attack surfaces and recommends standardization and automation to address interoperability issues.
Damaraju (2022), L. D. College of Engineering Ahmedabad, India	This study aims to assess the effectiveness of Zero Trust in cloud environments through survey data and expert interviews	Comparative Review	Mixed Method	Cloud (General cloud framework)	Organizations with full Zero Trust implementation report significantly fewer security incidents, driven by maturity, leadership, and collaboration.
Nzeako & Shittu (2024), Finland (Independent) & Greensboro, NC, USA (University of North Carolina)	To explore the implementation of Zero Trust Security in cloud environments by presenting a practical framework, identifying challenges, and discussing potential benefits	Theoretical Framework Study	Qualitative	Multi-Cloud	Zero Trust enhances cloud security by enforcing continuous access verification, micro-segmentation, and least privilege principles.
Sarkar, Choudhary, Shandilya, Hussain, & Kim (2022), Bhopal, India (VIT); Lyngby, Denmark (DTU); Cheonan, South Korea (SMU	To compare and evaluate the features of existing Zero Trust models for cloud computing, and to guide organizations in adopting effective security frameworks.	Comparative Review	Qualitative	Hybrid-Cloud	Zero Trust improves security by mitigating internal and external threats, enhancing visibility, and enabling automated trust evaluation in cloud networks
Dommari & Khan (2023), Hosur, Tamil Nadu (Adhiyamaan College) & Uttarakhand (MAHGU), India	To identify implementation challenges in cloud-native Zero Trust adoption and propose best practices for scalable, secure integration in modern IT environments	Narrative Review	Qualitative	Cloud-Native environment (microservices, DevOps)	Successful Zero Trust in cloud-native environments requires solving scalability and integration issues using best practices like IAM, micro-segmentation, and automation.
Sharma (2022), Santa Clara, California, USA (Netskope Inc.)	To analyse how Zero Trust Architecture enhances cloud security and to provide practical recommendations for organizations planning to adopt it.	Applied Conceptual Study	Qualitative	Hybrid & multi-cloud	Zero Trust minimizes cloud attack surfaces and improves compliance through strong identity verification, segmentation, and real-time monitoring
Johnny (2019), Manchester, UK	To examine how Zero Trust Architecture can be strategically	Conceptual Analysis	Mixed Methods	Hybrid Cloud	Zero Trust provides a strategic framework for hybrid cloud security by

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

(University of Manchester)	implemented in hybrid cloud environments to improve security and support digital transformation				ensuring continuous authentication and reducing risks across cloud and on-premises systems.
Pochu, Nersu, & Kathram (2024, India, DevOps teams using Google Cloud Platform)	To explore how Zero Trust can be implemented in DevOps-driven cloud environments	Conceptual Study	Qualitative	Cloud-based (GCP DevOps)	Zero Trust integration in DevOps enhances cloud security through continuous verification and automation.

III. FINDINGS

A. Introduction

This section presents results from the systematic review of the included studies.

B. Results from Systematic Review Using Themes

Thematic analysis was adopted for the systematic review to synthesize results from the included studies. A total of twelve (12) studies were included, and 4 themes were identified.

➢ *Theme One: Organisational and Technical Challenges*

Theme one captures the organisational and technical challenges in modern organizations for the effective implementation of Zero Trust and Cloud Security in IT audit functions. It includes the complexity of cloud integration, lack of centralized visibility, compliance burdens, high implementation costs, and resistance to change. Eleven of the included studies support the existence of these challenges (Ajani, 2024; Ashish & Manne, 2023; Damaraju, 2022a; Godwin Nzeako & Rahman Akorede Shittu, 2024; Muralidhara & Janardhan, 2016a; Sarkar et al., 2022; Segun Adanigbo et al., 2024; Sharma, 2022)

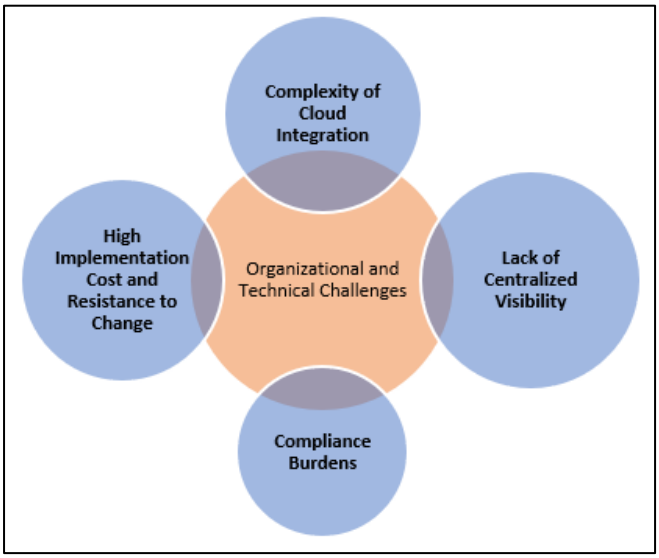

Fig 2 Organizational and Technical Challenges
Source: Author's Compilation

- *Complexity of Cloud Integration*

Muralidhara and Janardhan (2016) noted that deploying Zero Trust across multi-cloud environments is hindered by incompatible interfaces and vendor-specific configurations, while Ajani et al. (2024) highlighted architectural inconsistencies in hybrid systems that obstruct seamless policy enforcement. Adanigbo et al. (2024) and Manne (2023) further pointed to platform heterogeneity, fragmented governance, and the need for abstraction layers, which aligned with Dommari and Khan (2023), who emphasized the challenge of applying Zero Trust in distributed, container-based systems. Similarly, Nzeako and Shittu (2024) explained that the lack of static perimeters in cloud architectures makes it difficult to implement traditional access controls within a Zero Trust model.

- *Lack of Centralised Visibility*

Ajani et al. (2024) reported that decentralised monitoring in cloud infrastructures creates blind spots in real-time access auditing—an essential requirement in Zero Trust. Adanigbo et al. (2024) and Manne (2023) emphasized that inconsistent logging and fragmented security tools across cloud platforms prevent unified monitoring. Sharma (2022) added that visibility across hybrid and multi-cloud systems is limited, and Sarkar et al. (2022) reinforced that lack of visibility hinders policy enforcement and real-time threat detection.

- *Compliance Burden*

Muralidhara and Janardhan (2016) observed that aligning Zero Trust controls with regulatory frameworks like GDPR and HIPAA is difficult without centralized policy orchestration. Manne (2023) and Damaraju (2022) noted that maintaining compliance across multi-cloud platforms requires ongoing audits and standardized controls mapped to global regulations such as ISO 27001. Johnny (2019) emphasized the complexity of managing overlapping jurisdictional requirements in hybrid environments, while Sharma (2022) pointed out that Zero Trust's reliance on continuous monitoring increases the overall compliance workload.

- *High Implementation Cost and Resistance to Change*

Ajani et al. (2024), Muralidhara and Janardhan (2016), and Nzeako and Shittu (2024) acknowledged that implementing Zero Trust requires major investment in infrastructure upgrades and personnel training. Segun et al. (2024) added that integration costs rise in multi-cloud setups due to the need for interoperable controls. Johnny (2019) pointed out that organizations with legacy systems face greater costs and slower transitions, while Damaraju (2022)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

emphasized that staff resistance and lack of leadership buy-in can stall Zero Trust initiatives without targeted change management.

➢ *Theme Two: Core Implementation Strategies*

The Implementation strategies for Zero Trust and Cloud Security in IT audit function are listed and explained in Theme Two. With Eleven of the included studies agreeing to the items listed under the strategy (Ajani, 2024; Damaraju, 2022b; Dommari & Khan, 2023; Johnny, n.d.; Manne, 2023; Muralidhara & Janardhan, 2016b; Pochu et al., 2024; Sarkar et al., 2022; Segun et al., 2024; Sharma, 2022b; Yeoh et al., 2023)

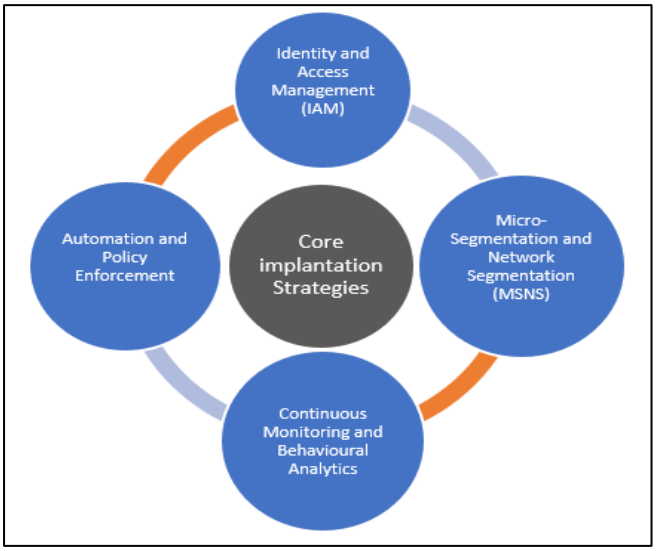

Fig 3 Core Implementation Strategies
Source: Authors Compilation

- *Identity and Access Management (IAM)*

Yeoh et al. (2023) described IAM as the foundation of Zero Trust, highlighting tools like Multi-Factor Authentication (MFA), which requires users to verify their identity using multiple methods (e.g., password and a mobile code), and Single Sign-On (SSO), which allows users to access multiple systems with one login—both of which reduce the risk of unauthorized access. Sharma (2022) and Dommari and Khan (2023) emphasized IAM for enforcing user verification across cloud systems. Ajani *et al.* (2024), Pochu *et al.* (2024), and Muralidhara and Janardhan (2016) echoed its importance, while Segun *et al.* (2024), Manne (2023), and Damaraju (2022) highlighted federated identity protocols like SAML (Security Assertion Markup Language) and OIDC (OpenID Connect) as crucial for ensuring secure, interoperable authentication across cloud services.

- *Micro-Segmentation and Network Segmentation (MSNS)*

Ajani *et al.* (2024), Yeoh *et al.* (2023), and Sharma (2022) supported micro-segmentation—a practice of dividing networks into smaller, isolated zones—so that access can be tightly controlled and limited to only what is necessary for each user or workload. Sarkar *et al.* (2022) emphasized segmentation as a method to limit lateral movement during breaches. While Muralidhara and Janardhan (2016) discussed traditional segmentation, Adanigbo *et al.* (2024), Manne (2023), and Damaraju (2022) expanded the discussion by referencing Software-Defined Networking (SDN) and service mesh architectures, which dynamically enforce Zero Trust boundaries across containerized environments.

- *Continuous Monitoring and Behavioural Analytics*

Pochu *et al.* (2024), Ajani *et al.* (2024), and Sharma (2022) emphasized the use of Security Information and Event Management (SIEM) systems and User and Entity Behaviour Analytics (UEBA) to detect anomalies in real time by analyzing deviations from normal user behavior. Dommari and Khan (2023) added that Zero Trust requires continuous monitoring to verify identities dynamically in cloud-native environments. Adanigbo *et al.* (2024), Manne (2023), and Damaraju (2022) reinforced the role of telemetry, behavioral analytics, and artificial intelligence (AI) in supporting adaptive access control and early threat detection.

- *Automation and Policy Enforcement*

Pochu *et al.* (2024), Dommari and Khan (2023), and Johnny (2019) stressed automation through Policy-as-Code—an approach where security rules are written as code and stored in version-controlled repositories, enabling consistent, auditable enforcement. Ajani et al. (2024) supported automation but placed less focus on audit integration. Adanigbo *et al.* (2024), Manne (2023), and Damaraju (2022) emphasized centralized policy engines and dynamic controls, which allow organizations to automatically enforce access policies in response to context, reducing human error and administrative overhead.

➢ *Theme Three: Interoperability and Standardisation*

Interoperability and standardization refer to implementing Zero Trust consistently across diverse cloud environments under unified security policies. The included studies support the key items under this theme.

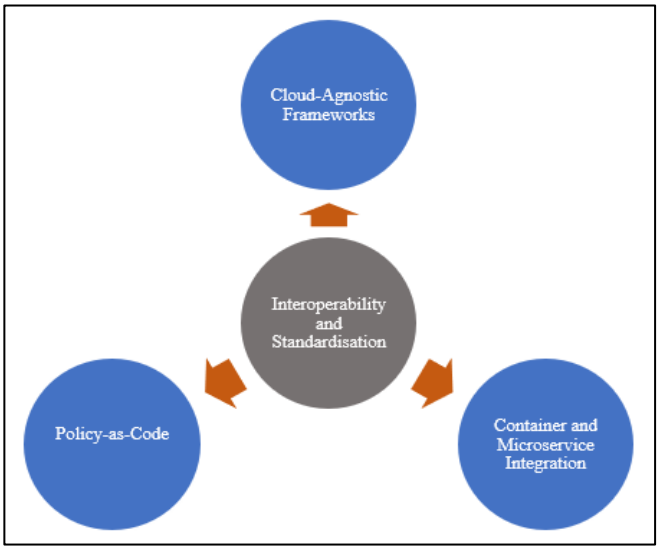

Fig 4 Interoperability and Standardization Strategies
Source: Authors Compilation

- *Cloud-Agnostic Frameworks*

Sarkar *et al.* (2022) and Sharma (2022) recommended using cloud-agnostic Zero Trust frameworks that are not tied

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

to any specific vendor, allowing consistent policy enforcement across hybrid and multi-cloud environments. Ajani *et al*. (2024) and Adanigbo *et al*. (2024) agreed, noting that vendor-neutral models reduce integration friction and improve consistency when organizations span multiple cloud providers.

- *Policy-as-Code*

Dommari and Khan (2023), Pochu *et al.* (2024), and Adanigbo *et al*. (2024) described Policy-as-Code as essential for automation, enabling policy versioning, peer review, and standardized deployment. Manne (2023) and Damaraju (2022) reinforced its importance, stating that expressing access rules as code increases transparency, simplifies auditing, and allows security policies to scale alongside infrastructure.

- *Container and Microservice Integration*

Dommari and Khan (2023) detailed how Zero Trust can be enforced within container orchestration platforms like Kubernetes, using workload identity, service mesh proxies, and runtime controls. Sharma (2022) added that Zero Trust should extend to inter-container communications, preventing unauthorized east-west traffic. Adanigbo *et al*. (2024), Manne (2023), and Damaraju (2022) also acknowledged the need for service-level enforcement in microservice environments to maintain trust boundaries between dynamic workloads.

➢ *Theme Four: Suggested Practices*

Implementing Zero Trust Architecture requires a phased and strategically guided approach that aligns with organizational context and operational needs. Johnny (2019) outlined a step-by-step design for hybrid environments, highlighting the importance of aligning security controls with business objectives and audit processes. Sharma (2022) proposed a strategic combination of identity management, automation, segmentation, and compliance integration to support both operational and regulatory outcomes. Sarkar *et al.* (2022) recommended adapting Zero Trust models based on organizational maturity and infrastructure type. Manne (2023) and Damaraju (2022) supported these perspectives by advocating progressive implementation, executive support, and the prioritization of high-risk areas to promote long-term adoption within existing governance structures.

C. Summary of Findings

The findings show that implementing Zero Trust in cloud environments is hindered by integration complexity, lack of visibility, compliance burdens, and high costs. Authors consistently emphasize Identity and Access Management using MFA, SSO, and federated protocols, along with micro-segmentation to limit lateral movement. Continuous monitoring with SIEM and behavioral analytics, and automation via Policy-as-Code, are critical for enforcement. Cloud-agnostic frameworks and container-level controls support interoperability. Strategic adoption requires phased deployment, executive support, and alignment with compliance goals, highlighting the need for both technical readiness and organizational commitment to achieve effective Zero Trust implementation

IV. DISCUSSIONS

➢ *Objective One*

The findings reveal several challenges limiting the application of IT audit functions in implementing Zero Trust across cloud environments. A key issue is the complexity of integration in hybrid and multi-cloud systems, with Muralidhara and Janardhan (2016), Ajani *et al*. (2024), and Adanigbo et al. (2024) identifying incompatible interfaces, vendor-specific configurations, and architectural inconsistencies. Manne (2023) and Dommari and Khan (2023) noted further complications due to platform heterogeneity, fragmented governance, and container-based systems, while Nzeako and Shittu (2024) emphasized the difficulty of enforcing access controls without static perimeters. Decentralized monitoring also emerged as a concern, with Ajani et al. (2024), Adanigbo *et al.* (2024), and Manne (2023) reporting inconsistent logging and fragmented tools, and Sharma (2022) and Sarkar *et al.* (2022) highlighting reduced audit capacity due to limited oversight. Compliance burdens and organizational resistance compound these challenges; aligning Zero Trust with regulatory frameworks such as GDPR and HIPAA remains difficult without centralized control (Muralidhara & Janardhan, 2016; Manne, 2023; Damaraju, 2022). Additional barriers include high infrastructure costs, the presence of legacy systems, limited training, and leadership support (Ajani *et al*., 2024; Nzeako & Shittu, 2024; Johnny, 2019). These findings underscore the need for frameworks that address technical, regulatory, and organizational constraints.

➢ *Objective Two*

The findings indicate that effective IT audit functions in Zero Trust environments depend on robust identity and access control mechanisms. Identity and Access Management (IAM) emerged as central, with Yeoh *et al.* (2023), Sharma (2022), and Dommari and Khan (2023) emphasizing the role of Multi-Factor Authentication (MFA), Single Sign-On (SSO), and verified access across distributed systems. Adanigbo e*t al*. (2024), Manne (2023), and Damaraju (2022) highlighted federated protocols like SAML and OIDC as essential for securing and auditing identity across cloud platforms. Additional practices supporting audit functions include micro-segmentation, continuous monitoring, and policy automation. Ajani *et al.* (2024), Yeoh *et al.* (2023), and Sharma (2022) noted that micro-segmentation limits lateral movement and enforces defined access zones. Continuous monitoring tools such as SIEM and UEBA (Pochu *et al.,* 2024; Sharma, 2022) aid anomaly detection. Finally, policy automation through Policy-as-Code (Dommari & Khan, 2023; Pochu *et al.,* 2024) enhances audit consistency and reduces human error.

➢ *Objective Three*

The findings support a framework that addresses key barriers—such as integration complexity, limited visibility, compliance burden, and cost—in hybrid and multi-cloud environments (Muralidhara & Janardhan, 2016; Ajani *et al.,* 2024; Sharma, 2022; Johnny, 2019). To mitigate these, it should include centralized policy management, continuous monitoring, and platform standardization (Manne, 2023;

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct056

Damaraju, 2022; Sarkar *et al.,* 2022). Core functions like IAM (MFA, SSO, federated protocols), micro-segmentation, SIEM/UEBA tools, and Policy-as-Code enhance audit traceability and control (Yeoh *et al*., 2023; Pochu *et al.,* 2024; Dommari & Khan, 2023; Adanigbo et al., 2024). Cloud-agnostic designs and phased strategies support broader implementation.

V. STRENGTHS AND LIMITATIONS OF INCLUDED STUDIES

The included papers present a provide valuable insights into Zero Trust and cloud security, consistently highlighting core practices such as identity management, network segmentation, continuous monitoring, and policy automation. While the frameworks proposed align well with IT audit functions, they are largely conceptual, with minimal empirical validation. Common challenges, including integration complexity, interoperability, and organisational resistance, are acknowledged but not addressed through tested solutions. This limits the generalizability and practical depth of their proposed approaches.

VI. CONCLUSIONS

This systematic review explored how IT audit functions can be modernised to support Zero Trust and cloud security in contemporary organisations. Findings show that implementation is challenged by technical complexity, compliance demands, limited visibility, and high costs—especially in hybrid and multi-cloud environments. However, consistent strategies were identified across the studies. These include identity and access management using Single Sign-On, Multi-Factor Authentication, and federated identity protocols; micro-segmentation for network security; continuous monitoring through SIEM and UEBA; and policy automation using Policy as Code. Cloud-agnostic designs and phased deployment approaches enhance adaptability and audit alignment. While most included studies are conceptual, they collectively emphasise the need for integrated and security-focused audit practices. This review provides a strong foundation for developing resilient IT audit frameworks across varied infrastructures. Future research should empirically validate proposed frameworks and address practical implementation challenges.

REFERENCES

[1]. Ajani, S. N. (2024). Cloud Security: Implementing Zero Trust Architecture in Distributed Environments. Computer Fraud and Security, 176–184. https://doi.org/10.52710/cfs.75

[2]. Aldossary, S., & Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. International Journal of Advanced Computer Science and Applications, 7(4). https://doi.org/https://dx.doi.org/10.14569/ijacsa.2016.070464

[3]. Aljohani, A. (2023). Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks. Shifra. https://peninsula-press.ae/Journals/index.php/SHIFRA/article/view/35

[4]. Ashish, T., & Manne, K. (2023). Implementing Zero Trust Architecture in Multi-Cloud Environments. In International Journal of Computing and Engineering (Vol. 4, Issue 3). www.carijournals.orgwww.carijournals.orgwww.carijournals.org

[5]. Bee, P., Brooks, H., Fraser, C., & Lovell, K. (2015). Professional perspectives on service user and carer involvement in mental health care planning: A qualitative study. International Journal of Nursing Studies, 52(12), 1834–1845. https://doi.org/10.1016/j.ijnurstu.2015.07.008

[6]. Bell, C., Broklyn, P., & Egon, A. (2024). ZERO-TRUST SECURITY MODEL FOR ENHANCED CLOUD SECURITY AND DATA PRIVACY. SSRN Electronic Journal. https://doi.org/https://doi.org/10.2139/ssrn.4904958

[7]. Brignardello-Petersen, R., Santesso, N., & Guyatt, G. H. (2024). Systematic reviews of the literature: an introduction to current methods. American Journal of Epidemiology. https://doi.org/10.1093/aje/kwae232

[8]. Brooks, H., Sanders, C., Lovell, K., Fraser, C., & Rogers, A. (2015). Re-inventing care planning in mental health: Stakeholder accounts of the imagined implementation of a user/carer involved intervention. BMC Health Services Research, 15(1), 1–12. https://doi.org/10.1186/s12913-015-1154-z

[9]. Coker, D. C. (2021). Making Thematic Analysis Systematic: The Seven Deadly Sins. Journal of Studies in Education, 11(3), 126. https://doi.org/10.5296/jse.v11i3.18882

[10]. Cree, L., Brooks, H. L., Berzins, K., Fraser, C., Lovell, K., & Bee, P. (2015). Carers' experiences of involvement in care planning: A qualitative exploration of the facilitators and barriers to engagement with mental health services. BMC Psychiatry, 15(1), 1–11. https://doi.org/10.1186/s12888-015-0590-y

[11]. Damaraju, A. (2022a). Integrating Zero Trust with Cloud Security: A Comprehensive Approach. Journal Environmental Sciences And Technology. https://www.researchgate.net/profile/Dash-Karan/publication/388497339_Integrating_Zero_Trust_with_Cloud_Security_A_Comprehensive_Approach/links/679b02c84c479b26c9c1df7a/Integrating-Zero-Trust-with-Cloud-Security-A-Comprehensive-Approach.pdf

[12]. Damaraju, A. (2022b). Integrating Zero Trust with Cloud Security: A Comprehensive Approach. In International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence.

[13]. Dommari, S., & Khan, S. (2023). Implementing Zero Trust Architecture in Cloud-Native Environments: Challenges and Best Practices. In International Journal of All Research Education and Scientific Methods (IJARESM) (Vol. 11, Issue 8). www.ijaresm.com

[14]. Elston, D. M. (2019). Mendeley. In Journal of the American Academy of Dermatology (Vol. 81, Issue 5,

p. 1071). Mosby Inc. https://doi.org/10.1016/j.jaad.2019.06.1291

[15]. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. http://arxiv.org/abs/2309.03582

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

[17]. Harzing, A.-W. (2010). The Publish or Perish Book: Your guide to effective and responsible citation analysis (1st ed.). Tarma Software Reserach Pty Ltd.

[18]. Johnny, R. (n.d.). Implementing Zero Trust for Hybrid Cloud Models: A Strategic Approach to Secure Digital Transformation. https://www.researchgate.net/publication/388105685

[19]. Kahale, L. A., Elkhoury, R., El Mikati, I., Pardo-Hernandez, H., Khamis, A. M., Schünemann, H. J., Haddaway, N. R., & Akl, E. A. (2021). PRISMA flow diagrams for living systematic reviews: a methodological survey and a proposal. F1000Research, 10, 192. https://doi.org/10.12688/f1000research.51723.1

[20]. Khedkar, A. (2014). SYSTEMATIC REVIEW: AN APPROACH FOR TRANSPARENT RESEARCH SYNTHESIS. South American Journal of Clinical Research, 1(2), 121–131.

[21]. Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. Encyclopedia, 4(4), 1520–1533. https://doi.org/10.3390/encyclopedia4040099

[22]. Manne, T. A. K. (2023). Implementing Zero Trust Architecture in Multi-Cloud Environments. International Journal of Computing and Engineering. https://doi.org/10.47941/ijce.2753

[23]. Muralidhara, P., & Janardhan, V. (2016a). Enhancing Cloud Security: Implementing Zero Trust Architectures in Multi-Cloud Environments. International Journal of Scientific Research and Management (IJSRM), 4(9), 4636–4664. https://doi.org/10.18535/ijsrm/v4i9.22

[24]. Nicholson, E., Murphy, T., Larkin, P., Normand, C., & Guerin, S. (2016). Protocol for a thematic synthesis to identify key themes and messages from a palliative care research network. BMC Research Notes, 9(1). https://doi.org/10.1186/s13104-016-2282-1

[25]. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372. https://doi.org/10.1136/bmj.n71

[26]. Pochu, S., Nersu, S. R. K., & Kathram, S. R. (2024). Zero Trust Principles in Cloud Security: A DevOps Perspective. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 6(1), 660–671. https://doi.org/10.60087/jaigs.v6i1.302

[27]. Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & ... (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability. https://www.mdpi.com/2071-1050/14/18/11213

[28]. Segun, Adanigbo O., Iyanu, Adekunle B., Ogbuefi, E., Timothy, Odofin O., Aderemi, Agboola O., & Kisina, D. (2024). Implementing Zero Trust Security in Multi-Cloud Microservices Platforms: A Review and Architectural Framework. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2402–2409. https://doi.org/10.62225/2583049X.2024.4.6.4357

[29]. Sharma, H. (2022). Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security. ESP Journal of Engineering &Technology …. https://www.researchgate.net/profile/Himanshu-Sharma-197/publication/383822594_Zero_Trust_in_the_Cloud_Implementing_Zero_Trust_Architecture_for_Enhanced_Cloud_Security/links/66db35fcfa5e11512ca3b69a/Zero-Trust-in-the-Cloud-Implementing-Zero-Trust-Architecture-for-Enhanced-Cloud-Security.pdf

[30]. Suri, H. (2019). Ethical Considerations of Conducting Systematic Reviews in Educational Research. In Systematic Reviews in Educational Research: Methodology, Perspectives and Application (pp. 41–54). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-27602-7_3

[31]. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

[32]. Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computers &Security. https://www.sciencedirect.com/science/article/pii/S0167404823003223X