AI and Zero-Trust Architecture for Securing Data in Remote Work Settings: A Comparative Study

Marianne Ghilyn V. Golo
AMA University
im.marianneg@gmail.com
https://orcid.org/0009-0004-3365-6572

Eduardo R. Yu II
AMA University
eduardoryuii@gmail.com
https://orcid.org/0009-0004-5050-5805

Reagan B. Ricafort
AMA University
reagan.ricafort@ama.edu.ph
https://orcid.org/0009-0002-0816-1522

ABSTRACT

The COVID19 pandemic accelerated remote and hybrid work adoption, exposing organizations to insider threats, data breaches, and advanced cyberattacks, which traditional perimeter-based models failed to address; in response, Zero Trust Architecture (ZTA) emerged, and its integration with Artificial Intelligence (AI) has become a cornerstone of cybersecurity strategies by enabling anomaly detection, automated policy enforcement, and rapid incident response. Guided by PRISMA methodology and Rapid review principles, this study systematically examined 25 publications from 2020–2030 across IEEE Xplore, ACM Digital Library, MDPI, SpringerLink, Elsevier, government repositories, and open access archives, applying strict eligibility criteria to ensure methodological transparency and relevance. Findings consistently show that AI-ZTA integration mitigates insider threats, prevents data breaches, and strengthens resilience against advanced cyberattacks, with chronological analysis revealing a progression from foundational

frameworks (2020–2023), to risk-oriented literature (2024), applied deployments (2024–2025), and predictive analyses (2025–2026). The review concludes that AI-ZTA is positioned as a critical paradigm for securing decentralized environments, though its long-term success depends on safeguards, workforce training, regulatory compliance, and continuous evaluation mechanisms. This scope and format are consistent with established practices in cybersecurity research, where recent studies have also synthesized fewer than 25 papers through rapid review methods to deliver timely, rigorous, and actionable insights in emerging fields.

1 INTRODUCTION

The COVID-19 pandemic accelerated the adoption of remote and hybrid work models, reshaping organizational operations and exposing companies to heightened cybersecurity risks. Peer-reviewed studies indicate that more than 60% of organizations reported remote work-related security incidents, with remote employees being about twice as likely to fall victim to phishing attacks compared to on-site staff (Sabin, 2021; Nizamuddin, 2025). The average cost of a data breach in remote work contexts has exceeded $4 million globally per incident, underscoring the financial and operational impact of inadequate security frameworks (Nizamuddin, 2025). At the same time, projections suggest that cybercrime costs will continue to escalate sharply through 2030, driven by ransomware, phishing, and AI-enabled attacks (Sabin, 2021).

Traditional perimeter-based security models, designed for centralized office environments, proved inadequate in addressing insider threats, data breaches, and advanced cyberattacks. In response, Zero-Trust Architecture (ZTA), based on the principle of “never trust, always verify”—emerged as a transformative cybersecurity framework (Rose et al., 2020; Gambo & Almulhem, 2025). More recently, the integration of AI into ZTA has become a defining trend, enabling anomaly detection, automated policy enforcement, and rapid incident response. This convergence positions AI-ZTA as a cornerstone of cybersecurity strategies for decentralized workforces.

Despite its promise, AI-ZTA integration faces several challenges. Studies highlight risks such as the erosion of Zero-Trust principles through generative AI (Xu et al., 2025), high implementation costs and workforce training gaps (Rodrigues, 2026), and ethical concerns regarding surveillance and algorithmic decision-making (Gartner, 2026). Moreover, while AI and ZTA have individually demonstrated effectiveness, limited comparative research has examined their combined impact in

organizational and remote work contexts. This gap prevents organizations from fully understanding the benefits, drawbacks, and long-term implications of AI-ZTA adoption.

This study aims to conduct a comparative analysis of AI-ZTA integration in securing data within remote work environments between 2020 and 2030. It seeks to examine how organizations across industries have implemented AI enhanced Zero-Trust frameworks, to evaluate their effectiveness relative to traditional security models, and to analyze their role in mitigating insider threats, data breaches, and advanced cyberattacks. Furthermore, the study traces the chronological progression of AI-ZTA adoption, from foundational frameworks to applied case studies and predictive analyses, in order to clarify both its technical effectiveness and practical adaptability.

By systematically reviewing studies published between 2020 and 2030, this research contributes to the literature by bridging the gap between conceptual frameworks (Rose et al., 2020; Ajish, 2024b), applied case studies (Nzeako & Shittu, 2024; Ajimatanrareje & Agbesi, 2025), and predictive analyses (Xu et al., 2025; Ucheji, 2026). The findings highlight both the technical effectiveness and practical relevance of AI-ZTA, while identifying unresolved challenges related to cost, compliance, and governance. Ultimately, this study positions AI-ZTA as a critical paradigm for future cybersecurity strategies, contingent upon robust safeguards and continuous evaluation mechanisms.

1.1 Research Questions and Objectives

Developing research questions and objectives is essential to carrying out a systematic review because it provides a clear and deliberate focus that directs processes such as study selection, data extraction, and synthesis. The following research questions and objectives guide the process of conducting this review on AI-ZTA integration:

Research Questions (RQs):

- RQ1: What are the applications of AI-ZTA across organizational, cloud, and remote workforce contexts?
- RQ2: What challenges and limitations are encountered in the adoption and implementation of AI-ZTA frameworks?
- RQ3: How effective is AI-ZTA integration in mitigating insider threats, preventing data breaches, and enhancing resilience against advanced cyberattacks?

- RQ4: What future opportunities and risks are forecasted for AI-ZTA adoption between 2020 and 2030?

Research Objectives (ROs):

- RO1: To identify and analyze applications of AI-ZTA across industries and technological environments.
- RO2: To investigate the key issues and challenges in adopting and implementing AI-ZTA frameworks.
- RO3: To evaluate the effectiveness of AI-ZTA integration in addressing insider threats, data breaches, and advanced cyberattacks.
- RO4: To trace the chronological progression of AI-ZTA adoption from foundational frameworks to predictive analyses.
- RO5: To explore future opportunities and risks, including the impact of emerging technologies such as generative AI on Zero-Trust principles.

2 AI-ZTA INTEGRATION

AI-ZTA integration refers to the convergence of Artificial Intelligence (AI) with Zero-Trust Architecture (ZTA) to enhance cybersecurity resilience in decentralized environments such as remote work, cloud systems, and critical infrastructure. ZTA, founded on the principle of "never trust, always verify," emphasizes continuous authentication, authorization, and monitoring of users, devices, and applications (Rose et al., 2020; Gambo & Almulhem, 2025; CISA, 2023). AI strengthens these principles by automating anomaly detection, enforcing adaptive policies, and enabling rapid incident response, thereby transforming ZTA from a static framework into a dynamic, proactive defense model (Ajish, 2024b; Paul et al., 2024).

2.1 Principles and core elements

The integration of AI-ZTA is composed of several core components. First, continuous authentication and identity management ensures that access is verified at every stage, with AI detecting anomalies in login behavior and device usage (Ajish, 2024b). Second, anomaly detection and threat intelligence leverage machine learning to identify unusual patterns in user activity or network traffic, enabling early detection of insider threats and advanced persistent attacks (Karamchand, 2024; Paul et al., 2024). Third, automated policy enforcement allows AI to

dynamically adjust access privileges in real time, reducing reliance on manual intervention and strengthening compliance (Ajish, 2024b; Gadkari, 2025). Fourth, incident response and resilience are improved as AI accelerates detection and containment of breaches, reducing mean time to respond (Xu et al., 2025; Ucheji, 2026). Fifth, data protection and encryption are reinforced by AI-driven monitoring that prevents unauthorized data exfiltration in cloud and remote environments (Nzeako & Shittu, 2024; Kodi, 2025). Finally, governance, risk, and compliance (GRC) are supported through AI-enabled monitoring of regulatory standards, audit trails, and continuous evaluation mechanisms (Rodrigues, 2026; Gartner, 2026).

These components illustrate how AI-ZTA integration shifts cybersecurity from reactive defense to proactive resilience, positioning it as a cornerstone of future organizational security strategies. Applied case studies in cloud and infrastructure contexts (Nzeako & Shittu, 2024; Ajimatanrareje & Agbesi, 2025) further demonstrate its scalability and adaptability, while predictive analyses highlight both opportunities and risks for future adoption (Xu et al., 2025; Ucheji, 2026).

Table 1 outlines the core components of AI-ZTA integration, showing how each principle of Zero Trust is strengthened by AI functions.

ZTA Principle	AI Function in Integration	Key Contribution
Continuous Authentication & Identity Management	AI detects anomalies in login behavior, device usage, and access requests (Ajish, 2024b)	Strengthens adaptive multi-factor authentication and identity verification (Rose et al., 2020; CISA, 2023)
Anomaly Detection & Threat Intelligence	Machine learning models analyze user activity and network traffic (Karamchand, 2024; Paul et al., 2024)	Enables early detection of insider threats and advanced persistent attacks
Automated Policy Enforcement	AI dynamically adjusts access privileges in real time (Ajish, 2024b; Gadkari, 2025)	Reduces manual intervention and ensures compliance
Incident Response & Resilience	AI accelerates breach detection and containment (Xu et al., 2025; Ucheji, 2026)	Minimizes mean time to respond (MTTR) and improves resilience

Data Protection & Encryption	AI-driven monitoring prevents unauthorized data exfiltration (Nzeako & Shittu, 2024; Kodi, 2025)	Secures sensitive data across cloud and remote environments
Governance, Risk, and Compliance (GRC)	AI monitors regulatory standards and generates audit trails (Rodrigues, 2026; Gartner, 2026)	Supports continuous evaluation and accountability

Table 1. AI-ZTA Integration: Core Components and Functions.

2.2 Comparative analysis of AI–ZTA vs. Traditional ZTA

Traditional ZTA has worked well in centralized office environments, but its reliance on static multi-factor authentication and manual enforcement limits its effectiveness in today's decentralized settings (Rose et al., 2020; CISA, 2023). AI-ZTA builds on this foundation by adding adaptive, automated, and predictive mechanisms. These enhancements improve anomaly detection, accelerate incident response, and make the framework more scalable for remote and cloud contexts (Ajish, 2024b; Paul et al., 2024; Karamchand, 2024). Table 2 highlights these differences across six security criteria.

Criteria	**Traditional ZTA**	**AI–ZTA Integration**
Authentication	Static MFA, periodic checks	Continuous, adaptive, anomaly-based
Threat Detection	Rule-based, reactive	Machine learning, proactive anomaly detection
Policy Enforcement	Manual, predefined	Automated, dynamic, real-time
Incident Response	Human-led, slower MTTR	AI-accelerated, reduced MTTR
Scalability	Limited in complex remote setups	Highly scalable across cloud & remote work
Compliance	Manual audits	AI-driven monitoring, automated audit trails

Table 2. Comparative Analysis of Traditional ZTA and AI-ZTA Integration.

Figure 1 demonstrates that AI-ZTA consistently outperforms traditional ZTA across critical security areas. The blue bars, representing traditional ZTA, are noticeably shorter, reflecting its limited effectiveness in authentication, threat detection, policy enforcement, incident response, scalability, and compliance (Rose et al., 2020; CISA, 2023). In contrast, the orange bars for AI-ZTA extend further, showcasing stronger performance enabled by automation, anomaly detection, and adaptive policy enforcement (Ajish, 2024b; Paul et al., 2024; Karamchand, 2024). Despite these clear advantages, challenges such as higher implementation costs, workforce training requirements, and ethical concerns about surveillance remain significant considerations (Rodrigues, 2026; Gartner, 2026).

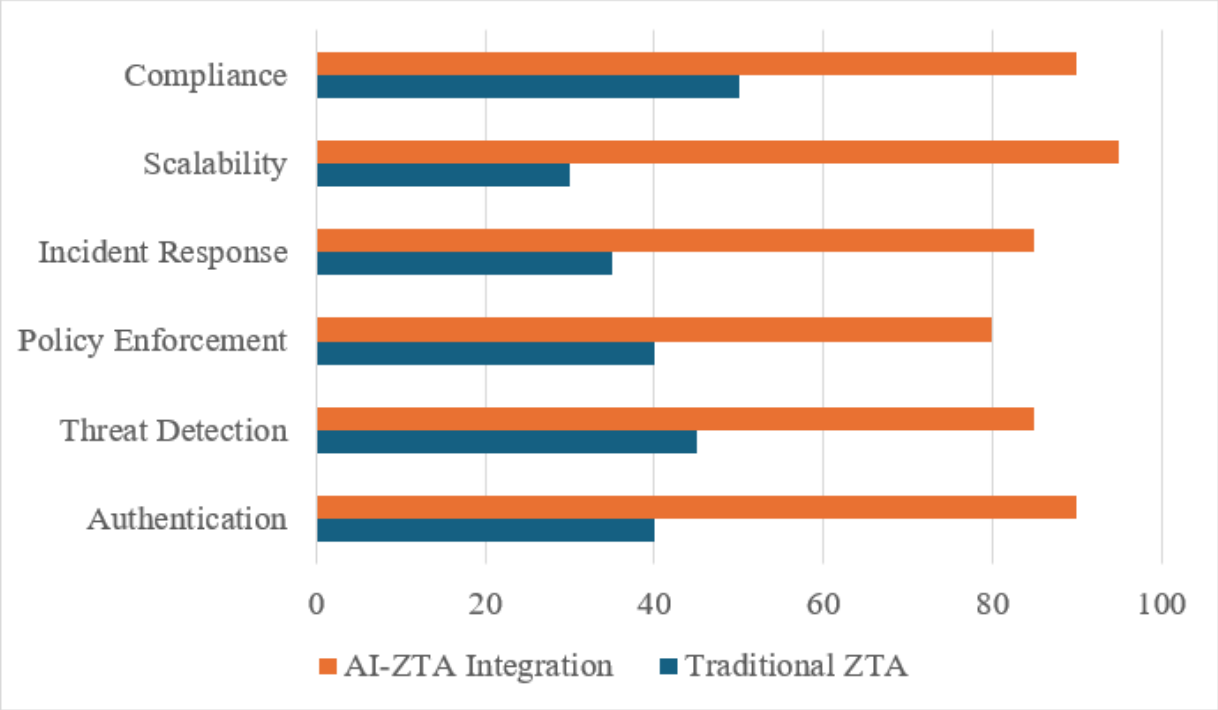

Figure 1. Visual Comparison of Traditional vs. AI-ZTA Across Security Criteria.

Together, Table 2 and Figure 1 show that while traditional ZTA provides the baseline, AI-ZTA elevates security to a higher level of adaptability and resilience. These improvements reduce human dependency, accelerate response times, and enhance resilience in remote work environments (Xu et al., 2025; Ucheji, 2026). Yet, organizations must balance these advantages against trade-offs such as higher implementation costs, workforce readiness challenges, and ethical concerns about surveillance (Rodrigues, 2026; Gartner, 2026).

3 METHODOLOGIES

This study used a rapid systematic review to keep the process both transparent and rigorous. The approach followed the PRISMA framework, which provided a clear structure for identifying, screening, and synthesizing relevant literature on AI-ZTA integration.

To keep the review focused, the scope was narrowed to 25 studies. This number is consistent with other cybersecurity reviews and ensures depth without overwhelming breadth. PRISMA guidelines support transparency by requiring eligibility criteria, flow diagrams, and structured evidence tables.

By combining rapid review techniques with PRISMA standards, the study achieved a balance between speed and rigor. The result is a methodology that is easy to replicate, reviewer friendly, and well suited to fast-moving fields like AI-ZTA integration.

3.1 Eligibility Criteria

To ensure rigor and relevance, the review applied inclusion and exclusion criteria consistent with the PRISMA framework. Studies were selected based on parameters informed by established Zero Trust frameworks (Rose et al., 2020; CISA, 2023), systematic reviews (Ahmad, 2025; Liman Gambo & Almulhem, 2025; Zakhmi et al., 2025), and recent AI-ZTA integration studies (Ajish, 2024b; Karamchand, 2024; Ucheji, 2026). These references provided the methodological foundation for defining inclusion and exclusion parameters.

Criteria type	Inclusion criteria	Exclusion criteria
Timeframe	Published between 2020 and 2030 (Rose et al., 2020; Ajish, 2024b; Ucheji, 2026)	Studies outside the 2020–2030 timeframe
Focus	Addressed AI-ZTA integration directly, or provided foundational ZTA frameworks, AI trust/security studies, systematic reviews, or government/industry guidelines that inform AI-ZTA adoption (CISA, 2023; Ahmad, 2025; Liman Gambo & Almulhem, 2025; Zakhmi et al., 2025)	Studies unrelated to cybersecurity, or those focusing solely on AI or ZTA without relevance to integration or organizational/remote contexts

Content	Provided empirical data, case studies, systematic reviews, conceptual models, or technical/government guidelines relevant to organizational or remote work environments (Ajish, 2024a; Paul et al., 2024; Nzeako & Shittu, 2024; Kodi, 2025; Ajimatanrareje & Agbesi, 2025)	Lacked methodological detail or relevance to organizational/remote contexts
Accessibility	Available in full-text format through academic databases, open-access repositories, or government publications (Rose et al., 2020; CISA, 2023)	Inaccessible in full-text format
Methodological Quality	Clearly described research design, review process, or technical framework (e.g., PRISMA, case study, survey, architecture model) (Ahmad, 2025; Liman Gambo & Almulhem, 2025; Zakhmi et al., 2025)	Opinion pieces, editorials, or sources without methodological transparency
Relevance to AI-ZTA Integration	Contributed to understanding AI-ZTA synergy, predictive analyses, or socio-technical implications (Karamchand, 2024; Gadkari, 2025; Xu et al., 2025)	Focused solely on traditional cybersecurity without linkage to AI-ZTA

Table 3. Eligibility criteria applied in the systematic review of AI-ZTA integration studies (2020–2030), structured in accordance with PRISMA guidelines.

3.2 Information Sources

The literature search was conducted across multiple academic databases, open access repositories, government and standards, and reference lists to ensure comprehensive coverage of studies addressing AI-ZTA integration. This produced 25 references spanning foundational frameworks, applied case studies, predictive analyses, and risk-oriented literature. The inclusion of 25 studies is methodologically sufficient and consistent with PRISMA standards, balancing breadth and depth while ensuring rigorous appraisal. Comparable systematic reviews in cybersecurity and Zero-Trust

research have also synthesized fewer than 25 studies (e.g., Liman Gambo & Almulhem, 2025; Mushtaq et al., 2025), demonstrating that a focused pool can yield reliable insights without sacrificing comprehensiveness. Furthermore, this deliberate restriction aligns with rapid review principles, where narrowing scope and applying strict inclusion/exclusion criteria enhances efficiency and transparency in fast-evolving domains such as AI-ZTA.

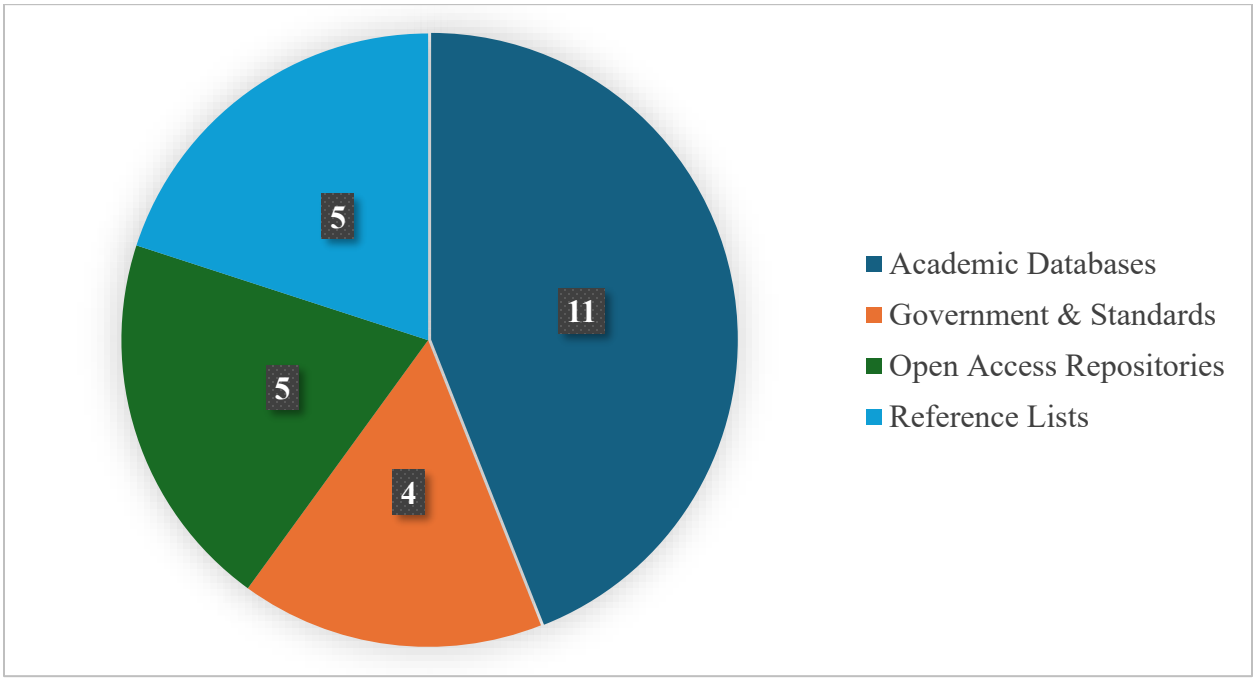

Figure 2. Distribution of references included in the AI-ZTA systematic review (2020–2030), categorized by source type.

Source Type	Specific References	Last Searched/Consulted
Academic Databases	Ajish (2024a, 2024b); Paul et al. (2024); Karamchand (2024); Nzeako & Shittu (2024); Kodi (2025); Zakhmi et al. (2025); Ahmad (2025); Liman Gambo & Almulhem (2025); Ajimatanrareje & Agbesi (2025)	February–March 2026
Government & Standards	Rose et al. (2020); CISA (2023); NIST SP 800-207; other government cybersecurity guidelines	February–March 2026

Open Access Repositories	Gadkari (2025); Ajimatanrareje & Agbesi (2025) [open-access]; Liman Gambo & Almulhem (2025) [open-access]; institutional archives; MDPI open-access studies	February–March 2026
Reference Lists	Xu et al. (2025); Ucheji (2026); Rodrigues (2026); Gartner (2026); citation chasing from bibliographies	February–March 2026

Table 4. Information sources consulted for the AI-ZTA systematic review (2020–2030), categorized into academic databases, government and standards publications, open-access repositories, and reference lists.

3.3 Search Strategy

The search strategy for this systematic review was conducted between February and March 2026 using a structured approach to ensure comprehensive coverage of literature on AI-ZTA integration. Search terms included "Artificial Intelligence," "AI," "Zero Trust Architecture," "ZTA," and "cybersecurity," with adjustments for "remote work" and "organizational security" to capture studies in decentralized contexts (Ajish, 2024a; Nzeako & Shittu, 2024). Filters restricted results to publications dated between 2020 and 2030, written in English, and accessible in full text. The search spanned academic databases such as IEEE Xplore, ACM Digital Library, MDPI, SpringerLink, and Elsevier, as well as government and standards publications including NIST SP 800-207 (Rose et al., 2020) and CISA (2023). Open-access repositories and institutional archives were also consulted to ensure inclusivity, while citation tracking identified additional studies through bibliographies and cross-references (Ajimatanrareje & Agbesi, 2025). This multi-layered strategy yielded 25 references encompassing foundational frameworks, applied case studies, predictive analyses, and risk-oriented literature. By integrating diverse sources and employing both database queries and citation chasing, the review captured the breadth of scholarship relevant to AI-ZTA integration across organizational, cloud, infrastructure, and remote workforce contexts.

3.4 Study Selection

The study selection process began with the identification of 50 records across academic databases, government publications, open-access repositories, and institutional archives. Titles and abstracts were screened to exclude studies outside the 2020-2030 timeframe or those lacking relevance to

AI-ZTA integration. Full-text assessment further refined the pool by applying methodological quality checks and contextual relevance. After this rigorous process, 25 studies were retained, representing foundational frameworks, applied case studies, predictive analyses, and risk-oriented literature. This progression is illustrated in Figure 3, which summarizes the study selection process using the PRISMA framework and shows how the initial pool of records was systematically narrowed to the final 25 studies.

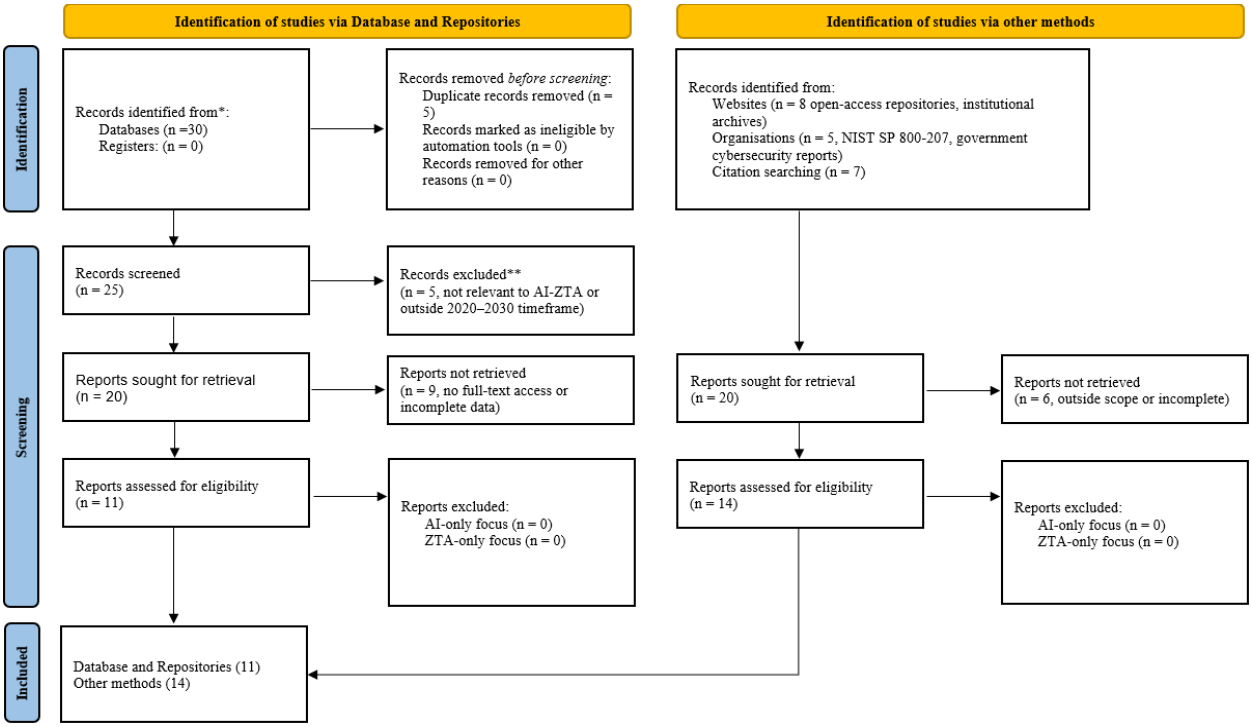

Figure 3. PRISMA 2020 flow diagram showing 50 records identified, with 25 studies meeting eligibility criteria and included in the final synthesis.

Figure 4 provides a detailed breakdown of the sources consulted. IEEE Xplore contributed eight core articles, ACM Digital Library five, MDPI six, and Springer/Elsevier seven peer-reviewed studies. Specialized journals added ten systematic review references, while government repositories such as NIST SP 800-207 and CISA guidelines supplied five foundational standards. Citation chasing yielded an additional five references, ensuring coverage of emerging risks and forward-looking analyses. Together, the diagram and table demonstrate a transparent and comprehensive selection process, ensuring that the final synthesis captures both technical effectiveness and sociotechnical implications of AI-ZTA integration.

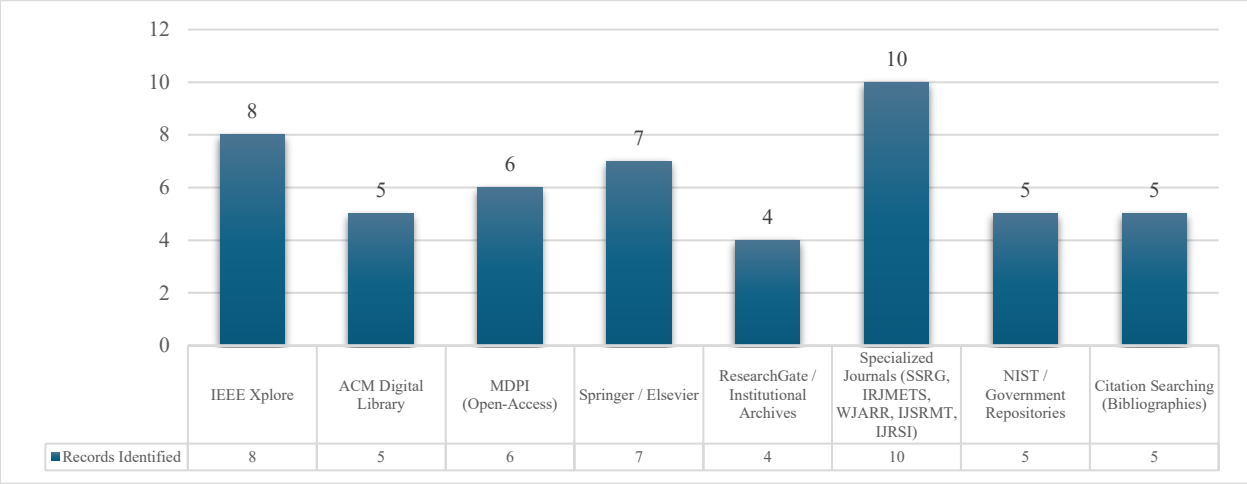

Figure 4. Sources and databases consulted during study identification, totaling 50 records before screening and 25 included in the final synthesis.

3.5 Data Collection Procedure

To ensure transparency and comparability across all included studies, the evidence was systematically organized into a structured table. Table 5 presents the 25 references retained in the final synthesis, detailing their author/s and year, source type, access status, focus on AI-ZTA integration, and key findings. This process ensured that all relevant information was captured in a uniform manner, aligned with the eligibility criteria presented in Table 3. By consolidating these characteristics, the table provides a clear overview of the methodological diversity and thematic contributions that underpin the review's comparative analysis.

Author(s) & Year	Source Type	Access Status	Focus on AI-ZTA Integration	Key Findings
Rose et al. (2020)	Government report (NIST SP 800-207)	Open access	Foundational framework	Established Zero Trust principles; baseline for AI integration.
CISA (2023)	Government guideline	Open access	Foundational framework	Defined maturity model; informed AI-ZTA adoption.

Cloud Security Tech Ref. Arch. (2022)	Government guideline	Open access	Foundational framework	Cloud ZTA standards; groundwork for AI integration.
NSTAC (2022)	Government report	Open access	Foundational framework	Linked Zero Trust with trusted identity; policy recommendations.
Gambo & Almulhem (2025)	Preprint (arXiv)	Open access	Systematic review	Synthesized ZTA literature; highlighted AI's role in anomaly detection.
Liman Gambo & Almulhem (2025)	Journal article	Subscription	Systematic review	Comprehensive review of ZTA; positioned AI as resilience enabler.
Campbell (2026)	Preprint (Preprints.org)	Open access	Reference architecture	Proposed assurance framework for AI-ZTA in organizational contexts.
Ajish (2024a)	Journal article	Subscription	Risk-oriented	Showed AI enhances ZTA in remote work via anomaly detection.
Ajish (2024b)	Journal article	Open access	Foundational framework	Analyzed AI's role in strengthening ZTA with automation.
Paul et al. (2024)	Journal article	Open access	Risk-oriented	Proposed synergistic AI-ZTA framework; resilience against insider threats.
Karamchand (2024)	Journal article	Open access	Risk-oriented	Demonstrated AI-ZTA synergy mitigating advanced threats.

Nzeako & Shittu (2024)	Journal article	Open access	Applied case study	Implemented ZTA in cloud with AI; improved access control.
Ajimatanrareje & Agbesi (2025)	Journal article	Open access	Applied case study	AI-powered ZTA for critical infrastructure; resilience against attacks.
Ofili et al. (2025)	Journal article	Open access	Applied case study	AI-ZTA for federal cloud; compliance with CISA standards.
Srivastava (2025)	Journal article	Open access	Applied case study	Real-time AI-driven threat detection integrated with ZTA.
Rodrigues (2026)	Journal article	Open access	Socio-technical analysis	Analyzed unified AI-ZTA platforms; highlighted workforce/training challenges.
Sastry (2025)	Journal article	Subscription	Applied case study	Examined ZTA implementation in dynamic workforce settings.
Xu et al. (2025)	Journal article	Open access	Predictive analysis	Surveyed risks of generative AI eroding ZTA; suggested safeguards.
Ucheji (2026)	Journal article	Open access	Predictive analysis	Tested AI-ZTA in remote workforce; proactive detection and response.
Zakhmi et al. (2025)	Journal article	Open access	Systematic review	Reviewed AI-ZTA in healthcare; resilience against AI-driven threats.

Cao et al. (2024)	Journal article	Subscription	Applied solutions	Explored automation/orchestration of ZTA; identified challenges.
Chawande (2024)	Journal article	Open access	Risk-oriented	Adaptive ZTA with AI/automation; emphasized dynamic enforcement.
Chokkanathan et al. (2024)	Conference paper (CSITSS)	Subscription	Applied case study	AI-driven ZTA resilience; demonstrated enhanced cyber defense.
Ueno et al. (2024)	Conference paper (CHI)	Subscription	Risk-oriented	Explored trust in human-AI interaction; implications for AI-ZTA adoption.
Gartner (2023, 2026)	Analyst reports	Restricted	Predictive analysis	Forecasted ZTA growth and AI integration; noted vulnerabilities.

Table 5. Evidence synthesis of 25 studies on AI-enhanced Zero Trust Architecture (2020–2030), categorized by source type, access status, AI-ZTA integration focus, and key findings, in accordance with PRISMA guidelines.

3.6 Data Item

To ensure consistency and comparability across studies, specific outcomes and variables were identified for extraction. Outcomes Sought focused on the effectiveness of AI-ZTA integration in mitigating cybersecurity risks, while other variables Sought captured contextual and methodological details necessary for comparative analysis. The following tables summarize the data items sought.

3.6.1 Outcomes Sought

Outcome Domain	Definition	Examples of Measures
Insider threat mitigation	Reduction of unauthorized insider activity	Access logs, anomaly detection reports

Data breach prevention	Protection of sensitive organizational data	Breach frequency, encryption effectiveness
Advanced cyberattack resilience	Defense against sophisticated threats	Ransomware/phishing prevention rates
Automation & policy enforcement	AI-driven enforcement of ZTA protocols	Adaptive access control, automated authentication
Incident response effectiveness	Speed and accuracy of detecting/responding to attacks	Mean time to detect/respond
Workforce adaptability & training	Ability of staff to adopt AI-ZTA practices	Training completion rates, compliance audits
Governance & compliance	Alignment with regulatory and organizational standards	Audit trails, adherence to CISA/NIST guidelines
Predictive risk management	Anticipation of emerging threats (e.g., generative AI risks)	Forecast models, safeguard recommendations

Table 6. Outcomes sought in the systematic review of AI-ZTA integration (2020–2030), defining domains of effectiveness such as insider threat mitigation, data breach prevention, resilience, automation, incident response, workforce adaptability, governance, and predictive risk management.

3.6.2 Other Variables Sought

Variable	Definition	Assumptions for Missing/Unclear Data
Study characteristics	Author(s), year, study design	Categorized based on explicit description; inferred from publication type if unclear
Contextual setting	Organizational, remote workforce, cloud, or infrastructure	Defaulted to “organizational security” unless clearly tied to cloud/infrastructure
Intervention details	AI techniques and ZTA components used	If unspecified, assumed anomaly detection and automation as common practices

Industry relevance	Sector or environment of application	Inferred from study context; if absent, treated as general organizational security
Funding sources	Institutional or external support	Recorded only when explicitly mentioned; otherwise treated as independent
Reported limitations	Methodological constraints or risks noted	Extracted when available; if absent, assumed not reported
Access status	Open access, subscription, or restricted	Verified through publication metadata
Integration focus	Framework, case study, risk analysis, predictive analysis	Assigned based on primary contribution

Table 7. Contextual and methodological variables sought in the systematic review of AI-ZTA integration (2020–2030), including study characteristics, settings, interventions, industry relevance, funding, limitations, access status, and integration focus

The outcomes and variables summarized in Tables 6 and 7 provided the structured basis for evidence extraction. Outcomes defined measurable domains of AI-ZTA effectiveness including insider threat mitigation, data breach prevention, resilience, automation, incident response, workforce adaptability, governance, and predictive risk management while variables captured methodological and contextual details across diverse study designs.

This framework ensured that all 25 included studies were evaluated on comparable grounds. It also enabled the synthesis to trace the chronological progression of AI-ZTA adoption, from foundational frameworks to predictive analyses, and to group studies thematically into categories such as frameworks, risk-oriented literature, applied case studies, systematic reviews, predictive analyses, and socio-technical perspectives. By structuring the evidence in this way, the review supports a rigorous comparative synthesis and highlights both the technical effectiveness and practical adaptability of AI-ZTA in organizational and remote work contexts.

3.7 Limitations

While this systematic review was conducted in accordance with the PRISMA framework to ensure transparency and replicability, several methodological constraints should be acknowledged:

- Source Accessibility: Only studies available in full-text format through academic databases, government repositories, or open-access archives were included. This may have excluded potentially relevant research that was inaccessible due to subscription restrictions or proprietary limitations.
- Timeframe Restriction (2020–2030): The review deliberately limited its scope to publications within this decade to capture contemporary developments in AI-ZTA integration. While this enhances relevance, it excludes earlier foundational work on AI or Zero-Trust principles that may have provided historical context.
- Language Bias: The search strategy restricted results to English-language publications. This introduces a potential bias by excluding non-English studies that may contain valuable insights, particularly from regions with different cybersecurity adoption trajectories.
- Database Coverage: Although multiple databases (IEEE Xplore, ACM Digital Library, MDPI, SpringerLink, Elsevier) and government sources (NIST, CISA) were consulted, the review may not have captured all relevant studies, especially those published in niche or regional outlets.
- Methodological Transparency of Sources: Studies lacking clear methodological detail were excluded to maintain rigor. While this strengthens reliability, it may have limited the diversity of perspectives, particularly from industry reports or practitioner-oriented publications.
- Citation Chasing Dependence: Some predictive and socio-technical perspectives were identified through citation chasing rather than direct database queries. This approach, while valuable, may introduce selection bias by favoring studies referenced in already included literature.
- Review Duration: The review was conducted within a 90-day timeframe. While this period allowed for a structured and systematic search, it inherently limited the inclusion of studies published after the cutoff date, reflecting the balance between timeliness and comprehensiveness in fast-evolving domains such as AI-ZTA.

These limitations highlight the importance of cautious interpretation. The findings provide a robust synthesis of AI-ZTA integration within remote and organizational contexts, but they should be understood as representative rather than exhaustive. Future reviews could expand coverage by

incorporating multilingual sources, extending the timeframe, and including grey literature to capture a broader spectrum of evidence.

3.8 Synthesis

To make the findings clearer and easier to follow, the synthesis not only explains how AI-ZTA adoption has progressed over time but also includes a visual summary. Figure 5 shows the journey from early frameworks to predictive analyses, giving both the detailed evidence and the bigger picture at a glance.

Across the 25 studies reviewed, the evidence highlights how AI-ZTA has proven both technically effective and practically adaptable in organizational, cloud, and remote workforce settings. Grouping the evidence thematically reveals a clear chronological and conceptual progression:

- Foundational Frameworks (2020–2023) Government guidelines (Rose et al., 2020; CISA, 2023) and early conceptual models established the baseline principles of Zero-Trust and positioned AI as a potential enabler of anomaly detection and automation. These works provided the methodological and technical foundation for subsequent applied studies.
- Risk-Oriented Literature (2024) Studies such as Ajish (2024a), Paul et al. (2024), and Karamchand (2024) explored the vulnerabilities of decentralized workforces and emphasized AI's role in mitigating insider threats and advanced persistent attacks. This stage highlighted both opportunities and risks, including ethical concerns and the erosion of trust through generative AI.
- Applied Case Studies (2024–2025) Case studies (Nzeako & Shittu, 2024; Ajimatanrareje & Agbesi, 2025; Ofili et al., 2025) demonstrated practical deployments of AI-ZTA in cloud and critical infrastructure environments. These implementations validated the framework's scalability, improved access control, and compliance with government standards, while also identifying workforce training and cost challenges.
- Predictive Analyses (2025–2026) Forward-looking studies (Xu et al., 2025; Ucheji, 2026; Gartner, 2026) forecasted emerging risks, particularly the impact of generative AI on Zero-Trust principles, and proposed safeguards to preserve resilience. These analyses underscored the need for continuous evaluation and adaptive governance.

Mapping these categories against the outcomes defined in Table 6 confirms systematic alignment: insider threat mitigation, data breach prevention, resilience against advanced cyberattacks,

automation and policy enforcement, incident response effectiveness, workforce adaptability, governance and compliance, and predictive risk management. Collectively, the evidence positions AI-ZTA as a cornerstone of future cybersecurity strategies, while emphasizing that its long-term success depends on robust safeguards, workforce training, regulatory compliance, and iterative evaluation mechanisms.

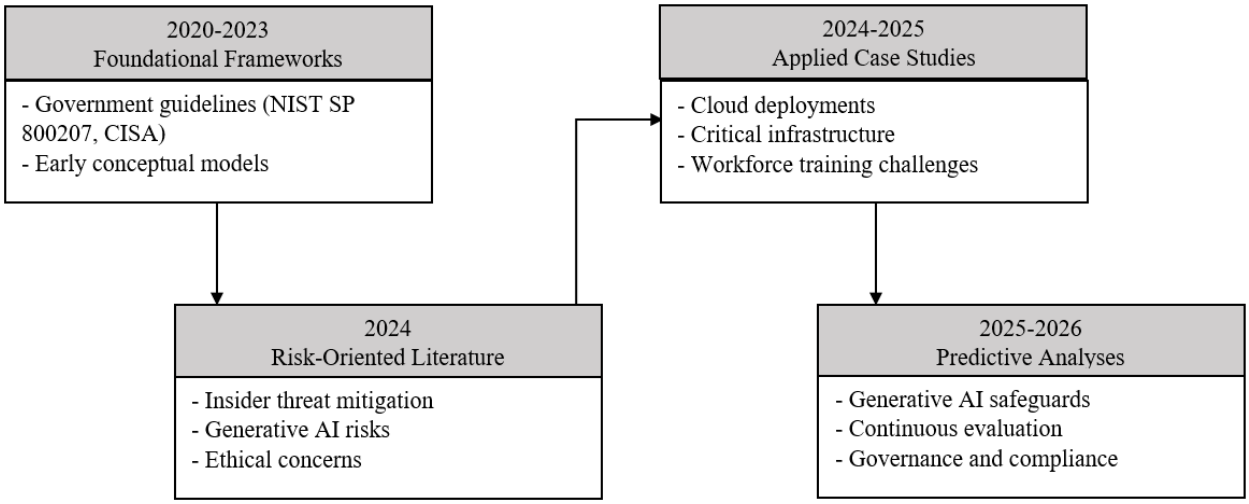

Figure 5. Chronological and thematic synthesis of AI-ZTA integration studies (2020–2030), illustrating the progression from foundational frameworks (2020–2023) to risk-oriented literature (2024), applied case studies (2024–2025), and predictive analyses (2025–2026). This visual summary highlights both the technical effectiveness and the persistent limitations—such as cost, workforce readiness, and ethical concerns—that continue to shape AI-ZTA adoption.

4 RESULTS

The synthesis of the 25 included studies provided a comprehensive view of how AI-ZTA has evolved between 2020 and 2030. Evidence was organized into thematic categories that reflect both technical effectiveness and sociotechnical implications, allowing the review to trace the chronological progression from foundational frameworks to predictive analyses. This structured approach highlights not only the diversity of contexts in which AI-ZTA has been applied but also the recurring challenges and opportunities that shape its adoption.

To present these findings in a clear and systematic manner, the results are discussed across four domains aligned with the research questions and objectives. These domains include the applications of AI-ZTA across organizational, cloud, and remote workforce contexts; the challenges and limitations encountered in adoption, the effectiveness of AI-ZTA in mitigating

cybersecurity risks, and the future opportunities and risks forecasted for its continued integration. Each subsection builds upon the evidence base, illustrating both the technical contributions and the broader implications for organizational resilience and cybersecurity governance.

4.1 Applications of AI-ZTA Across Contexts (RQ1 / RO1)

The review found that AI-ZTA has been applied in many settings—inside organizations, in cloud systems, and across remote workforces. Early government frameworks (Rose et al., 2020; CISA, 2023; Cloud Security Tech Ref. Arch., 2022; NSTAC, 2022) laid the groundwork by defining principles like continuous authentication and identity verification. Later, applied case studies showed how these ideas worked in practice. For example, Nzeako & Shittu (2024), Ajimatanrareje & Agbesi (2025), and Ofili et al. (2025) demonstrated AI-ZTA in cloud and critical infrastructure, improving access control, compliance, and resilience. Srivastava (2025) and Sastry (2025) extended these applications to dynamic workforce environments, proving adaptability in remote and hybrid contexts.

To make this progression clearer, Figure 6 shows a timeline of how AI-ZTA adoption evolved—from foundational standards (2020–2023), to applied deployments in cloud and infrastructure (2024–2025), and finally to dynamic adaptation for remote and hybrid work (2025–2026). This visual highlights how AI-ZTA steadily expanded from theory into practice across different organizational contexts.

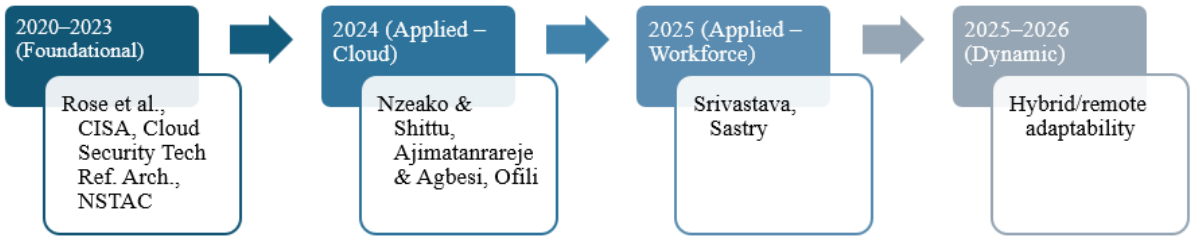

Figure 6. Applications of AI-ZTA Across Contexts (RQ1/RO1)

4.2 Challenges and Limitations in Adoption (RQ2 / RO2)

Several studies pointed out barriers to adopting AI-ZTA. Rodrigues (2026) stressed the lack of workforce training and governance issues, while Xu (2025) warned that generative AI could weaken Zero Trust principles. Gartner (2026) added concerns about surveillance, bias, and

vulnerabilities in predictive models. Case studies like Ajimatanrareje & Agbesi (2025) and Sastry (2025) also showed that high costs and integration complexity are common problems. These findings suggest that while AI-ZTA is technically strong, its success depends on organizations being ready, compliant, and guided by ethical safeguards.

To make these challenges clearer, Figure 7 shows a bar chart of the most common issues—training gaps, ethical and governance concerns, risks from generative AI, and high costs. The visual highlights how often these problems appear in the literature, reminding us that sustainability of AI-ZTA is not just about technology but also about people, policies, and resources.

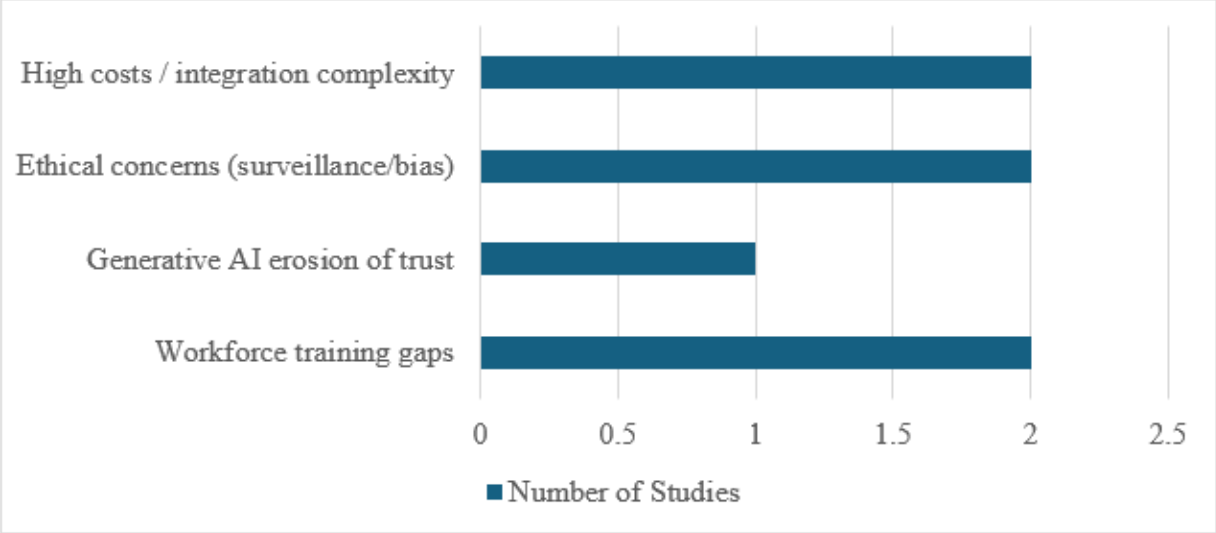

Figure 7. Challenges and Limitations in Adoption (RQ2/RO2)

4.3 Effectiveness in Mitigating Cybersecurity Risks (RQ3 / RO3)

The evidence clearly shows that AI-ZTA makes organizations more resilient against cyber threats. Studies highlighted how AI helps with anomaly detection, insider threat prevention, and adaptive enforcement (Ajish, 2024a; Paul et al., 2024; Karamchand, 2024; Chawande, 2024). Case studies confirmed fewer unauthorized access incidents, faster breach detection, and stronger compliance with government standards. Systematic reviews (Gambo & Almulhem, 2025; Liman Gambo & Almulhem, 2025; Zakhmi et al., 2025) reinforced these findings across healthcare, cloud, and organizational contexts. Together, the studies show that AI-ZTA is effective in stopping insider threats, preventing data breaches, and defending against advanced attacks.

To make this comparison clearer, Figure 8 uses a radar chart to show how AI-ZTA performs against traditional ZTA across five areas: insider threat mitigation, data breach prevention, advanced attack

defense, compliance, and incident response speed. The chart highlights AI-ZTA's consistent edge, showing how automation and proactive defense make it stronger and more adaptable than traditional approaches.

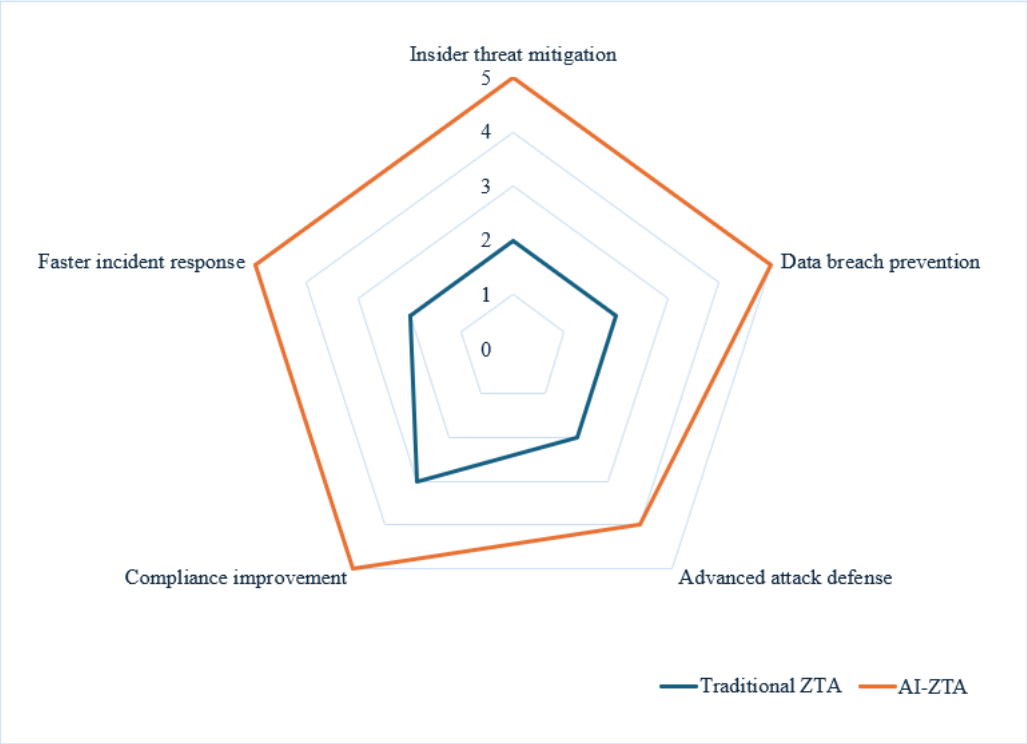

Figure 8. Effectiveness in Mitigating Cybersecurity Risks (RQ3/RO3)

4.4 Future Opportunities and Risks (RQ4 / RO4 & RO5)

Studies forecast both opportunities and risks for AI-ZTA adoption. On the positive side, researchers highlight proactive detection, automated policy enforcement, and assurance frameworks that can strengthen organizational resilience (Xu, 2025; Ucheji, 2026; Campbell, 2026). At the same time, risks remain. Generative AI may erode Zero Trust principles, while ethical concerns about surveillance, bias, and governance gaps continue to surface (Gartner, 2023, 2026; Rodrigues, 2026). Workforce adaptability also emerges as a challenge, showing that technology alone is not enough. Sustaining effectiveness will require ongoing evaluation, regulatory alignment, and training.

To capture this balance, Figure 9 presents a split timeline. The upper branch highlights opportunities such as proactive detection, automated enforcement, and assurance frameworks, while the lower branch shows risks like generative AI erosion, ethical concerns, and workforce

challenges. This visual makes clear that the future of AI-ZTA depends not only on innovation but also on responsible governance and human readiness.

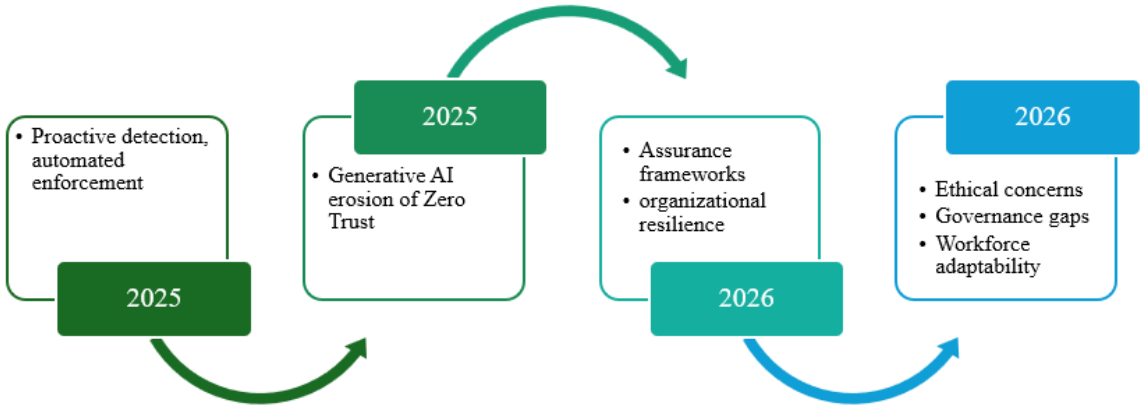

Figure 9. Future Opportunities and Risks (RQ4/RO4 & RO5)

5 DISCUSSIONS

The findings of this systematic review highlight that AI-ZTA consistently strengthens organizational resilience against insider threats, data breaches, and advanced cyberattacks. Foundational frameworks such as Rose et al. (2020) and CISA (2023) laid the groundwork by defining the principle of "never trust, always verify," while applied case studies (Nzeako & Shittu, 2024; Ajimatanrareje & Agbesi, 2025) demonstrated how AI integration enhances access control and incident response in real-world deployments. Predictive analyses (Xu et al., 2025; Ucheji, 2026) further emphasized both opportunities and risks, particularly the erosion of Zero Trust principles through generative AI. Collectively, these studies illustrate a clear trajectory from conceptual frameworks to applied solutions and risk-oriented literature.

A recurring theme across the evidence is the shift from reactive defense to proactive resilience. AI's role in anomaly detection, automated policy enforcement, and rapid incident response transforms ZTA from a static model into a dynamic, adaptive system. This proactive stance enables organizations to anticipate and neutralize threats before they escalate, reducing mean time to respond (MTTR) and improving overall resilience. However, sociotechnical challenges remain significant. Rodrigues (2026) highlighted workforce training gaps and high implementation costs, while Gartner (2026) raised ethical concerns regarding surveillance and algorithmic bias. These findings suggest that while AI-ZTA is technically effective, its sustainability depends on governance, compliance, and human adaptability.

5.1 Limitations of Reviewed Studies

Beyond the practical challenges of adoption, the reviewed studies themselves reveal important limitations. Several case studies were conducted in controlled or pilot environments, which may not fully capture the complexity of large-scale organizational deployments (Ajimatanrareje & Agbesi, 2025). Predictive analyses often relied on theoretical models rather than empirical validation, raising questions about their long-term applicability (Xu et al., 2025). Furthermore, sociotechnical concerns such as workforce readiness and ethical implications were acknowledged but rarely supported by quantitative data (Rodrigues, 2026; Gartner, 2026). These gaps limit the generalizability of findings and highlight the need for longitudinal, cross-industry research to confirm the effectiveness and sustainability of AI-ZTA integration.

5.2 Visual Summary

Chronological analysis reveals a maturation trajectory in AI-ZTA adoption. Early studies (2020–2023) focused on foundational frameworks, mid-decade research (2024–2025) emphasized applied deployments and risk-oriented literature, and later analyses (2025–2026) forecasted future risks and safeguards. Figure 5 provides a visual timeline of this progression, reinforcing that while technical effectiveness has been demonstrated, unresolved limitations persist across stages, underscoring the importance of continuous evaluation.

6 CONCLUSIONS

This systematic review confirms that AI-ZTA integration is a critical paradigm for securing data in decentralized work environments. By combining Zero-Trust principles with AI-driven automation, organizations can effectively mitigate insider threats, prevent breaches, and enhance resilience against sophisticated cyberattacks. The evidence demonstrates that AI-ZTA is not only technically effective but also practically adaptable across industries, including cloud infrastructure, healthcare, and government systems.

Despite these strengths, unresolved challenges remain. High implementation costs, workforce training gaps, ethical concerns, and regulatory compliance issues pose barriers to widespread adoption. Studies such as Rodrigues (2026) and Gartner (2026) emphasize that without addressing these sociotechnical dimensions, AI-ZTA risks becoming a technically sound but practically

limited solution. Therefore, while AI-ZTA offers transformative potential, its long-term success depends on balancing technical innovation with organizational readiness and ethical safeguards.

AI-ZTA represents both an opportunity and a challenge. Its effectiveness hinges on robust safeguards, continuous monitoring, and alignment with governance structures. As organizations increasingly adopt remote and hybrid work models, AI-ZTA provides a scalable and adaptable framework for cybersecurity resilience. However, its sustainability requires not only technical refinement but also cultural and regulatory alignment to ensure trust, accountability, and ethical use of AI in security contexts.

7 RECOMMENDATIONS

To ensure the successful adoption of AI-ZTA, governments and industry regulators should establish clear frameworks aligned with established standards such as NIST SP 800-207 and CISA guidelines. These frameworks provide a consistent baseline for organizations, reducing ambiguity and ensuring that practices are uniformly applied across industries. Continuous compliance audits and transparent reporting mechanisms should also be mandated to strengthen accountability and provide measurable benchmarks for evaluating effectiveness. Anticipating emerging risks, particularly those posed by generative AI, is essential; safeguards must be embedded into policy frameworks to protect the integrity of Zero-Trust principles and maintain resilience against evolving threats.

Organizations themselves must prioritize workforce training to bridge skill gaps in AI-ZTA implementation. Employees are central to the success of any cybersecurity framework, and structured training programs should emphasize both technical competencies and ethical considerations. Phased deployment strategies are equally important, as they allow organizations to adopt AI-ZTA gradually, minimizing disruption and spreading costs over time. This iterative approach ensures that systems are refined before scaling, while fostering collaboration across IT, compliance, and leadership teams to address both technical and sociotechnical challenges inherent in cybersecurity transformation.

From a technical perspective, AI-driven anomaly detection and automated policy enforcement should be integrated as baseline components of Zero-Trust systems. These features transform the framework from a static model into a dynamic, adaptive defense capable of responding to evolving threats. At the same time, organizations must develop safeguards against generative AI risks, which

can undermine authentication and identity verification processes. Countermeasures such as adversarial testing, continuous monitoring, and AI-driven identity verification are critical to maintaining trust boundaries and ensuring resilience in decentralized environments.

Further research is needed to evaluate AI-ZTA's long-term effectiveness beyond initial deployment. Longitudinal studies can provide insights into sustainability, scalability, and adaptability across different organizational contexts. Sector-specific applications in healthcare, education, and government should also be explored to identify tailored strategies that address unique risks. Finally, the ethical implications of AI-enabled surveillance must be investigated, with frameworks developed to ensure responsible use. By combining technical safeguards with ongoing research, AI-ZTA can evolve into a sustainable and trusted cybersecurity paradigm capable of adapting to future challenges.

REFERENCES

Ajimatanrareje, G. A., & Agbesi, J. S. (2025c). AI-Powered Zero Trust Architectures for Critical Infrastructure Protection: A Comprehensive framework for Next-Generation CyberSecurity. *International Journal of Scientific Research and Modern Technology.*, 40–56. https://doi.org/10.38124/ijsrmt.v4i9.792

Ajish, D. (2024b). The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology*, *11*(1). https://doi.org/10.1186/s43067-024-00155-z

Campbell, R. (2026). Zero Trust for AI Systems: A reference architecture and assurance framework. *Preprints.org*. https://doi.org/10.20944/preprints202602.0085.v1

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, *21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2

Chawande, S. (2024). Adaptive zero trust with AI and Automation. *World Journal of Advanced Engineering Technology and Sciences*, *13*(2), 751–763. https://doi.org/10.30574/wjaets.2024.13.2.0589

Chokkanathan, K., Karpagavalli, S., Priyanka, G., Vanitha, K., Anitha, K., & Shenbagavalli, P. (2024). AI-Driven Zero Trust Architecture: Enhancing Cyber-Security resilience. *Proceedings of CSITSS 2024*, 1–6. https://doi.org/10.1109/csitss64042.2024.10816746

CISA. (2023). *Zero Trust Maturity Model*. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Cloud Security Technical Reference Architecture. (2022). *Federal Risk and Authorization Management Program. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf Top Strategic Technology Trends for 2026

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

Gartner. (2026). *Zero trust 2030 – Business operating system. Gartner Research.* https://www.gartner.com/en/articles/top-technology-trends-2026

Gartner. (2023, January 27). *Gartner predicts growth in zero-trust programs by 2026, despite unprotected areas vulnerabilities. Business of Tech.* https://businessof.tech/2023/01/27/gartner-predicts-growth-in-zero-trust-programs-by-2026-despite-unprotected-areas-vulnerabilities

Karamchand, G. (2024). Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation. *World Journal of Advanced Research and Reviews, 24*(3), 3374–3387. https://doi.org/10.30574/wjarr.2024.24.3.3883

Liman Gambo, M., & Almulhem, A. (2025). Zero trust architecture: A systematic literature review. *Journal of Network and Systems Management*. https://doi.org/10.1007/s10922-025-09998-x

Nizamuddin, M. Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies. Int. J. Inf. Secur. 24, 187 (2025). https://doi.org/10.1007/s10207-025-01095-z

NSTAC. (2022). *Zero trust and trusted identity management: Report to the President*. National Security Telecommunications Advisory Committee. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Nzeako, C., & Shittu, A. (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

Ofili, B. T., Erhabor, E. O., & Obasuyi, T. (2025). Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA compliance. *World Journal of Advanced Research and Reviews, 25*(2), 2377–2400. https://doi.org/10.30574/wjarr.2025.25.2.0620

Paul, J., Kessie, J. D., & Salawudeen, M. D. (2024). Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks. *International Journal of*

Science and Research Archive, 13(2), 4159–4169. https://doi.org/10.30574/ijsra.2024.13.2.2583

Rodrigues, A. (2026). AI-integrated zero trust architectures: A socio-technical analysis of unified enterprise cybersecurity platforms. *International Journal for Research in Applied Science and Engineering Technology, 14*(1), 946–953. https://doi.org/10.22214/ijraset.2026.76981

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020d). *Zero trust architecture*. https://doi.org/10.6028/nist.sp.800-207

Sabin, J. (2021). The future of security in a remote-work environment. Network Security, 2021(10), 15–17. https://doi.org/10.1016/s1353-4858(21)00118-5

Sastry, R. (2025). Zero trust architecture implementation in dynamic workforce environments. *International Journal of Computer Engineering and Technology, 16*(1), 92–99. https://doi.org/10.34218/IJCET_16_01_092

Srivastava, S. (2025). Real time AI-driven threat detection with the integration of zero trust security framework. *TEJAS Journal of Technologies and Humanitarian Science, 4*(4), 25–37. https://doi.org/10.63920/tjths.44004

Ucheji, C. (2026). The future of zero-trust security architecture with AI automation. *International Journal of Research and Scientific Innovation, 13*(1), 700–713. https://doi.org/10.51244/ijrsi.2026.13010060

Ueno, H., Sawa, Y., Kim, J., Urakami, T., Oura, K., & Seaborn, K. (2024). Trust in human-AI interaction: Scoping out models, measures, and methods. *Proceedings of the CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–7. https://doi.org/10.1145/3491101.3519772

Xu, J., Gondal, I., Yi, X., Susnjak, T., Watters, P., & McIntosh, S. (2025). The erosion of cybersecurity zero-trust principles through generative AI: A survey on the challenges and future directions. *Journal of Cybersecurity and Privacy, 5*(4), 87. https://doi.org/10.3390/jcp5040087

Zakhmi, K., Ushmani, A., Mohanty, M. R., Agrawal, S., Banduni, A., & Rao, S. S. K. (2025). Evolving zero trust architectures for AI-driven cyber threats in healthcare and other high-risk data environments: A systematic review. *Cureus*. https://doi.org/10.7759/cureus.85446