Peertechz

ENGINEERING GROUP

Trends in
Computer Science and Information Technology
OPEN ACCESS JOURNAL

ISSN: 2641-3086 Journal DOI: https://dx.doi.org/10.17352/tcsit

Review Article

Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture

Kevin Nehemiah Onchoka*, Zachary Omariba Bosire, Peter Kiprono Kemei

Department of Computer Science, Egerton University, Kenya

Submitted : 06 May, 2026
Accepted : 11 June, 2026
Published : 12 June, 2026

***Corresponding author**: Kevin Nehemiah Onchoka, Department of Computer Science, Egerton University, P.O. Box 536, 20115 Egerton, Kenya,
E-mail: kevin.onchoka@egerton.ac.ke

Keywords: Zero trust; Architecture; Framework; Identity management; Cybersecurity; Authentication; Authorization

https://www.engineegroup.us

Check for updates

Abstract

The rapid evolution of digital transformation, cloud computing, remote work environments, and mobile technologies has significantly weakened traditional perimeter-based cybersecurity models. Conventional security approaches relied heavily on securing organizational network boundaries while assuming that users and devices within the network could be trusted. However, increasing cyber threats, insider attacks, credential theft, and sophisticated attack vectors have demonstrated the limitations of this trust-based model. Consequently, Zero Trust Architecture (ZTA) has emerged as a modern cybersecurity paradigm founded on the principle of "never trust, always verify." Within this framework, identity has become the central element of security enforcement, replacing the traditional network perimeter. This paper examines the evolution of Identity and Access Management (IAM) from traditional authentication systems to identity-centric security mechanisms that support Zero Trust principles. The paper discusses the role of IAM technologies such as Multi-Factor Authentication, Single Sign-On, Privileged Access Management, adaptive authentication, and behavioral analytics in enabling ZTA. Additionally, the paper explores the challenges associated with implementing IAM in Zero Trust environments, including complexity, privacy concerns, legacy systems integration, and usability issues. Finally, password less authentication, artificial intelligence-driven identity analytics, and decentralized identity systems as emerging trends are discussed which forms the future directions in identity-centric cybersecurity.

Abbreviations

ZTA: Zero Trust Architecture; IAM: Identity and Access Management; MFA: Multi-Factor Authentication; SSO: Single Sign-On; PAM: Privileged Access Management; VPN: Virtual Private Network; IoT: Internet of Things; IDS: Intrusion Detection Systems; IPS: Intrusion Prevention Systems; DMZ: Demilitarized Zone; RBAC: Role Based Access Control; ABAC: Attribute Based Access Control; IP: Internet Protocol; IEEE: Institute of Electrical and Electronics Engineers; FIdM: Federated Identity Management; IdP: Identity Provider; OTP: One Time Password; SAML: Security Assertion Markup Language; OAuth: Open Authentication; OIDC: OpenID Connect; FIDO: Fast Identity Online; SIEM: Security Information and Event Management; UEBA: User and Entity Behavior Analytics; AI: Artificial Intelligence; JIT: Just In Time; SSI: Self-Sovereign Identity; API: Application Programming Interface; VLAN: Virtual Local Area Network; DID: Decentralized Identity; CTAP: Client To Authenticator Protocol; MTTD: Mean Time To Detect; MTTR: Mean Time To Respond; sPACA: Strong PIN-based Access Control for Authenticators; IRR: Incident Response Rate; UAR: Unauthorized Access Rate

Introduction

Background of the study

Cybersecurity has traditionally depended on perimeter-based security models designed to protect organizational resources by establishing trusted internal networks and untrusted external environments. This approach, commonly referred to as the "castle-and-moat" security model, focused on securing firewalls, intrusion detection systems, and virtual private networks (VPNs) at the network boundary. Once users gained access to the internal network, they were often granted

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

broad access privileges with minimal additional verification [1,2].

However, technological advancements such as cloud computing, Internet of Things (IoT), mobile devices, remote working environments, and distributed enterprise systems have significantly transformed organizational IT infrastructures [1,2]. Modern users access organizational resources from multiple devices, locations, and networks beyond traditional corporate boundaries. Consequently, cyber attackers increasingly exploit compromised credentials, insider privileges, and weak authentication systems to gain unauthorized access.

These evolving threats have exposed the limitations of traditional perimeter-based security architectures. In response, Zero Trust Architecture (ZTA) has emerged as a modern security framework that eliminates implicit trust and continuously validates every user, device, application, and transaction before granting access [4]. Within this model, identity becomes the primary security control mechanism.

Identity and Access Management (IAM) plays a central role in enabling Zero Trust principles by ensuring that only authenticated and authorized users can access organizational resources. Modern IAM solutions integrate advanced authentication mechanisms, adaptive access control, behavioral analytics, and least privilege enforcement to provide continuous identity verification. This transformation has led to the concept of "identity as the new perimeter," where security decisions are increasingly based on user identity rather than network location [3,5,6].

This paper examines the evolution of IAM technologies and their integration within Zero Trust Architecture frameworks to enhance modern cybersecurity strategies.

Problem statement

Traditional cybersecurity models rely heavily on perimeter-based defenses that assume internal users and devices can be trusted once authenticated into organizational networks. However, the growth of cloud services, remote access, insider threats, and credential-based attacks has rendered these assumptions ineffective. Cybercriminals increasingly exploit compromised identities and privileged accounts to bypass traditional defenses [2,5,7].

Although Zero Trust Architecture provides a more secure approach by enforcing continuous verification and least privilege access, many organizations face challenges in transitioning from conventional IAM systems to identity-centric security frameworks. Furthermore, the rapid evolution of IAM technologies has created complexities related to scalability, interoperability, usability, and policy enforcement.

Therefore, there is a need to examine how IAM has evolved within Zero Trust Architecture and how identity-centric security can effectively address modern cybersecurity challenges.

Objectives of the study

General objective

To examine the evolution of Identity and Access Management within a Zero Trust Architecture framework.

Specific objectives

1. To evaluate traditional perimeter-based security models and identify their limitations in addressing modern cybersecurity threats.
2. To examine the evolution of Identity and Access Management technologies.
3. To evaluate the role of identity in Zero Trust Architecture.
4. To identify challenges associated with implementing IAM in Zero Trust environments.

Research questions

1. What limitations do traditional perimeter-based security models face in addressing modern cybersecurity threats?
2. How has Identity and Access Management evolved over time?
3. Why is identity considered the new perimeter in Zero Trust Architecture?
4. What are the challenges affecting IAM implementation in Zero Trust environments?

Significance of the study

This study contributes to the growing body of knowledge on modern cybersecurity architectures by examining the transition from traditional perimeter-based security to identity-centric security models. The findings may benefit organizations seeking to implement Zero Trust security frameworks, cybersecurity professionals interested in IAM modernization strategies, researchers exploring emerging cybersecurity paradigms and policymakers developing identity governance and access control policies. The study also provides academic insights into how IAM technologies support secure digital transformation initiatives.

Scope of the study

This paper focuses on the evolution of Identity and Access Management within the context of Zero Trust Architecture. The study examines traditional and modern IAM technologies, identity-centric security principles, IAM challenges in ZTA implementation, and emerging trends shaping future cybersecurity systems. The study is limited to conceptual and literature-based analysis without conducting empirical data collection.

Literature review

Traditional perimeter-based security

Traditional perimeter-based security underpins the

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

"castle-and-moat" model that Zero Trust and identity-centric approaches are now replacing. It assumes that the internal network is trusted while the outside is not, with defenses focused on the boundary rather than every user and device.

Core concepts and architecture of the traditional perimeter-based security

Security perimeter is one of the concepts where networks are split into an internal trusted zone and an external untrusted zone, typically enforced by firewalls, border routers, IDS/IPS, VPNs, DMZs, and screened subnets [8,9]. Trust model is another concept where internal entities are trusted by default; external entities must authenticate once to gain lasting trust ("trust but verify") [9-11]. Castle-and-moat analogy is also another concept in which there are strong outer walls but "soft" inside and once an attacker gets in, there is often little internal segmentation or further checks [12].

Key weaknesses of perimeter-based security

Some of the key weaknesses of perimeter-based security include (a) insider and post-breach risk whereby once the perimeter is breached, attackers can move laterally with few checks, threatening critical data and systems (b) static and single-barrier defense whereby a single, mostly static perimeter becomes a single point of failure in dynamic, distributed environments (c) poor fit for cloud, remote work, and IoT whereby blurred boundaries, remote access, and distributed services make location-based trust unreliable (d) assumed "safe internal traffic" whereby lack of continuous verification leaves networks vulnerable to compromised credentials and malicious insiders.

These limitations drive the shift from perimeter-centric to identity- and access-based controls. Zero Trust and modern IAM continuously authenticate and authorize every user, device, and transaction, regardless of network location, directly addressing the weaknesses of traditional perimeter security [8,9].

Zero Trust Architecture (ZTA)

ZTA is built on "never trust, always verify," assuming any user, device, or app may be compromised, inside or outside the network [1,2].

Core principles and practices

ZTA is based on the following core principles and practices (a) continuous authentication and authorization whereby every request is verified based on identity, device health, behavior, and context, not just initial login [3,13] (b) least privilege access whereby users/devices get only the minimal permissions needed, reducing damage from compromised accounts [1,2,13] (c) micro-segmentation whereby networks are split into small segments with strict policies, limiting lateral movement during breaches [2,6] (d) continuous monitoring and analytics whereby real-time behavior analysis, anomaly detection, and logging detect and respond to threats quickly [1-3] (e) identity-centric security where strong identity verification (often with MFA and IAM) is the cornerstone of ZTA [1-3,13]. ZTA shifts protection from static network boundaries to who/what is accessing what, under which conditions, making it suitable for cloud, hybrid, and remote environments.

ZTA components and effects

Table 1 shows the Zero Trust Architecture components and effects.

Identity and Access Management (IAM)

IAM manages digital identities and controls who can access which resources, when, and how [3,6,14] as illustrated in figure 1.

Core IAM functions

Identity and Access Management has the following core functions: (a) authentication which verify user/device identity via passwords, MFA, biometrics, or behavioral signals (b) authorization which enforce what authenticated entities can do using role-based or attribute-based models (c) identity governance which does lifecycle management, policy enforcement, and compliance reporting (d) access provisioning & role management which assigns/removes access based on roles and business needs, reducing privilege misuse.

Modern IAM capabilities

The modern Identity and Access Management capabilities are: (a) Single Sign-On (SSO) and MFA to strengthen and streamline login (b) adaptive/authentication & risk-based access which involve context-aware checks using behavior, device, and location (c) Privileged Access Management (PAM) for tight control and monitoring of high-risk accounts (d) AI- and behavior-driven IAM such as machine learning and user behavior analytics for anomaly detection and dynamic policies.

Table 1: Zero Trust Architecture Components and Effects.

ZTA Component	Main Purpose
Least privilege + RBAC/ABAC	Minimize access and privilege creep
Continuous authentication	Re-check trust for every request
Micro-segmentation	Limit blast radius of breaches
Strong identity & MFA	Make identity the primary control point
Monitoring & analytics	Detect anomalies in real time

Abbreviations: RBAC: Role-Based Access Control; ABAC: Attribute Based Access Control; MFA: Multi-Factor Authentication.

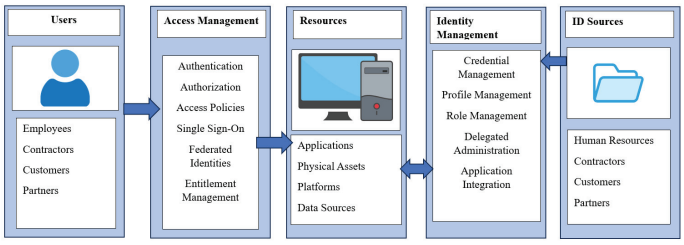

Figure 1: An overview of Identity and Access Management (IAM) flow.

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

Research consistently positions IAM as foundational for enforcing Zero Trust. ZTA relies on IAM plus MFA, behavioral analytics, and micro-segmentation to implement continuous, least-privilege, identity-centric access decisions. AI-enhanced IAM further aligns with ZTA by enabling continuous, adaptive authentication and real-time risk scoring for every access attempt.

In conclusion, ZTA redefines security around continuous verification, least privilege, micro-segmentation, and identity-centric controls. IAM supplies the identity, authentication, authorization, and governance backbone that makes these Zero Trust principles enforceable in practice, especially when strengthened with MFA, behavioral analytics, and AI-driven adaptive policies. Together, ZTA and IAM create a tightly integrated, context-aware defense against modern cyber threats. Table 2 highlights the comparison between traditional perimeter-based security and zero trust model.

Research gap and contribution

Existing work analyzes ZTA cost–effectiveness, enterprise security gains, AI-driven IAM, phishing resistant authentication, and decentralized identity for trustworthy governance. However, research remains fragmented: most studies focus on single technologies or domains rather than providing an integrated, critical synthesis of identity-centric Zero Trust, covering IAM evolution, MFA vs FIDO2, AI-driven IAM risks, decentralized identity scalability, and quantified Zero Trust outcomes.

This paper addresses that gap by (a) unifying seminal IAM, ZTA, FIDO2/WebAuthn, AI-IAM, and decentralized identity (DID) literature into a coherent identity-as-perimeter perspective, (b) critically evaluating benefits and limitations (e.g., phishing resistance vs downgrade attacks, AI explainability and bias, DID interoperability), and (c) aligning these insights with quantitative evidence on Zero Trust adoption costs and security metrics.

The contribution is a multi-dimensional critical review that connects these strands into a coherent picture of "identity as the new perimeter" in practice.

Methodology

This study followed a structured literature review process guided by PRISMA principles to examine how Identity and Access Management (IAM) has evolved and how it enables Zero Trust Architecture (ZTA), with a focus on "identity as the new perimeter" hence ensuring reproducibility and transparency.

Searches were conducted in IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, ScienceDirect, Web of Science, and Google Scholar, selected for their comprehensive coverage of security, networking, IAM, AI, and cryptography research.

Search strings combined Zero Trust, IAM, MFA, AI, and decentralized identity concepts using Boolean operators, for example: ("Zero Trust Architecture" OR "ZTA") AND ("identity and access management" OR "IAM"), ("multi-factor authentication" OR "MFA" OR "FIDO2" OR "WebAuthn") AND (phishing OR "password less"), ("AI-driven IAM" OR "machine learning" AND ("access control" OR "anomaly detection")), ("decentralized identity" OR "self-sovereign identity" OR "blockchain-based identity") AND (interoperability OR scalability OR governance), ("human factors" OR "insider threats" AND "cybersecurity awareness training"). The objectives include (a) trace the evolution from perimeter-based security to Zero Trust and identity-centric models (b) analyze how IAM capabilities support ZTA principles (c) identify challenges and future directions. The temporal scope was 2011 - 2026, covering the formalization of Zero Trust and contemporary IAM and identity research.

Studies were included if they (a) addressed ZTA concepts, implementation, or roadmaps with explicit reference to identity, IAM, or continuous verification (b) focused on IAM technologies, such as MFA, SSO, PAM, AI-driven anomaly detection, or risk-based access (c) investigated decentralized/SSI identity, blockchain-based IAM, or privacy-preserving authentication (d) explored human factors, insider threats, and training in cybersecurity contexts connected to Zero Trust or identity controls. Conceptual opinion pieces without clear methodological grounding and purely technical works unrelated to IAM/ZTA integration were excluded.

Screening followed a PRISMA-style process: Initial screening of titles and abstracts to remove clearly irrelevant papers, full-text review of remaining studies to verify relevance to IAM–ZTA, identity-centric security, or human / AI / decentralized identity aspects. Classification and mapping of selected works into themes: Evolution of perimeter vs Zero Trust and identity, IAM technologies and AI-driven enhancements, Decentralized/SSI identity frameworks, Human factors and awareness strategies.

For each included paper, key data elements were extracted as in the ZTA SLR [15] which include: objectives, methodology type, IAM/ZTA components studied, challenges, and reported results, using classification approaches from prior mapping studies. Findings were synthesized using narrative, comparative analysis: cross-comparing how different studies conceptualize Zero Trust and the identity perimeter, aggregating evidence about the effectiveness and limitations of MFA, PAM, AI-driven IAM, and decentralized identity, integrating insights on human behavior, training, and culture to complement technical IAM controls. A PRISMA-style flow diagram (Figure 2) summarizes the screening and selection stages.

Table 2: A comparison between Traditional Perimeter Security and Zero Trust Model.

Aspect	Traditional Perimeter Security	Zero Trust Model
Trust assumption	Inside = trusted, outside = untrusted	No implicit trust anywhere
Authentication	One-time at perimeter	Continuous, context-aware
Access basis	Network location, Internet Protocol (IP)/port rules	Identity-, attribute-, and risk-based
Encryption	Often external only; internal often unencrypted	Encrypt data in transit and at rest
Segmentation	Coarse zones, few internal barriers	Fine-grained micro-segmentation

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

Evolution of Identity and Access Management (IAM)

Identity and Access Management has undergone several stages of transformation namely; password-based authentication era, role-based access control, federated identity management and single sign-on, multi-factor and adaptive authentication and identity-centric security.

Password-based authentication era

Early IAM systems relied almost exclusively on username–password pairs stored in centralized credential databases as illustrated in figure 3. While simple and cheap to deploy, passwords suffer from poor memorability, leading users to choose weak, guessable passwords and to reuse or slightly modify them across many services [16-18]. Large-scale analyses of leaked credentials show that password reuse and similarity allow attackers to compromise up to approximately 16% of accounts in targeted guessing attacks, even in the presence of modern countermeasures [17]. Password databases are also attractive breach targets; once stolen, they enable offline cracking and credential stuffing, where attackers test known username–password pairs across multiple sites [19,20]. Measurements on real web traffic found that approximately 1.5% of logins used already-breached credentials [19]. Phishing further exploits password-based models by tricking users into submitting credentials to fake sites, with usability issues (too many passwords, confusing browser indicators) worsening this risk [18]. The password-based authentication is shown in figure 2.

These systemic weaknesses motivated stronger IAM models, password managers, breach-alerting services, and new authentication factors [17-20].

Role-Based Access Control (RBAC)

RBAC shifted access management from individual users to roles that encapsulate job functions. Permissions are assigned to roles, and users are assigned to roles, simplifying administration, supporting least privilege, and easing personnel changes [21] as illustrated in figure 4. In large enterprises and cloud environments, RBAC improves scalability and regulatory compliance by standardizing who can do what [21].

However, traditional RBAC is largely static and non-contextual. It struggles with dynamic, fine-grained needs (e.g., time, device, risk level) and can suffer from "role explosion" and over-permissive roles if not carefully engineered and audited [21]. These limitations have driven interest in risk-aware and attribute-based extensions [22].

Federated Identity Management (FIdM) and Single Sign-On (SSO)

Federated Identity Management (FIdM) lets users authenticate once with an Identity Provider (IdP) and then access multiple independent services (Service Providers) via Single Sign-On, reducing password proliferation and improving usability [23-26] as illustrated in figure 5.

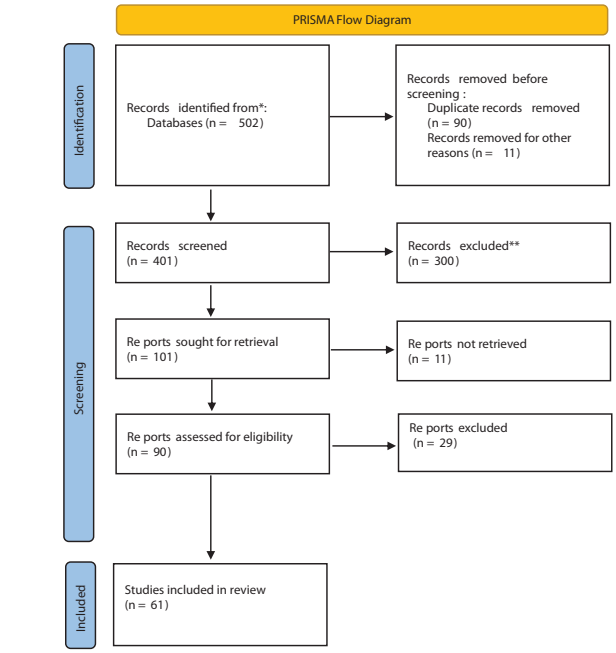

Figure 2: PRISMA flow diagram showing the identification, screening and inclusion of studies in this review.
Source: Page MJ, et al. BMJ 2021; 372:n71. doi: 10.1136/bmj.n71 adopted from https://www.prisma-statement.org/prisma-2020-flow-diagram

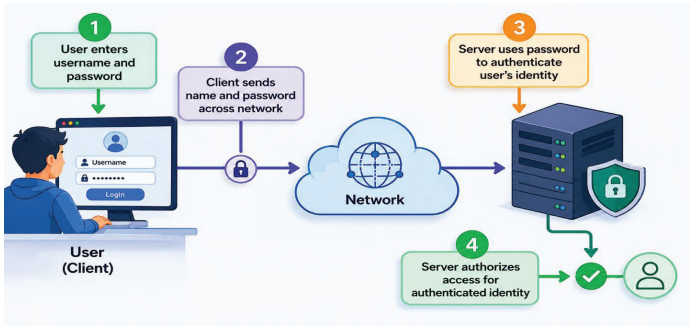

Figure 3: Password-based authentication.

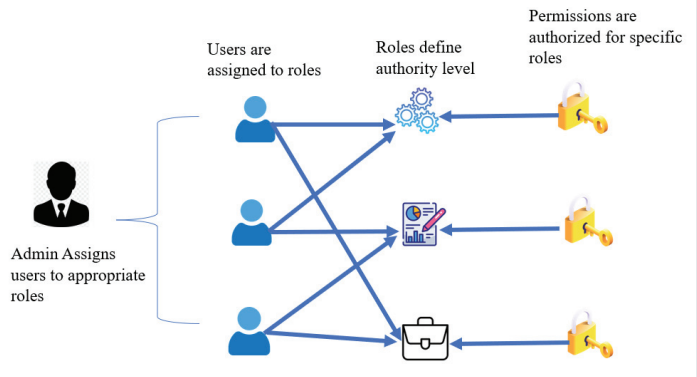

Figure 4: Role-Based Access Control.

Core technologies include Security Assertion Markup Language (SAML 2.0) which is XML-based assertion widely used for enterprise SSO across domains, Open Authentication (OAuth 2.0) a delegation protocol allowing limited access to resources without sharing credentials and OpenID Connect

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

(OIDC) an identity layer on OAuth 2.0 standardizing user authentication and profile claims as illustrated in figure 6.

These standards improve interoperability across organizations and clouds, support centralized authentication, and reduce the amount of sensitive data shared between parties [23-26]. However, they were designed for earlier assumptions and now require extensions and new profiles to address mobile apps, privacy, and emerging zero-trust and decentralized identity use cases [24-26].

Multi-factor and adaptive authentication

To mitigate password weaknesses, Multi-Factor Authentication (MFA) combines something you know (password), something you have (tokens, devices), and something you are (biometrics) [27,28] as illustrated in figure 7. One-time passwords (OTPs), hardware/software tokens, and biometric checks significantly raise the bar for account takeover, especially in high-risk sectors like finance [16,22]. Modern systems go further with adaptive (risk-based) authentication, which evaluates contextual factors, device characteristics, location, time, historical behavior, and threat signals to assign a dynamic risk score and adjust requirements in real time [22,27]. Low-risk logins may proceed with minimal friction, while high-risk events trigger step-up MFA, session restrictions, or denial. Machine learning and user behavior analytics increasingly power these assessments and anomaly detection.

In regulated or compliance-critical environments, unified risk-based IAM frameworks combine identity federation, MFA, behavioral analytics, and continuous monitoring to improve both security and regulatory adherence [22,27].

Identity-centric security in zero trust

As organizations adopt Zero Trust Architecture (ZTA), identity has become the effective security perimeter. Instead of trusting anything "inside" a network, ZTA assumes potential compromise and enforces "never trust, always verify" for every request, regardless of location [16,27,29] as illustrated in figure 8.

Identity-centric Zero Trust IAM typically includes (a) strong, continuously evaluated user and device identities, with

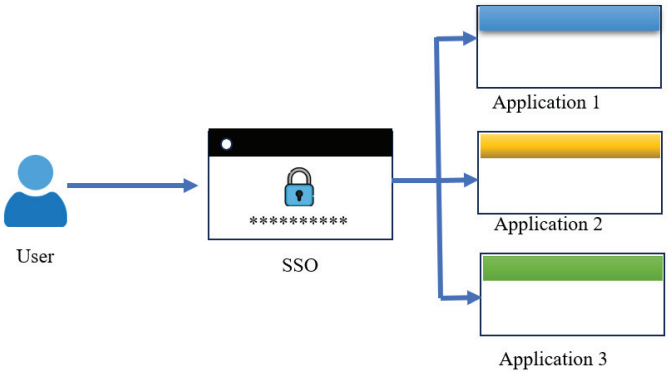

Figure 5: Single Sign-On Scheme.

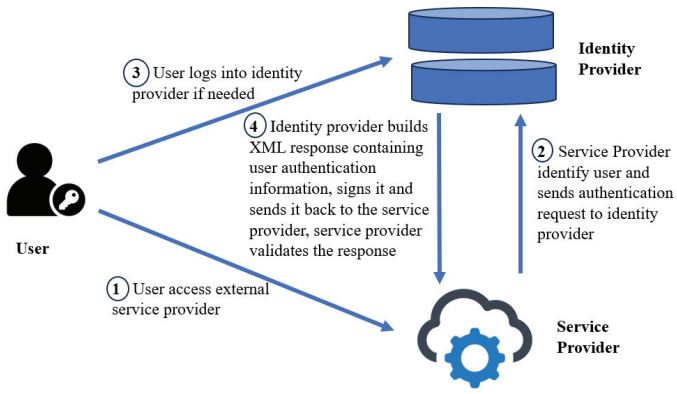

Figure 6: Single Sign-On Process.

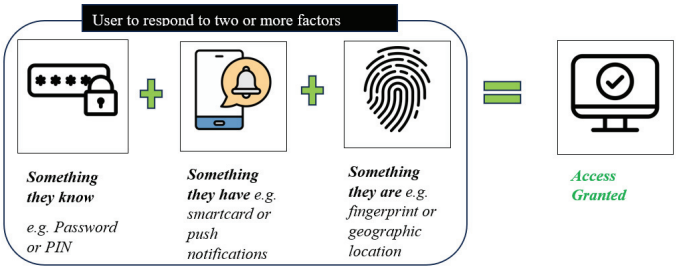

Figure 7: Multi-Factor Authentication.

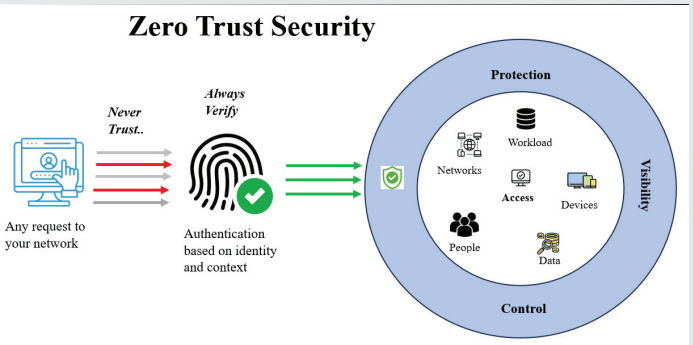

Figure 8: Zero Trust Security.

devices treated as first-class identities and categorized as safe/unsafe (b) device health and posture checks integrated into access decisions (c) contextual and behavioral analytics, using sign-in logs, behavior baselines, and anomaly detection to compute risk scores on an ongoing basis, sometimes every few minutes (d) least privilege and dynamic policies, where roles, attributes, and risk jointly determine minimal, time-bounded access, often enforced alongside micro-segmentation and role-based network access management.

Research shows that AI-driven IAM and risk-based authentication, aligned with Zero Trust principles, can significantly improve detection of identity spoofing, privilege escalation, and misuse of stolen credentials while maintaining user experience through adaptive friction [16,22,27,28]. This represents a fundamental move from static, one-time checks toward continuous, intelligence-driven trust evaluation as the core of modern IAM. Table 3 highlights the IAM main eras, their primary focus and key limitations.

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

Identity as the new perimeter

Identity-centric security treats identity (human and non-human) as the primary control plane, shifting protection from static network borders to continuous verification of users, devices, applications, Application Programming Interface (APIs), and workloads [6,30].

Modern Zero Trust and cloud-native IAM systems use (a) strong identity proofing and MFA before any session is established (b) context signals such as device health, geolocation, time, and resource sensitivity to drive access decisions (c) continuous validation of identity and session behavior, not just at login, using monitoring and behavioral analytics. This reduces reliance on IP ranges or VLANs and instead enforces identity-based policies.

IAM Technologies Supporting ZTA

Table 4 capture the various IAM technologies and how they support ZTA.

Advanced patterns such as Just-in-Time (JIT) access and behavior-based dynamic access further tighten least-privilege enforcement [30,31].

Benefits of identity-centric security

Research links identity-centric, Zero Trust IAM to (a) reduced insider and credential-based threats through continuous authentication, PAM, and behavioral analytics (b) improved access visibility and auditability via centralized IAM, identity governance, and detailed session trails, especially for privileged accounts (c) better compliance with regulations that require strong authentication, least privilege, and demonstrable access controls (d) stronger remote/hybrid work security, as access is based on identity and context rather than physical location (e) reduced attack surface and lateral movement through micro-segmentation, least privilege, JIT, and per-segment identity enforcement.

Table 3: Main IAM Eras, their primary focus and limitations.

Era / Model	Primary Focus	Key Limitations
Password-only	Simple user authentication	Weak/reused passwords, phishing, credential stuffing
RBAC	Role-structured authorization	Static roles, little context, role explosion
Federated SSO	Cross-domain SSO & interoperability	Protocol complexity, evolving use cases
MFA & Adaptive	Stronger, context-aware auth	Integration, usability, policy complexity
Zero Trust / Identity-centric	Continuous, risk-based access	Organizational and technical migration challenges

Abbreviations: RBAC: Role-Based Access Control; MFA: Multi-Factor Authentication; SSO: Single Sign-On

Table 4: Identity and Access Management Technologies supporting Zero Trust Architecture.

Technology	Identity-Centric Role in ZTA
Multi-Factor Authentication	Adds extra factors (biometrics, OTP, hardware keys) to resist phishing, credential theft, and brute force
Single-Sign On & federation	Centralizes authentication across Software-as-a Service (SaaS), cloud, and on-premise via SAML, OAuth2, OIDC; reduces password reuse and identity sprawl
Privilege Access Management (PAM)	Discovers, isolates, monitors, and audits privileged accounts; enforces least privilege and "need-to-know" for admins and critical systems
Conditional / risk-based access	Dynamically allows, challenges, or blocks access based on risk scores, device posture, and context
Behavioral analytics / User and Entity Behavior Analytics (UEBA)	Builds normal behavior baselines and detects anomalies (unusual logins, access patterns) for identity-driven threat detection

Abbreviations: OTP: One Time Password; SAML: Security Assertion Markup Language; OAuth: Open Authentication; OIDC: OpenID Connect; PAM: Privilege Access Management; UEBA: User and Entity Behavior Analytics

Challenges of IAM in ZTA

(I) Legacy System Integration: Legacy applications often lack modern protocols (SAML, OAuth2, OIDC, Fast Identity Online (FIDO2) and fine-grained policy hooks, complicating Zero Trust rollouts [30,32]. Integration issues include brittle custom authentication, mainframe/monolith constraints, and limited telemetry for continuous verification [30,332].

(II)Complexity of Implementation: ZTA with IAM demands policy redesign from coarse network rules to granular identity and attribute-based policies; infrastructure modernization (cloud-native IAM, micro-segmentation, telemetry pipelines); continuous monitoring stacks (Security Information and Event Management (SIEM), UEBA, AI models) that can scale across multi-cloud. This raises complexity and cost, and requires new skills and operating models [6,30,32].

(III) User Privacy Concerns: Continuous monitoring, UEBA, and AI-driven analytics may expose sensitive behavioral data and raise concerns about surveillance, especially in cloud and multi-tenant contexts [2,33]. Privacy-preserving techniques (such as zero-knowledge proofs and minimal data collection) are being explored in some MFA and identity designs [33,34].

(IV) MFA Fatigue and User Experience: Frequent prompts and poor design can create MFA fatigue, encourage risky workarounds and impact productivity [30,35]. Adaptive and risk-based authentication aim to reduce friction by challenging only higher-risk activities.

(IV) Identity Sprawl: Hybrid and multi-cloud adoption often lead to multiple overlapping identity stores (AD, cloud directories, SaaS accounts), increasing admin overhead, inconsistent policies, and blind spots. Federated identity and centralized governance are proposed to reduce this sprawl [31,32,34].

MFA vs FIDO2/WebAuthn and Identity in Zero Trust

Conventional MFA (e.g., OTPs over SMS, email, or apps) improves security over passwords but remains vulnerable to real-time phishing and adversary-in-the-middle credential relay [36]. In contrast, FIDO2/WebAuthn offers phishing-resistant authentication using device-resident private keys and origin-bound public keys, significantly raising the bar for attackers [37-39].

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

Formal and empirical analyses confirm WebAuthn's strong authentication guarantees, while also identifying weaknesses and proposing protocol-level improvements (e.g., stronger CTAP security models, sPACA, and enhanced downgrade resilience) [39,40]. Recent work further explores high-assurance architectures that secure virtual FIDO2 authenticators with QES-grade tokens and untrusted cloud synchronization, maintaining a pure WebAuthn interface while strengthening key protection [37]. Alternative protocols such as QRAuth seek to retain public-key security while addressing FIDO2's usability and accessibility limitations [38].

Within Zero Trust, identity becomes the primary trust anchor: every access request is authenticated and authorized continuously, often combining phishing-resistant mechanisms like FIDO2/WebAuthn with contextual checks and micro-segmentation. Nonetheless, implementation must account for device and platform dependencies, recovery processes, fallback mechanisms that may reintroduce phishing risks, and user experience constraints.

Emerging trends in IAM and ZTA

(I) Password less Authentication: Passwordless aims to remove passwords, which are prone to phishing and brute-force attacks. Reviews show benefits in security and user experience but note deployment cost, usability, and scalability challenges [35].

(II) Artificial Intelligence in IAM: AI and machine learning enhance IAM by threat detection & risk assessment where (User and Entity Behavior Analytics) UEBA and ML models flag anomalous logins, access patterns, or device behavior in real time [2]. Adaptive authentication & policy automation require dynamic trust scoring to provide feeds for conditional access, JIT access, and continuous authorization. Research highlights improved detection accuracy but also stresses data quality and governance requirements [2,41].

(III) Decentralized Identity: Decentralized identity and blockchain-based credentials support self-sovereign identity, where users control verifiable credentials without a single central IdP. Work links these models with ZTA to enhance privacy and resilience while maintaining strong trust guarantees [2,33,34].

(IV) Identity Threat Detection and Response (ITDR): Multiple works describe identity-focused detection and response such as monitoring IAM, MFA, and PAM systems for credential abuse, privilege escalation, and account takeover; using AI-driven analytics and SIEM integration to orchestrate real-time containment (account lock, step-up auth, revoking tokens) [2,30,32,34]. ITDR is emerging as a dedicated layer for protecting the identity control plane in Zero Trust environments.

AI-Driven IAM and Decentralized Identity

AI-driven IAM leverages machine learning and behavioral analytics to enhance authentication, authorization, and monitoring, enabling adaptive access control and real-time anomaly detection [42]. Surveys show AI can reduce manual workload, improve detection of anomalous identities, and support continuous risk assessment.

However, these gains introduce new risks. Key challenges include data privacy, integration complexity, and the interpretability of ML-driven decisions [42,43]. AI in IAM must contend with model bias and fairness issues, as unbalanced training data can lead to discriminatory access decisions [44]. False positives can burden users and administrators, while false negatives may leave attacks undetected [42,45]. Adversarial attacks and data poisoning further threaten AI-based detection pipelines, especially when used to defend against AI-driven phishing and malicious URLs [36]. Governance requirements such as transparent communication, robust data governance, lifecycle model management, and human oversight are therefore emphasized as essential for trustworthy AI-IAM deployment.

Decentralized identity and DID systems promise user-controlled, privacy-preserving identity, but face interoperability, scalability, and governance challenges. Integrating explainable deep learning with DID is proposed as a way to align transparency, fairness, and privacy in algorithmic governance, using verifiable credentials, zero-knowledge proofs, and privacy-preserving audit trails [44]. These systems must still address cross-platform interoperability, performance under large-scale usage, and clear accountability models before they can be widely adopted as IAM underpinnings in Zero Trust environments.

Case studies in enterprise and government

Modern security architectures in enterprises and government agencies are moving from network perimeters to identity as the primary control point, often within Zero Trust frameworks. The case studies below show how this shift is implemented in practice and what outcomes organizations report.

Cases where identity has become the perimeter

Table 5 gives a highlight of the various organizations and sectors where identity has become the new security perimeter.

Government and public sector focus

Government and public-sector deployments use identity-centric Zero Trust to secure federal financial systems, distributed government systems, and tax administration platforms, emphasizing continuous verification, segmentation, and advanced identity management to protect citizen data and enable inter-agency collaboration [46-48,51].

Across enterprises and government institutions, real-world implementations show that treating identity as the new security perimeter within Zero Trust architectures measurably improves security, compliance, and visibility. These gains come with substantial design, integration, and change-management effort, but case studies suggest that when IAM is mature and

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

Table 5: Sample cases where identity replaces the network perimeter.

Organization / Context	Sector / Setting	How Identity is the Perimeter	Outcomes	Citation
Large banks, healthcare providers, and government agencies	Highly regulated enterprises	Centralized IAM, identity-centric access, AI/zero trust	Fewer security incidents, better compliance, higher user satisfaction	[46]
Federal tax administration system	Federal government	Zero Trust with identity, devices, networks, apps, and data pillars	Fewer credential compromises, better containment of breaches	[47]
Google BeyondCorp model	Tech / internal apps	Access based on user identity, device posture, context	Reduced insider/credential risk; secure remote work without a VPN	[48,49]
Mid-size Azure deployment	Enterprise, hybrid cloud	Strong identity verification, MFA, policy-driven access	Reduced attack surface but notable user friction and complexity	[50]

Abbreviations: IAM: Identity and Access Management; VPN: Virtual Private Network; MFA: Multi-Factor Authentication

change is well managed, identity-first security becomes a sustainable foundation for modern, distributed environments.

Comparative evaluation of zero trust frameworks

Recent empirical work quantifies the impact of Zero Trust frameworks compared to perimeter-based models. Large-scale evaluations across 300 enterprises report that ZTA deployments reduced Mean Time to Detect by 40%, improved Mean Time to Respond by 39%, and decreased successful breaches by 63%, also achieving 75% fewer annual incidents, 70% less downtime, and 78% lower financial losses; all improvements were statistically significant [52]. Another study found that ZTA improved breach detection rates by ~75% and reduced unauthorized access incidents by ~66.7%, albeit with higher implementation costs and some user-experience degradation due to continuous verification [53].

Cost–benefit analyses show that ZTA can reduce risk impact by an average of $684K over four years for small to large organizations, while demanding significant upfront investments [54]. Case-oriented research on mid-sized enterprises indicates up to 90% reduction in lateral movement, 65% fewer insider threats, and 80% reduction in attack surface through micro-segmentation and identity-centric controls [55].

Framework-level comparisons highlight that NIST SP 800-207 and the Forrester ZTX model share core principles (never trust, always verify; least privilege; micro-segmentation), but differ in emphasis and implementation guidance [48]. Studies combining these frameworks with industry case studies (e.g., BeyondCorp, Microsoft implementations, U.S. federal mandates) underscore trade-offs between improved access control, compliance, and threat mitigation versus integration challenges, performance overhead, and organizational readiness [48,52,53,55].

These quantitative and comparative findings support a more evidence-based discussion of Zero Trust frameworks, aligning them with measurable outcomes (IRR, UAR, MTTD, MTTR, financial impact) and contextual factors such as sector, legacy complexity, and governance maturity [52,54,55].

Recommendations

Organizational recommendations

(I) Adopt Zero Trust Principles via Phased IAM Modernization: Research emphasizes that ZTA adoption is a journey, not a single project, and should be implemented gradually to manage complexity, cost, and disruption [6,56]. Organizations should (a) start with identity and IAM as core pillars, integrating continuous authentication, MFA, and behavioral analysis into existing access flows before attempting full network micro-segmentation (b) conduct Zero Trust maturity assessments and baseline IAM capabilities to prioritize gaps (such as lack of MFA, over-privileged accounts, missing logs) (c) use a phased roadmap across key domains (identities, devices, applications, data, network, visibility) to reduce risk and maintain operational continuity (d) continuously refine policies and controls as threat patterns, infrastructure, and business processes evolve.

This staged approach aligns with recommendations that ZTA be introduced in ways that minimize performance overhead and integration risk, while enhancing resilience.

(II) Implement Multi-Factor Authentication (MFA) Across Critical Systems: MFA is repeatedly highlighted as a foundational Zero Trust and IAM control, significantly strengthening authentication beyond passwords [6,33,56]. Key implementation details include (a) prioritize MFA for high-value assets (such as admin accounts, cloud consoles, VPNs, remote access, financial and medical systems) and then expand to broader user populations (b) use a mix of factors (hardware/software tokens, biometrics, OTPs) appropriate to risk and usability requirements; blockchain-backed MFA with zero-knowledge proofs can further enhance integrity and privacy in advanced settings (c) integrate MFA into federated identity and SSO so that strong authentication is applied consistently across on-premise and cloud services, without excessive user friction (d) combine MFA with continuous authentication, where signals such as device posture and behavior can trigger step-up checks in a Zero Trust context.

Privacy-preserving MFA schemes using distributed authentication and zero-knowledge proofs demonstrate that strong verification can coexist with user privacy and resilience against single points of failure [33].

(III) Enforce Least Privilege Access Policies: Least privilege is a central ZTA and IAM principle for limiting lateral movement and damage from compromised accounts

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

[6,56]. Organizations should (a) transition from broad, static roles to granular, tightly scoped permissions, regularly reviewed for necessity and aligned with job functions (b) use role-based and attribute-based access control combined with contextual risk signals so that access is influenced by user role, device state, and environment (c) implement Privileged Access Management (PAM) to tightly control and monitor high-risk accounts, with just-in-time (JIT) elevation and detailed logging (d) pair least privilege with network micro-segmentation, using IAM to enforce strict access boundaries for each segment, reducing the blast radius if a segment is breached.

Research on ZTA and insider threats repeatedly shows that enforcing least privilege and micro-segmentation helps contain breaches and reduces opportunities for malicious or negligent insiders [6,57,58].

(IV) Invest in AI-Driven Identity Analytics and Anomaly Detection: AI and machine learning are increasingly seen as transformative for IAM, addressing the limitations of static, rule-based systems in detecting subtle or novel identity threats [6,59]. Recommended actions (a) deploy AI-driven anomaly detection within IAM to baseline normal user and device behavior, then flag deviations that may indicate credential misuse, insider threats, or account takeover (b) integrate behavioral analytics and risk scoring into access decisions, enabling adaptive authentication and dynamic authorization based on real-time context (c) use AI to automate identity governance tasks such as detecting toxic permission combinations, dormant accounts, or anomalous privilege usage (d) address AI challenges - bias, explainability, false positives, privacy - by incorporating human oversight, clear governance, and transparency into model design and deployment.

(V) Promote Cybersecurity Awareness and Identity Security Training: Multiple studies stress that human factors such as negligence, phishing susceptibility and intentional insiders remain critical weaknesses even in technologically advanced environments [1,57,60]. Organizations should (a) implement regular, targeted security education, training, and awareness programs (such as quarterly training and frequent risk communications) to address phishing, social engineering, password hygiene, and identity protection (b) tailor training for different roles (analysts, admins, general staff) and include psychological and behavioral aspects such as decision-making under pressure and ethical responsibilities (c) use simulations, and realistic phishing exercises to improve engagement and retention of knowledge (d) build a security-centric culture that encourages reporting suspicious activity without fear, reinforces adherence to policies, and supports cross-department collaboration (e) maintain detailed identity, authentication, and access logs; apply AI-driven analysis for real-time detection within a Zero Trust framework.

Evidence from banking, critical infrastructure, and fintech sectors shows that continuous awareness programs, combined with behavioral analytics and Zero Trust monitoring, significantly reduce insider and human-related vulnerabilities [57,58,60].

Future work recommendations

(I) AI - Driven Identity Management: Research already highlights opportunities and challenges of AI in IAM-adaptive authentication, real-time anomaly detection, and risk-based access, but overlooked issues like bias, explainability, and integration complexity [6,59]. Future work should (a) develop explainable AI models for identity analytics that security teams can understand and trust and (b) explore continuous learning frameworks that adapt to new attack patterns while minimizing false positives and privacy risks.

(II) Decentralized and Self-Sovereign Identity Systems: Systematic mapping and surveys show that decentralized and self-sovereign identity (SSI) is a promising but still early-stage field, heavily focused on security, privacy, and trust but lacking mature architectures and usability research [59,61]. Future work should (a) design scalable, interoperable SSI architectures with clearly defined components and best practices across domains; (b) investigate user experience, usability, and governance aspects, which are currently under-researched, to ensure decentralized identity can be adopted by non-experts; (c) study sector-specific implementations (such as transportation, healthcare) to validate benefits and challenges in real-world ecosystems.

(III) Privacy Preserving Authentication Mechanisms: Papers on blockchain-based MFA, privacy-preserving authentication, and AI-enhanced SSI emphasize the need to combine strong authentication with data minimization [33,61]. Future research should (a) enhance zero-knowledge proof-based authentication protocols for performance and usability in constrained environments (such as IoT), (b) investigate hybrid AI-blockchain approaches for trust prediction and anonymized verification, balancing transparency with confidentiality (c) explore quantum-resistant cryptography and long-term privacy guarantees in decentralized identity and authentication schemes.

Conclusion

The rapid evolution of modern computing environments has significantly weakened traditional perimeter-based cybersecurity models. Zero Trust Architecture has emerged as an effective approach for addressing contemporary cyber threats by eliminating implicit trust and enforcing continuous verification. Within this framework, Identity and Access Management has evolved into the foundation of modern cybersecurity. Identity is increasingly becoming the new security perimeter through technologies such as MFA,

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

adaptive authentication, PAM, and behavioral analytics. Although challenges such as implementation complexity, legacy systems, and privacy concerns remain, identity-centric security models provide stronger protection against evolving cyber threats. Future cybersecurity strategies will increasingly depend on advanced IAM technologies integrated within Zero Trust frameworks.

Conflict of interest

The author declares no conflict of interest associated with this study. No funding or external influence affected the preparation and presentation of this work.

Acknowledgement

The author wishes to acknowledge the support, guidance, and encouragement received from supervisors, lecturers, colleagues, and all individuals who contributed directly or indirectly to the successful completion of this paper. Appreciation is also extended to authors and researchers whose scholarly works formed the foundation of this study.

References

1. Ejiofor OE, Olusoga O, Akinsola A. Zero trust architecture: a paradigm shift in network security. Comput Sci IT Res J. 2025;6(3):104-124. Available from: https://doi.org/10.51594/csitrj.v6i3.1871

2. Hasan M. Enhancing enterprise security with zero trust architecture: mitigating vulnerabilities and insider threats through continuous verification and least privilege access. 2024. Available from: https://doi.org/10.48550/arXiv.2410.18291

3. Azad MA, Abdullah S, Arshad J, Lallie H, Ahmed YH. Verify and trust: a multidimensional survey of zero-trust security in the age of IoT. Internet Things (Neth). 2024;27. Available from: https://doi.org/10.1016/j.iot.2024.101227

4. Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture [Internet]. Gaithersburg (MD): National Institute of Standards and Technology; 2020. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

5. Intazar M, Zohra T, Ansari NM, Iqbal R, Gul H. Beyond perimeter defenses: implementing zero-trust security models for cloud computing in the era of advanced cyber threats. Glob Res J Nat Sci Technol. 2025:3-5. Available from: https://doi.org/10.53762/grjnst.03.02.02

6. Filho WLR. The role of zero trust architecture in modern cybersecurity: integration with IAM and emerging technologies. Braz J Dev. 2025;11(1):e76836. Available from: https://doi.org/10.34117/bjdv11n1-060

7. Ruambo FA, Masanga EE, Lufyagila B, Ateya AA, Abd El-Latif AA, et al. Brute-force attack mitigation on remote access services via software-defined perimeter. Sci Rep. 2025;15(1). Available from: https://doi.org/10.1038/s41598-025-01080-5

8. Kang H, Liu G, Wang Q, Meng L, Liu J. Theory and application of zero trust security: a brief survey. Entropy (Basel). 2023. Available from: https://doi.org/10.3390/e25121595

9. He Y, Huang D, Chen L. A survey on zero trust architecture: challenges and future trends. Wirel Commun Mob Comput. 2022;2022. Available from: https://doi.org/10.1155/2022/6476274?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

10. Nahar N, Anderson K, Scheele O. A survey on zero trust architecture: applications and challenges of 6G networks. IEEE Access. 2024;12:94753-94764. Available from: https://doi.org/10.1109/ACCESS.2024.3425350

11. Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, et al. A review and comparative analysis of relevant approaches of zero trust network model. Sensors (Basel). 2024. Available from: https://doi.org/10.3390/s24041328

12. Tyler D, Viana T. Trust no one? A framework for assisting healthcare organizations in transitioning to a zero-trust network architecture. Appl Sci (Basel). 2021;11(16). Available from: https://doi.org/10.3390/app11167499

13. Alibis JAJ, Anadozie CC, Ayodele GTA. Zero trust architecture: beyond perimeter security—implementing continuous authentication and least privilege access. Int J Adv Eng Manag. 2025;7(4):829-841. Available from: https://doi.org/10.35629/5252-0704829841

14. Premsai R. Cybersecurity risks in identity and access management using an adaptive trust authenticate protocol. Int J Sci Res Eng Manag. 2023. Available from: https://doi.org/10.55041/IJSREM25645

15. Mushtaq S, Mohsin M, Mushtaq MM. A systematic literature review on the implementation and challenges of zero trust architecture across domains. Sensors (Basel). 2025. Available from: https://doi.org/10.3390/s25196118

16. Premsai R. Cybersecurity risks in identity and access management using an adaptive trust authenticate protocol. Int J Sci Res Eng Manag. 2024;8(12):1-5. Available from: https://doi.org/10.55041/IJSREM25645

17. Pal B, Daniel T, Chatterjee R, et al. Beyond credential stuffing: password similarity models using neural networks. 2019. Available from: https://doi.org/10.1109/SP.2019.00056

18. Hatunic-Webster E, Mtenzi F. Password-based authentication and phishing. Comput Sci. 2011. Available from: https://scholar.google.co.in/citations?view_op=view_citation&hl=vi&user=4mChFLoAAAAJ&citation_for_view=4mChFLoAAAAJ:9yKSN-GCB0IC

19. Thomas K, Pullman J, Yeo K, Raghunathan A, Kelley PG, Invernizzi L, et al. Protecting accounts from credential stuffing with password breach alerting. 2019. Available from: https://www.usenix.org/conference/usenixsecurity19/presentation/thomas

20. Konduru SS, Mishra S. Detection of password reuse and credential stuffing: a server-side approach. 2023. Available from: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=WURdJmMAAAAJ&citation_for_view=WURdJmMAAAAJ:u-x6o8ySG0sC

21. Vinay RM. Decoding role-based access control (RBAC). Int J Sci Res Comput Sci Eng Inf Technol. 2025;11(1):2082-2090. Available from: https://doi.org/10.32628/CSEIT251112211

22. Oluoha OM, Odeshina A, Reis O, Okpeke I, Attipoe V, Orieno OH. A unified framework for risk-based access control and identity management in compliance-critical environments. J Front Multidiscip Res. 2022;3(1):23-34. Available from: https://www.multidisciplinaryfrontiers.com/uploads/archives/20250408184820_FMR-2025-1-041.1.pdf

23. Naik N, Jenkins P. Identity management and access control trends in cloud computing. In: Proceedings of the 11th International Conference on Research Challenges in Information Science. IEEE; 2017.

24. Dammalapati PK. Understanding federated identity management: architecture, protocols and implementation. World J Adv Eng Technol Sci. 2025;15(3):401-411. Available from: https://wjaets.com/sites/default/files/fulltext_pdf/WJAETS-2025-0919.pdf

25. Pohn D, Hommel W. New directions and challenges within identity and access management. IEEE Commun Stand Mag. 2023;7(2):84-90. Available from: https://doi.org/10.1109/MCOMSTD.0006.2200077

26. Akpe OE, Kisina D, Owoade S, Uzoka IC, Ubanadu BC, Daraojimba AI. Advances in federated authentication and identity management for scalable digital platforms. J Front Multidiscip Res. 2021;2(1):87-93. Available from: https://www.multidisciplinaryfrontiers.com/uploads/archives/20250509191753_FMR-2025-1-100.1.pdf

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112

27. Ugbaja US, Nwabekee US, Owobu WO, et al. Conceptual framework for role-based network access management to minimize unauthorized data exposure across IT environments. Int J Soc Sci Except Res. 2023;2(1):211-221. Available from: https://www.allsocialsciencejournal.com/uploads/archives/20250425152138_SER-2025-2-042.1.pdf

28. Kendyala SH, Byri A, Kumar A. Implementing adaptive authentication using risk-based analysis in federated systems. 2025;12:430. Available from: https://doi.org/10.2139/ssrn.5074862

29. Dasu LS, Dhamija M, Dishitha G. Defending against identity threats using risk-based authentication. Cybern Inf Technol. 2023;23(2):105-123. Available from: https://doi.org/10.2478/cait-2023-0016

30. Vikas P. Role of identity and access management in zero trust architecture for cloud security: challenges and solutions. Int J Adv Res Sci Commun Technol. 2025:6-18. Available from: https://doi.org/10.48175/IJARSCT-23902

31. Guntaka NYR. Zero trust and cloud identity: building a resilient security framework. Int J Sci Res Comput Sci Eng Inf Technol. 2025;11(1):3450-3460. Available from: https://doi.org/10.32628/CSEIT251112368

32. Agarwal S, Mehra S, Sathar S. CHEZ PL: a hyper-extensible AI-integrated zero-trust CIAM-PAM framework for enterprise security modernization. 2025. Available from: https://arxiv.org/pdf/2501.01732

33. Rivera JD, Muhammad A, Song WC. Securing digital identity in the zero trust architecture: a blockchain approach to privacy-focused multi-factor authentication. IEEE Open J Commun Soc. 2024;5:2792-2814. Available from:

34. Ganapathi A. Zero trust evolution: advanced architectures for resilient cloud-native IAM systems. Int J Sci Res Comput Sci Eng Inf Technol. 2025;11(1):679-685. Available from: https://doi.org/10.1109/OJCOMS.2024.3391728

35. Yusop MIM, Kamarudin NH, Suhaimi NHS, et al. Advancing passwordless authentication: a systematic review of methods, challenges, and future directions for secure user identity. IEEE Access. 2025;13:13919-13943. Available from: https://doi.org/10.1109/ACCESS.2025.3528960

36. Kabanda R, Ajayi R, Michael PO. Defending against AI-driven phishing and malicious URLs. Int J Sci Res Comput Sci Eng Inf Technol. 2026;12(1):410-425. Available from: https://doi.org/10.32628/CSEIT26121314

37. Bicakci K, Varli FM, Korkmaz ME. QES-backed virtual FIDO2 authenticators: architectural options for secure, synchronizable WebAuthn credentials. 2026. Available from: https://doi.org/10.48550/arXiv.2601.06554

38. Bicakci K, Drobi A. QRAuth: a secure and accessible Web authentication alternative to FIDO2. In: Proc 16th Int Conf Information Security and Cryptology (ISCTURKEY). 2023. Available from: https://research.itu.edu.tr/en/publications/qrauth-a-secure-and-accessible-web-authentication-alternative-to-/

39. Bindel N, Cremers C, Zhao M. FIDO2, CTAP 2.1, and WebAuthn 2: provable security and post-quantum instantiation. 2023. Available from: https://doi.org/10.1109/SP46215.2023.10179454

40. Barbosa M, Boldyreva A, Chen S. Provable security analysis of FIDO2. Lect Notes Comput Sci. 2021:125-156. Available from: https://par.nsf.gov/servlets/purl/10319868

41. Jimmy F. Zero trust security: reimagining cyber defense for modern organizations. Int J Sci Res Manag. 2022;10(4):887-905. Available from: https://doi.org/10.18535/ijsrm/v10i4.ec11

42. Phanireddy S. AI-driven identity access management (IAM). Int J Sci Res Eng Manag. 2021;5(6):1-9. Available from: https://doi.org/10.55041/IJSREM8931

43. Vitla S. The future of identity and access management: leveraging AI for enhanced security and efficiency. 2024. Available from: https://doi.org/10.32996/jcsts.2024.6.3.12

44. Oyebode O. Explainable deep learning integrated with decentralized identity systems to combat bias, enhance trust, and ensure fairness in algorithmic governance. World J Adv Res Rev. 2024;21(2):2146-2166. Available from: https://doi.org/10.30574/wjarr.2024.21.2.0595

45. Aboukadri S, Ouaddah A, Mezrioui A. Machine learning in identity and access management systems: survey and deep dive. Comput Secur. 2024;139:103729. Available from: https://doi.org/10.1016/j.cose.2024.103729

46. Sunil V, Grandhi K. Identity and access management transformation in large enterprises: a case study analysis. 2025. Available from: https://doi.org/10.32996/jcsts.2025.7.5.42

47. Bommareddy AR. Strengthening cybersecurity resilience in federal financial systems through zero-trust architectures. 2025.

48. Sunkara G. Implementing zero trust architecture in modern enterprise networks. SAMRIDDHI. 2025;17(3):1-11.

49. Owobu WO, Abieba OA, Gbenle P. Review of enterprise communication security architectures for improving confidentiality, integrity and availability in digital workflows. Int J Adv Multidiscip Res Stud. 2024;4(6):1417-1426. Available from: https://doi.org/10.62225/2583049X.2024.4.6.4024

50. Dakić V, Morić Z, Kapulica A. Analysis of Azure zero trust architecture implementation for mid-size organizations. J Cybersecur Priv. 2025;5(1). Available from: https://doi.org/10.20944/preprints202407.1454.v1

51. Fadare KO. Optimizing data center security with zero trust architecture. Int J Eng Adv Technol Stud. 2025;13(3):71-96. Available from: https://doi.org/10.37745/ijeats.13/vol13n37196

52. Dotse SK, Sebuabe SY, Obeng A. Zero trust architecture implementation in enterprise networks: evaluating effectiveness against cyber threats. Int J Comput Appl. 2025. Available from: https://doi.org/10.5120/ijca2025925740

53. Srinivas K, Rasveen, Kavitha. Evaluating the effectiveness of zero-trust architectures in modern cyber security. In: Proceedings of the Institute of Electrical and Electronics Engineers (IEEE). 2025. p. 1-5. Available from: https://doi.org/10.1109/ICSIT65336.2025.11294850

54. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput Secur. 2022;122:102911. Available from: https://doi.org/10.1016/j.cose.2022.102911

55. Chiagozie UV. From legacy to zero-trust: migration strategies, cost-benefit analysis, and security gains in mid-sized enterprises. 2024. Available from: https://orcid.org/0009-0005-7719-723X

56. Rajesh RN. Zero-trust architecture: redefining enterprise security paradigms. World J Adv Res Rev. 2025;26(2):968-977. Available from: https://doi.org/10.30574/wjarr.2025.26.2.1684

57. Raza MdA, Hossain MA, Mahjabeen F. Evaluating the human factor in bank cybersecurity: strategies for improving employee awareness and reducing insider threats. Indones J Adv Res. 2025;4(1):1-20. Available from: https://doi.org/10.55927/ijar.v4i1.13399

58. Ayanbode N, Abieba OA, Chukwurah N. Human factors in fintech cybersecurity: addressing insider threats and behavioral risks. Int J Multidiscip Res Growth Eval. 2024;5(1):1350-1356. Available from: https://doi.org/10.54660/.IJMRGE.2024.5.1.1350-1356

59. Jimmy F. AI-driven identity and access management: opportunities, challenges, and future directions. Journal. 2025;8:2. Available from: https://doi.org/10.60087/jaigs.v8i02.418

60. Ghafir I, Saleem J, Hammoudeh M. Security threats to critical infrastructure: the human factor. J Supercomput. 2018;74(10):4986-5002. Available from: https://doi.org/10.1007/s11227-018-2337-2?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

61. Čučko Š, Turkanović M. Decentralized and self-sovereign identity: systematic mapping study. IEEE Access. 2021;9:139009-139027. Available from: https://doi.org/10.1109/ACCESS.2021.3117588

Citation: Onchoka KN, Bosire ZO, Kemei PK. Identity as the New Security Perimeter: The Evolution of Identity and Access Management within Zero Trust Architecture. Trends Comput Sci Inf Technol. 2026;11(2):68-79. Available from: https://dx.doi.org/10.17352/tcsit.000112