Journal of Electrical Systems and Information Technology

REVIEW Open Access

The significance of artificial intelligence in zero trust technologies: a comprehensive review

Deepa Ajish[1*]

*Correspondence: deepajish@gmail.com

[1] Security and Compliance, ServiceNow Automation, MUFG Bank, Ltd., Los Angeles, CA, USA

Abstract

In the era of cloud computing, cybersecurity has assumed paramount importance. As organizations transition to cloud-based solutions, cyberattackers increasingly target cloud services as a lucrative avenue for unauthorized access to sensitive information. The traditional security perimeter, once robust, now exhibits porosity, necessitating a reevaluation of security strategies to counter these evolving threats. This paper delves into the critical role of artificial intelligence (AI) within zero trust security technologies. The convergence of AI and zero trust has garnered significant attention, particularly in the domains of security enhancement, risk mitigation, and the redefinition of trust paradigms. My exploration aims to uncover how AI actively observes and supports various technologies in zero trust model. By evaluating existing research findings, I illuminate the transformative potential of AI in fortifying security within zero trust security models. This scholarly perspective underscores the critical interplay between AI and zero trust technologies, highlighting their collective potential in safeguarding digital ecosystems.

Keywords: Artificial intelligence, Cloud security, Cybersecurity, Zero trust

Introduction

Cloud applications and platforms have revolutionized information technology (IT) by offering flexibility, scalability, and efficiency. Whether building web apps, analyzing data, or deploying enterprise solutions, the cloud provides a powerful foundation for modern businesses. The rise of cloud computing has significantly transformed the way businesses operate and deliver services. According to a Gartner study, the global cloud computing market is poised to reach a staggering US$679 billion in 2024 [24]. Gartner also forecasts that it is anticipated that by the year 2027, industry cloud platforms will be utilized by over 70% of enterprises as a strategy to expedite their business objectives. This is a significant increase from the less than 15% of enterprises that are projected to use these platforms in 2023 [24]. As enterprises increasingly allocate their IT budgets to public cloud services, the momentum toward cloud adoption persists, especially following the impact of COVID-19 from 2020 through 2024. In contrast to conventional on-premises data centers, cloud systems possess

the capability to dynamically scale up or down as required. This elasticity enables companies to effortlessly handle growth, adapt to fluctuating workloads, and maintain agility in a swiftly changing technological environment [2, 49]. Additionally, the cloud's capacity to deliver consistent updates for both software and hardware ensures that businesses remain up-to-date and efficient in their operations [1, 49].

As more organizations transition to cloud-based solutions, cyberattackers have shifted their attention [1]. They now perceive cloud services as a highly profitable target [1]. According to research by check point, cloud-based cyberattacks surged by nearly 48% in 2022 compared to the previous year [52, 54]. With the increasing adoption of cloud platforms, it is significant to move away from the traditional security structure based on the perimeter. Once the attacker is within the network, there is unrestricted lateral movement, which could cause a lot more damage. Additionally, there are more security risks associated with cloud platforms. Hackers often target cloud services to gain unauthorized access to sensitive information. The vast amount of data stored by cloud service providers (CSPs) makes them prime targets for data breaches. Medical records, financial data, and customer information could be at risk [42]. Cloud computing has blurred the boundaries, making it challenging to secure the perimeter around data centers. The ever-changing cloud environment can lead to an unmanaged attack surface, leaving vulnerabilities open [42].

The cloud environment is not immune to data loss, which can be a consequence of inadvertent erasure or system malfunctions. Cloud security emerges as a critical discipline within the broader field of cybersecurity. Cloud security encompasses a comprehensive set of measures designed to protect cloud-based resources. These resources include not only applications and data but also the underlying infrastructure. This protective shield involves a synergy of technologies, policies, services, and security controls [26]. Their collective purpose is to safeguard an organization's sensitive information, applications, and digital ecosystems.

Given the prevailing threat landscape, it becomes evident that a trust-oriented authorization mechanism is essential within a cloud network environment. This mechanism actively observes and supports various nodes within the network [28]. To mitigate uncertainties (as complete elimination is impossible), the emphasis lies on robust authentication and authorization, along with the reduction of implicit trust boundaries. Simultaneously, efforts are made to maintain system availability and minimize temporal delays in authentication processes. Access rules are meticulously crafted to enforce the least privileges necessary for executing the requested actions [25].

In reaction to the escalation in significant security violations, an executive order was promulgated by the American President in May 2021. This decree obliges U.S. Federal Agencies to incorporate the Zero Trust (ZT) principles delineated in the NIST Special Publication 800-207 as an essential constituent of their ZT security approach [41]. Consequently, this standard underwent rigorous validation and received substantial input from diverse stakeholders, including commercial customers, vendors, and government agencies. As a result, numerous private organizations now regard it as the de facto standard for securing their enterprise environments [40]. These principles emphasize the need for continuous monitoring, dynamic authentication, and the use of

collected data to improve security. These data can also be used to provide context for access requests from subjects [25].

In recent years, the intersection of artificial intelligence (AI) and ZT technologies has garnered significant attention from researchers, practitioners, and policymakers alike. This paper aims to delve into the critical role that AI plays within the context of ZT security models. By synthesizing existing research findings and analyzing online resources, I explore the multifaceted impact of AI on enhancing security, mitigating risks, and redefining trust paradigms.

Zero trust model

A zero trust architecture (ZTA) represents a paradigm shift in enterprise cybersecurity strategy, grounded in the principles of zero trust. Its primary objective is to forestall data breaches and restrict internal lateral progression. Rather than being a monolithic architecture, zero trust (ZT) embodies a collection of guiding tenets applicable to workflow, system design, and operations. These principles can be employed to enhance the security stance of systems across all classifications and sensitivity levels. The concept of ZT in cybersecurity has evolved, emphasizing a fundamental shift in how we approach security. It is based on the concept-never trust, always verify [30]. Rather than assuming that everything within the corporate firewall is secure, the ZT model operates under the assumption of a breach and rigorously verifies each request as if it were coming from an open network [46]. In 2010, an analyst from Forrester Research Inc. introduced the term "Zero Trust" while presenting the conceptual model. Subsequently, Google disclosed the implementation of ZT security within their network, leading to heightened interest in ZT adoption across the technology community [15]. The ZT model fundamentally shifts the security paradigm by assuming that no network boundary is inherently secure. Whether users operate within or outside the organization's network, they must undergo rigorous authentication, authorization, and continuous validation. ZT acknowledges the absence of a traditional network edge, recognizing that resources can reside anywhere—on-premises, in the cloud, or hybrid environments. This framework aligns with the challenges posed by remote workforces, hybrid cloud architectures, and the ever-evolving threat landscape. It enforces security policies based on context. It relies on least-privileged access controls and rigorous user authentication to establish a robust security posture.

ZT fundamentally works with the principles specifically aligned with the NIST 800-207 guidelines:

- *Continuous verification* It means always verify access—regardless of the user's location or the resource they seek. This perpetual validation ensures that only authorized entities gain entry.
- *Limiting the blast radius* In the event of an external or insider breach, zero trust aims to minimize impact. By compartmentalizing access and segmenting resources, the potential fallout from a security incident is contained.
- *Automated context collection and response* Zero trust doesn't rely on guesswork. Instead, it incorporates behavioral data from across the entire IT stack—identity,

endpoints, workloads, and more. This holistic context informs precise responses to security events.

In the zero trust model (ZTM), the principle of context collection and response plays a pivotal role. This principle emphasizes the importance of gathering real-time context about a user's or system's behavior, such as device information, user attributes, and network conditions. Context is an essential element in the ZTM as it helps make informed decisions [48]. For instance, when a device tries to access financial data on a network, context is needed to determine if this is an employee or a threat [48]. The device's location, the user's identity, and the data they are accessing provide valuable information. However, what's missing is whether that employee should have access to that specific data, from that particular device or location [48]. This missing piece is the context. It will be an incomplete picture of risk without context, which means different teams may interpret and respond to this request differently [48].

Another significant development in the realm of zero trust security is the release of the zero trust maturity model (ZTMM) by the Cybersecurity and Infrastructure Security Agency (CISA) in the USA. This model provides a structured approach to assessing and advancing an organization's zero trust capabilities [14].

The ZTMM is organized into five key pillars, each representing a critical aspect of zero trust implementation [14]:

- *Identity* This pillar focuses on identity management, authentication, and authorization. It aims to ensure that only authorized users and devices can access resources.
- *Device* The device pillar emphasizes securing endpoints and managing their trustworthiness. It includes measures to protect against compromised devices and unauthorized access.
- *Network/environment* Here, the focus is on network segmentation, microsegmentation, and network visibility. Organizations must carefully control network access and monitor traffic.
- *Application/workload* This pillar addresses application security and workload protection. It involves securing applications, APIs, and workloads against threats.
- *Data* Protecting sensitive data are crucial. The data pillar emphasizes data classification, encryption, and access controls. Within each pillar, several common elements contribute to achieving zero trust maturity, refer Fig. 1 [14].
- *Visibility and analysis* Organizations must have comprehensive visibility into their network, devices, and user behavior. Analyzing thes data helps identify anomalies and potential security risks.
- *Automation and orchestration* Automation streamlines security processes, while orchestration ensures coordinated responses to security incidents. These practices enhance efficiency and reduce manual effort.
- *Governance* Effective governance involves policies, procedures, and accountability. Organizations need clear guidelines for implementing and maintaining zero trust practices.

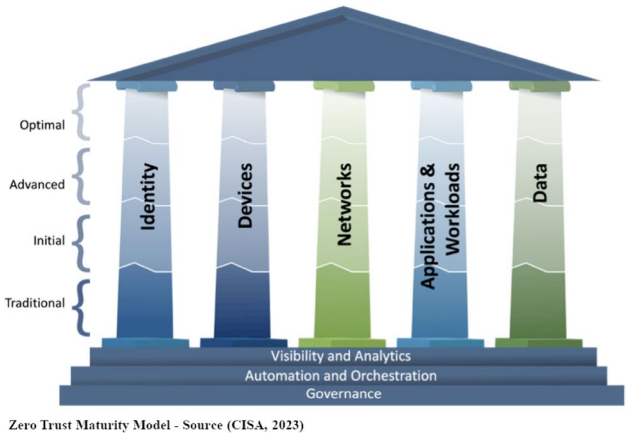

Fig. 1 Five pillars of zero trust maturity model. Identity describes attributes uniquely identifying an agency user or entity, including nonperson entities. Device encompasses assets (hardware, software, and firmware) capable of network connection. Network is an open communications medium, including internal networks, wireless networks, and the Internet. Applications and workloads refer to systems, programs, and services executed across different environments. Data include structured and unstructured files residing in systems, devices, networks, and backups. Each pillar also supports Visibility and Analytics, Automation and Orchestration, and Governance. Visibility and Analytics refers to the observable artifacts resulting from enterprise-wide events and cyber-related data analysis. Automation and Orchestration is utilization automated tools and workflows for security response functions while maintaining oversight and security. Governance enforces cybersecurity policies and processes across pillars to manage risks. The maturity levels are categorized into four. Traditional is about manually configured lifecycles, static security policies, and manual response and mitigation. Initial is the starting of automation of attribute assignment, configuration of lifecycles, policy decisions, and enforcement with initial cross-pillar solutions. Advanced is applicable automated controls for lifecycle and configuration assignment, with cross-pillar coordination. Optimal refers to fully automated, just-in-time lifecycles and attribute assignments based on automated/observed triggers.

Literature review

The digital transformation of our global society is driving an unprecedented increase in connectivity. This phenomenon is largely attributable to recent technological trends such as cloud computing, the Internet of Things (IoT), and Bring Your Own Device (BYOD) policies [39]. The digitalization of our world and the associated growth of network infrastructures are resulting in complex new network security requirements [13, 16]. Meeting these requirements necessitates a rethinking of existing security strategies and the development of innovative solutions capable of addressing the dynamic and complex nature of modern cyber threats.

In 2010, Kindervag 35, an analyst at Forrester Research, proposed the concept of the zero trust network architecture and the method to implement it in practical environments [35]. In 2020, [40] summarized existing basic ZTA schemes and proposed fundamental logical components for ZTA. The focus was primarily on the practical implementation of ZT, emphasizing its realization in real-world environments [40].

ZT represents a paradigm shift in cybersecurity methodologies, transitioning from a focus on location-based strategies to a more data-oriented approach. This shift facilitates enhanced security controls among users, systems, data, and assets, accommodating the dynamic nature of these elements [10].

Before the advent of the ZT model, the prevailing presumption among cybersecurity experts was that all data and transactions within the network perimeter were inherently trustworthy 5. Kindervag says ZT, as a cybersecurity strategy, is designed to rectify the

shortcomings of conventional perimeter-based models. It specifically targets insider threats within an internal network through a process known as de-perimeterization [36]. According to Kang et al. [33], this process signifies a shift that diminishes or even eradicates the network perimeter, thereby securing the system through a continuous verification methodology. This approach authenticates each device, user, transaction, and data flow throughout the entire access procedure [33].

He et al. [29] say the fundamental objective of the ZT model is to facilitate secure access for users in untrusted network zones to reach trusted areas. This is achieved through a combination of authentication and policy control mechanisms [29].

In ZTA, context collection and response involve gathering behavioral data and context from the entire IT stack, which includes identity, endpoint, workload, etc., for the most accurate response [17]. This process helps to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services [14]. The department of defense (DoD) and the national security agency (NSA) have developed a ZT reference architecture that provides a comprehensive framework for implementing ZTA [20]. They organized ZTA into 5 pillars and each of the pillars plays a role in context collection and response. For example, the identity pillar involves verifying the identity of every user and device trying to access resources in the network [14]. The devices pillar involves ensuring that all devices used to access resources are secure [14]. The networks pillar involves segmenting the network to prevent lateral movement of threats [14]. The applications and workloads pillar involves securing applications and their workloads [14]. The cross-cutting capabilities pillar involves capabilities that span across multiple pillars [14]. By automating context collection and response, ZTA aims to limit the "blast radius" and minimize the impact if an external or insider breach does occur [17].

In their 2021 work, Ramezanpour and Jagannath [44] introduced an intelligent zero trust architecture (i-ZTA). The i-ZTA leverages modern AI algorithms for intelligent detection, evaluation, and decision-making. Specifically, reinforcement learning is used in the policy enforcement point (PEP) to maximize guaranteed scores and joint learning is applied in the policy decision point (PDP) to provide context-aware scores to users 44.

According to Mohammed [38], when AI and identity access management (IAM) are integrated with effective monitoring and reporting tools, organizations can gain insights into connectivity patterns. By implementing intelligent and adaptive rules for identity and access management, they can proactively reduce the risk of security breaches [38].

The literature review conducted herein serves as a beacon, guiding me through the intricate landscape where AI and ZTA technologies converge.

Methodology

A framework for conducting a comprehensive literature review was established. This framework served as the guiding compass, ensuring systematic exploration. Existing research studies and scholarly papers formed the bedrock of the investigation. To curate a diverse set of insights, a paper selection strategy was devised. The criteria encompassed relevance, language, and experimental focus. Papers related to zero trust architecture (ZTA) and AI-driven ZT approaches were collected, while papers not published in English were excluded to maintain consistency and accessibility. Irrelevant studies that did not directly address ZT were pruned. Papers that conducted empirical studies on

ZTA were prioritized. To meaningfully contribute to this critical domain, papers and articles that significantly advanced the understanding of AI's role in ZT were chosen.

AI in identity access management (IAM)

The fundamental tenets for realizing ZTA encompass both authentication and access control. These elements serve as the mechanisms through which a user's identity is verified and their permissions are determined for executing various operations on safeguarded resources.

The objective of this verification is to facilitate the user's shift from an unidentified to an identified state. In the swiftly advancing field of cloud computing, the importance of sturdy IAM systems has been significantly heightened due to the rise in cybersecurity threats and the intricate characteristics of digital identities [11].

As data breaches and complex cyber threats become more prevalent, organizations are seeking innovative solutions to bolster their IAM strategies. One such revolutionary technology that is gaining traction in this domain is AI, a sophisticated variant that enables machines to learn, adapt, and generate new data. AI is increasingly crucial in IAM as it gains prominence in cloud computing. Its influence extends to the training and deployment of enerative AI (GenAI) models, leading to a transformation of the IAM landscape. This includes the implementation of automated policy generation and the enhancement of security measures [7].

The intricacies of network interaction become evident, thereby empowering IT departments to implement astute administrative measures and make more enlightened decisions regarding user licenses [38]. IAM is founded on four key pillars: Authentication, Authorization, Administration, and Audit. Each pillar plays a vital role in creating a secure and efficient access management system.

1. *Authentication*

   Authentication is concerned with verifying the identities of users, ensuring that only valid individuals gain access to the system.

   1.1 *Adaptive and continuous user authentication* This method continuously monitors user behavior throughout a session and asks to re-authenticate in the event of anomaly detection. The lifecycle of continuous authentication systems commences with modeling users' behavior during their interactions with their devices over a specific time frame. Once the data is collected, it undergoes preprocessing and is stored in a dataset containing relevant information about user behavior patterns. To create an accurate dataset for a user's profile, careful selection of characteristics or features from various dimensions of the devices such as sensors, applications, communications, screen gestures, etc. is crucial. Finally, the last step involves comparing current usage with the well-established user behavior stored in the dataset [32]. AI can enable adaptive and continuous user authentication by combining with behavioral biometrics, anomaly detection, and user and entity behavior analytics (UEBA). Figure 2 shows the steps in AI-driven adaptive and continuous user authentication. The

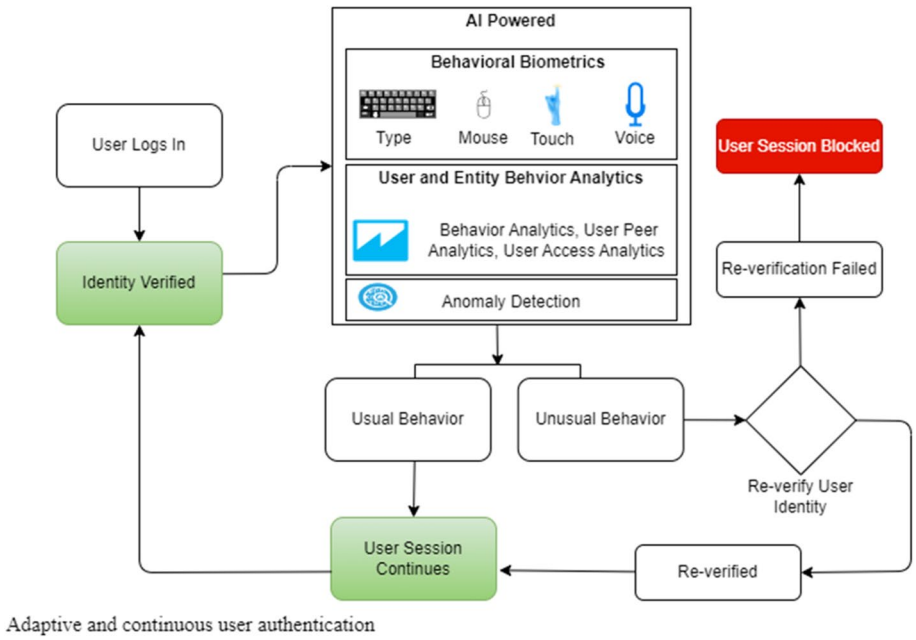

Fig. 2 Adaptive and continuous user authentication. When a user logs in, the identity is verified and the AI-powered system continuously monitors the user behaviors. Behavioral biometrics detects subtle differences in how a person types, clicks mouse, holds their phone, or interacts with touchscreens. User and Entity Behavior Analytics (UEBA) analyzes data from all possible enterprise sources like firewalls, routers, virtual private networks (VPN), identity access management solutions, antivirus, anti-malware software, endpoint detection and response (EDR), security information and event management (SIEM), active directory, and threat intelligence feeds. The anomaly detection system identifies suspicious deviation from the baseline in real time and asks for re-verification of user identity. User logged in and triggered anomaly detection. System prompted for re-verification and the user failed to re-verify and the system blocks the user session.

IAM system can persistently evaluate user behavior and dynamically modify authentication requirements based on risk levels, ensuring a balance between security and user convenience. Furthermore, the UEBA solution employs behavioral analysis to establish connections between seemingly unrelated activities, thereby proactively preventing attacks before any harm or lateral movement occurs [6].

1.2 *Voice and speech recognition* Voice authentication is a biometric technology that verifies users based on their distinctive voice characteristics. The AI can learn and distinguish individual users' voices, enhancing the accuracy of voice-based authentication and making it more resistant to spoofing attempts. AI and ML have the capacity to process vast datasets and enhance efficiency by autonomously learning and adapting to environmental shifts [37]. For instance, machines can be trained to discern various accents, dialects, contexts, and emotional cues. Additionally, they can effectively handle intricate and diverse data, which is essential for tasks like data mining and machine learning [8].

1.3 *Facial recognition* Facial recognition is a method of identifying human faces using technology and biometrics, often by mapping facial features from photographs or videos. The system then compares this information with a database of known faces to determine a match. Facial recognition is widely

deployed, from airports and cellphones to classrooms, social media platforms, and businesses. Notably, some organizations have replaced traditional security badges with facial recognition systems [43]. AI can construct sophisticated facial recognition systems and it can generate and analyze facial data, enabling the identification and authentication of users based on their unique facial features.

1.4 *AI-driven anomaly detection* AI-driven anomaly detection identifies data irregularities that deviate from the norm using artificial intelligence and machine learning algorithms, thereby enhancing security. ML-based anomaly detection leverages unlabeled data to learn patterns. Techniques such as k-means clustering, isolation forest, and one-class support vector machines (SVM) identify anomalies and flag deviations from normal behavior as potential threats. In the realm of online security, AI-driven models and algorithms play a crucial role in detecting and responding to threats proactively [4]. The AI system can continuously monitor user behavior and identify unusual patterns indicating potential security threats or compromised accounts.

2. *Authorization*

Authorization determines the extent of access each authenticated user is allowed, ensuring they can only access resources pertinent to their roles and responsibilities. AI can be effectively utilized for user authorization and role-based access controls (RBAC) in IAM deployments within organizations. AI in these areas amplifies access management, optimizes role assignments, and enhances overall security. Here's how AI is amplifying the user authorization and RBAC in IAM:

2.1 *Intelligent role assignment* It involves dynamically assigning roles to users based on contextual factors, enhancing access management and security. AI can smartly analyze historical access data and user behavior to propose role assignments. The AI system can discern patterns and similarities among users with analogous job functions, facilitating more precise and efficient role provisioning.

2.2 *Automated role-based access controls* RBAC is a method for managing access to systems, networks, or resources by assigning permissions based on an individual's role within an organization. In RBAC, employees are granted access only to the information relevant to their job responsibilities. The emergence of new identity types such as machines, devices, APIs, applications, and microservices has necessitated the development of sophisticated access control methods. Traditional RBAC solutions heavily rely on manual role discovery and modeling. However, this manual approach faces significant challenges in keeping up with the ever-evolving landscape of identities in today's dynamic business environments. Frequent employee role changes and organizational shifts contribute to this complexity.

The repercussions of relying solely on manual RBAC processes include overprovisioned access, orphaned accounts, and the insidious phenomenon known as entitlement creep—all of which exacerbate both insider and external security threats. While RBAC theoretically ensures that access is restricted to

authorized individuals, achieving a ZTA using manual processes and static data is exceptionally difficult due to the inherent pitfalls.

AI-driven RBAC approach involves leveraging AI to discover and analyze role access patterns across the entire enterprise. By doing so, it identifies high-risk roles and role combinations, defines high-quality roles based on robust access patterns, customizes risk criteria, and provides role recommendations and impact analysis. In essence, AI-driven RBAC paves the way for achieving a more secure and adaptive access control framework in the context of ZT.

2.3 *Continuous role reviews* AI systems have the capability to constantly monitor user behavior as they navigate through a network, adhering to their authorized access rights [12]. However, these systems also possess the ability to detect anomalous, illogical, or unpredictable behavior [12]. For instance, they can identify instances where users venture into system sections they wouldn't typically visit or retrieve an unusually high number of files compared to their usual patterns. The AI system can automatically initiate role reviews when it detects anomalies or changes in user behavior, ensuring that access permissions remain current and aligned with users' responsibilities.

2.4 *Role mining and optimization* Role Mining plays a pivotal role in the context of RBAC. Its primary objective is to effectively determine roles within an enterprise by leveraging the permissions already assigned to users. By doing so, it assists IT administrators in enhancing cybersecurity by addressing the issue of users having access privileges beyond their job requirements.

The process of role mining leveraging AI-based techniques, particularly those rooted in ML can identify potential role hierarchies and dependencies. Through these methods, organizations can identify and categorize various business roles along with their associated access privileges and resource entitlements. The AI system can analyze access patterns and user attributes to suggest optimizations, such as merging or splitting roles to reduce role clutter and bolster security.

2.5 *Dynamic access controls* AI-powered dynamic access control, which takes contextual factors into account, enables access control decisions based on several critical parameters. These include the user's geographical location, the time of day, and the specific device they are using. The AI can dynamically adjust access permissions based on user actions and contextual factors, ensuring that users have the appropriate level of access at any given moment.

3. *Administration*

Administration involves the effective management of user accounts, roles, and access privileges, reducing the complexity of IAM for IT administrators. Here's how AI can be employed to automate identity administration in IAM:

3.1 *Automated user de/provisioning* De-provisioning, a crucial process in IAM, involves revoking privileges or access from user accounts. This action is prompted by various factors, including internal employee transfers, departures, or security threats. During de-provisioning, accounts may be disabled or entirely

deleted. Additionally, users are removed from any groups or roles they were associated with.

The integration of AI-driven de-provisioning has significantly transformed this process. By automating access adjustments, AI minimizes manual tasks and reduces the risk of human error. AI can power self-service user management portals, enabling employees to request access, update their profiles, or reset passwords without human intervention. The AI can process these requests, verify their legitimacy, and automatically fulfill them when appropriate.

3.2 *Access request automation* AI-powered systems can dynamically apply IAM policies, taking into account user-specific requirements and constraints. By doing so, they alleviate the burden on IT professionals who would otherwise manually determine the "least privilege" for each use case [23, 38].

The ZT principle of least privilege—where users are granted only the minimum permissions necessary to perform their tasks—is crucial for security. AI-driven IAM policies ensure that access is precisely tailored, enhancing both efficiency and security.

AI can automate authentication for low-risk access scenarios by closely monitoring user activity patterns. As a result, certain IAM management tasks are alleviated, while simultaneously safeguarding users from experiencing "security fatigue." [31].

3.3 *Intelligent user profile management* User profiling involves deducing hidden information about users based on observable data related to their actions or verbal expressions [56]. In adaptive systems, the user profile serves to customize behavior according to individual users [9]. AI can build intelligent user profiles based on historical behavior and access patterns and these profiles assist in making data-driven decisions regarding access rights and security policies.

4. *Auditing, governance, and compliance*

The audit entails the continuous monitoring and recording of access events to detect potential security risks, enforce compliance, and maintain a comprehensive record of user activities. Here's how AI can be employed to automate governance and compliance for IAM:

4.1 *Access policy management* AI can analyze access policies and historical access data to discern patterns and anomalies. Based on this analysis, AI can suggest updates or optimizations to access policies, ensuring that permissions align with the principle of least privilege and compliance requirements.

4.2 *Automated access reviews* AI-driven access reviews facilitate compliance maintenance, mitigate persistent privileges, and enhance security without requiring manual intervention. These reviews offer valuable insights, including usage patterns, risk assessments, and indicators related to job roles and departments, aiding in informed review decisions. Additionally, the system automatically approves low-risk access and handles access de-provisioning. Comprehensive reports, access certification outcomes, and remediation

activities are meticulously tracked and readily available for auditors through streamlined reporting.

4.3 *Privileged Access Management (PAM)* AI and ML have the capability to analyze and learn from the login patterns of privileged users. By establishing a baseline of normal behavior, these technologies can identify anomalies that may signal security risks. One of the most impactful applications of AI and ML in PAM lies in their predictive abilities. By scrutinizing historical data and detecting patterns, they can forecast potential security threats before they materialize, empowering organizations to proactively address them. Within a PAM framework, AI can optimize and secure privilege elevation and delegation processes. Additionally, an effective PAM solution should incorporate risk scoring based on individual user behavior and historical context. Real-time analysis of access requests allows for adaptive decision-making beyond rigid rules. Furthermore, AI can seamlessly integrate with threat intelligence feeds, bolstering PAM solutions' capacity to identify and respond to emerging threats.

4.4 *Continuous compliance monitoring* Continuous compliance monitoring is a systematic process that involves ongoing scanning, monitoring, and assessment of security and compliance standards across an organization's IT infrastructure. This practice ensures that the organization consistently adheres to regulatory requirements and industry best practices. AI-driven tools can process vast datasets against ever-changing regulations. These advanced algorithms enhance accuracy, efficiency, and adaptability, ensuring businesses remain compliant. Identity verification tools enhance accuracy and efficiency in screening and monitoring customer activities.

4.5 *Adaptive compliance responses* AI-driven systems are not static; they adapt and learn [45] by analyzing compliance data and trends, these systems continuously enhance and can recommend changes to access policies or authentication requirements based on evolving compliance regulations or security best practices.

4.6 *Automated audit trail generation* AI can generate detailed audit trails for IAM activities, helping organizations maintain comprehensive records of access events and changes. This automated audit trail generation simplifies compliance reporting and reduces the administrative burden on IT teams.

4.7 *Predictive compliance analysis* Predictive compliance analysis, empowered by AI, leverages historical compliance trends to offer predictive analytics regarding potential future compliance risks. By anticipating critical areas of concern, AI proactively recommends measures to ensure continuous compliance.

AI in multi-factor authentication (MFA)

MFA enhances security by introducing additional layers of verification. In addition to a basic authentication method (such as a password), MFA involves sending a onetime password (OTP) to the user's email or mobile device. This OTP generates a time-based code, ensuring that at least two factors have been successfully verified [50]. MFA involves various authentication principles applied to the login process of a system

through multiple devices by gathering enough evidence to verify a user is who they claim to be [50].

Adaptive MFA (AMFA)

AMFA is a method for using contextual information and business rules to determine which authentication factors to apply to a particular user in a particular situation. Adaptive authentication is often used in conjunction with MFA and single sign-on (SSO) solutions. AI-powered AMFA solutions monitor user activity over time to identify patterns, establish baseline user profiles, and detect anomalous behavior. Adaptive authentication considers the following factors:

- *Device profile* It examines the system from which the request originates.
- *Location awareness* This involves assessing the request's source, including whether it comes from an IP address range associated with risk or from a potentially risky country.
- *User behavior* Understanding the purpose behind the user's access to servers, applications, or data [18]. AMFA assigns risk scores to suspicious events and adjusts authentication factors in real time based on administratively defined policies.
- *Low-risk behavior* Users can authenticate using only their username and password.
- *Medium-risk behavior* Users need an additional SMS code for authentication.
- *High-risk behavior* Users must provide further information to complete authentication and proceed to authorization.

Figure 3 depicts the steps in AMFA. AMFA serves the fundamental purpose of enhancing enterprise security by allowing access only to authorized users for business applications and data. Notably, it minimizes challenges for users who exhibit expected behavior patterns [53].

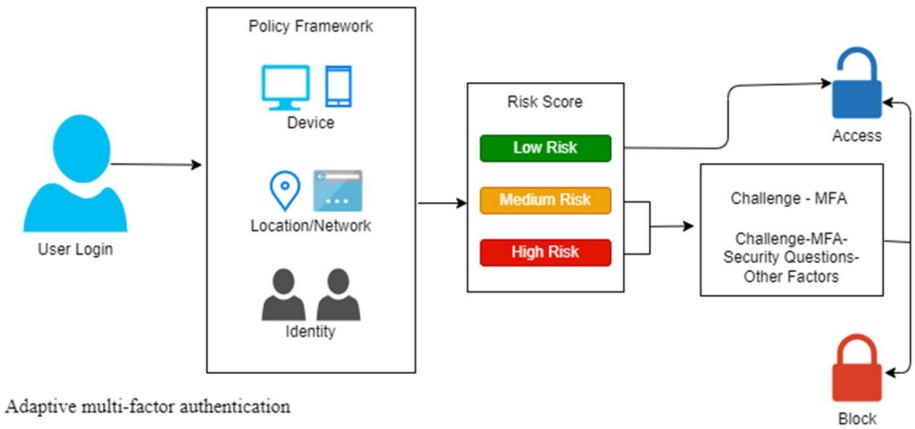

Fig. 3 Adaptive multifactor authentication. When a user logs in, the system examines the device from which the request originated, the request's location, the IP address associated with the request, and the purpose of the request. System compares this data against the baseline user profile, and generates risk scores. If the behavior is low-risk, the system permits login using a username and password. For medium-risk behavior, the system prompts for additional SMS code authentication. In cases of high-risk behavior, the system seeks further information. User logged in with low-risk behavior, medium-risk behavior, and attempted with high-risk behavior. User failed to provide additional details and access is blocked.

AMFA strengthens the ZT model by:

- *Contextual verification* It assesses factors such as device profiles, location awareness, and user behavior. ZT assumes that attackers may exist both within and outside the network perimeter. AMFA helps prevent unauthorized access even if valid credentials are compromised. By continuously verifying identity, it minimizes the impact of compromised accounts.
- *Risk-based authentication* Based on risk scores, it dynamically adjusts authentication requirements.
- *Biometric and token authentication* These factors bolster identity verification.
- *Location-agnostic access* Regardless of user location or network origin, AMFA ensures secure access to services.
- *Scalability and cloud readiness* AMFA adapts seamlessly across various endpoints, including cloud-based machines, software as a service (SaaS) applications, and personal devices.

AI in endpoint protection

Endpoint detection and response (EDR) is a cybersecurity technology engineered to monitor and safeguard endpoints. Endpoints refer to physical devices such as mobile phones, laptops, Internet of Things (IoT) devices, corporate workstations, or point-of-sale terminals. Contrary to web endpoints, which pertain to specific URLs or web addresses, EDR concentrates on the security of physical devices.

EDR assumes a critical role in identifying and responding to potential threats by offering detailed security incident detection and investigation capabilities. It aids in pinpointing and rectifying security incidents effectively, ensuring the comprehensive safety of an organization's endpoints [34]. In the prevailing work-from-home conditions, the complexity of EDR has escalated. With a transition from on-premise computing and conventional corporate networks toward hybrid, managed, or cloud-based services, the risks associated with hacking and malware insertion have become more conspicuous and challenging to trace.

AI has already been integrated into numerous cybersecurity platforms, facilitating effective threat detection and protection [34]. Specifically, EDR serves as an optimal data collection point, enabling AI algorithms to ascertain if actions deviate from the norm. Data analysis assumes a pivotal role in EDR, assisting in establishing a baseline for normal behavior and augmenting behavioral analysis to identify anomalies. AI can also aid in mitigating human errors, as individuals are often the most vulnerable link when safeguarding against cyberattacks. Consolidating the information across multiple systems further enhances the accuracy of AI components for superior precision in identifying anomalous events and eliminates false positives, thereby reducing alert fatigue for the IT administrator or cyber analyst. The fundamental capabilities of EDR include:

- *Continuous endpoint data collection* EDR solutions meticulously record and store behavioral data from endpoints. This continuous data collection enables retrospective analysis, aiding in threat detection and incident investigation. By

capturing endpoint behaviors, EDR solutions create a rich dataset for subsequent analysis. AI and machine learning algorithms can ingest more datasets and can lead to faster breach detection.

- *Real-time analysis and threat detection* EDR tools employ advanced analytics techniques to scrutinize endpoint activities in real time. Suspicious patterns, anomalies, and indicators of compromise (IoCs) are swiftly identified. These solutions act as vigilant sentinels, detecting both known threats and novel, previously undetected ones.
- *Automated threat response* When a security incident is detected, EDR solutions spring into action. Automated responses include isolating the affected endpoint, blocking malicious processes, and preventing lateral movement within the network. By automating incident containment, EDR minimizes the impact of threats and reduces manual intervention.
- *Threat isolation and remediation* EDR solutions isolate compromised endpoints to prevent the further spread of threats. They provide contextual information about the incident, aiding security teams in understanding the attack vector. Remediation guidance is offered, allowing organizations to restore affected systems efficiently.
- *Support for threat hunting* EDR solutions empower security analysts with tools for proactive threat hunting. Analysts can explore historical data, search for hidden threats, and identify potential risks. Threat hunting enhances the organization's ability to stay ahead of adversaries.

Endpoint protection technologies

1. *Next-generation firewall (NGFW)* NGFW represents a significant advancement beyond traditional firewalls. Its enhanced functionalities include:

    - *Deep Packet Inspection (DPI)* It is a method of examining the content of data packets as they pass by a checkpoint on the network. Unlike basic packet filtering, DPI examines the actual content within data packets. It ensures that no malicious software or harmful instructions are concealed.
    - *Application awareness* In NGFW, application awareness involves analyzing network traffic at the application layer. NGFWs excel at distinguishing various types of web traffic. For instance, they can differentiate between Facebook and Google Drive traffic, allowing for more precise control.
    - *Identity-based controls* It is the method of enforcing security policies based on user identities, groups, or roles. While traditional firewalls primarily focus on IP addresses, NGFWs associate rules with user identities. This dynamic approach simplifies rule management.
    - *Encrypted traffic inspection* Encrypted traffic inspection is the method of decrypting and inspecting the encrypted traffic to detect and prevent potential threats. With the widespread adoption of HTTPS, many attacks occur over

encrypted channels. NGFWs can decrypt, inspect, and then re-encrypt traffic, effectively closing this vulnerability.

According to Forrester Research, NGFWs serve as the "cornerstone of zero trust" in cybersecurity [22].

2. *End-to-end encryption* End-to-end encryption involves encrypting data as it travels between devices. While the sending and receiving devices can access the original data, no other intermediaries possess the correct keys to decrypt the message. End-to-end encryption serves as a robust safeguard against unauthorized access or interception during data transit [27]. When data are sent, it gets encrypted right at the sender's device. This ensures that the information remains secure in transit. Upon reaching the recipient, the data are decrypted only on their device. The process ensures that data remains unaltered during transit, maintaining its integrity.
3. *Secure web gateway (SWG)* SWG is a network security technology that filters internet traffic and ensures compliance with corporate and regulatory policies. A SWG serves as a critical defense against web-based threats on the Internet. Its primary function is to prevent malicious content from reaching endpoints. SWG solutions achieve this by enforcing policies set by the enterprise cybersecurity team, effectively blocking inappropriate or harmful websites. The SWG can send suspicious content to systems like data loss prevention (DLP) and CASB for analysis.
4. *Cloud access security broker (CASB)* A CASB is a security policy enforcement point positioned between cloud service consumers and providers. Its primary function is to enforce an organization's security policies related to cloud app access and usage [3].
5. *DNS filtering* DNS filtering involves selectively blocking access to specific sites, often based on content. When a site or category of sites is considered a threat, its IP address is blocked. DNS filtering is a crucial cybersecurity mechanism that leverages the domain name system (DNS) to enhance security and control over web content [51].

AI in zero trust network access (ZTNA)

ZTNA, also referred to as the software-defined perimeter (SDP), encompasses a suite of technologies and functionalities designed to facilitate secure access to internal applications for remote users [19]. Operating on an adaptive trust model, ZTNA ensures that trust is never assumed implicitly. Instead, access is granted based on a need-to-know and least-privileged approach, meticulously defined by granular policies. By leveraging ZTNA, remote users can establish secure connectivity to private applications without being placed directly on the network or exposing these applications to the broader internet.

ZTNA fundamentally separates the process of granting application access from network access. By doing so, it mitigates network-related risks, such as infections from compromised devices. Only authorized users who have undergone authentication gain access to specific applications. ZTNA ensures that outbound connections are the norm, minimizing exposure to the network. Both network and application

infrastructure remain concealed from unauthorized users. The resulting configuration renders the network virtually undetectable. Once users are authorized, ZTNA grants application access on a personalized basis. Authorized users interact solely with specific applications, avoiding unrestricted network access. This segmentation strategy curtails overly permissive access and mitigates lateral movement risks posed by malware. ZTNA diverges from traditional network security approaches. Encrypted transport layer security (TLS) micro-tunnels replace multiprotocol label switching (MPLS), ensuring secure communication between users and applications.

Leveraging machine learning techniques, an intelligent grouping of applications can be established by analyzing both applications and users. This process involves utilizing features such as fully qualified domain names (FQDN), port numbers, protocols, user departments, job titles, and other labeled data. Additionally, insights derived from application access patterns contribute to the creation of these application groupings. Ultimately, these well-defined groups serve as the foundational basis for implementing least-privileged access policies.

Network segmentation breaks the corporate network into isolated segments based on purpose and trust level. Microsegmentation takes this a step further, placing each application within its segment and applying security policies and access controls to all traffic crossing the network. ZTNA leverages microsegmentation to enforce its zero trust security policies. Microsegmentation places trust boundaries around each application, allowing ZTNA to inspect and apply access control policies to requests to that application. The AI-powered solution learns the environment, recommends segments, and creates policies, so IT teams don't have to develop policies manually. It verifies the identity of all communicating software every time it tries to communicate.

The secure access service edge (SASE) represents an emerging solution that integrates comprehensive software-defined wide area network (SD-WAN) capabilities with a suite of network security functions. These security functions include SWG, CASB, firewall as a service (FWaaS), and ZTNA [55]. Figure 4 shows the main components and connections of the SASE framework and ZTNA functions are illustrated in Fig. 5. ZTNA is a component of SASE and the ZTNA controller function becomes part of the SASE points of presence (PoP). PoPs function as entry points to SaaS and cloud services, ensuring efficient network performance irrespective of geographical location or the type of endpoint. Devices connect to the SASE PoP, get validated and users are only given access to those applications (and sites) allowed by the security policy in the SASE next-generation firewall (NGFW). ZTNA can be bundled with a complete suite of security services—NGFW, SWG, anti-malware, and Managed XDR—and with network services such as SD-WAN, WAN optimization, and a private backbone.

AI-powered SASE efficiently collects extensive data from network and security events. These data are consolidated in a central data lake, serving a dual purpose: providing a unified system view and serving as raw material for AI algorithms to learn and enhance. By leveraging AI, effective data management is achieved, leading to meaningful insights for informed decision-making. The integration of machine learning techniques within AI-powered SASE significantly enhances security. Unlike traditional security measures, AI covers a broader range of threats. Specifically, it

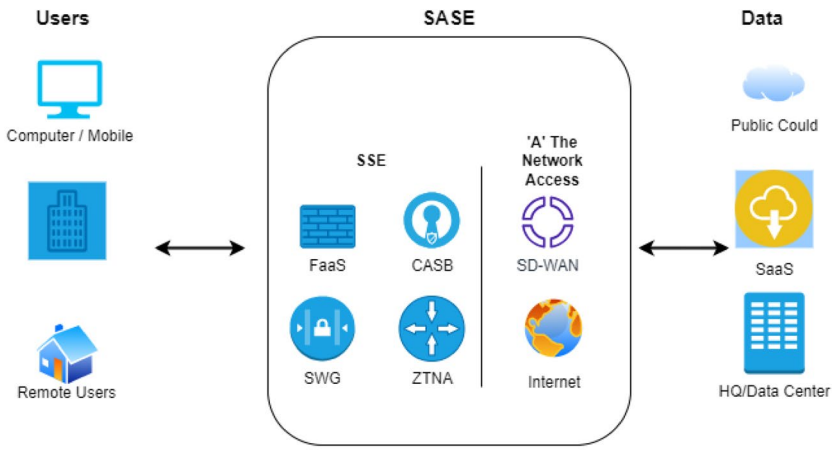

Fig. 4 Secure access service edge (SASE). SASE integrates software-defined wide area network (SD-WAN) capabilities with network security functions. These security functions include secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), software as a service (SaaS), and zero trust network access (ZTNA). ZTNA serves as the SASE point of presence (PoP) and acts as an entry point for SaaS and cloud services. Unlike traditional inspection engines in data centers, the SASE platform does not rely on them. Devices connect to the SASE PoP, undergo validation, and users are granted access only to applications and sites permitted by the security policy within the SASE next-generation firewall (NGFW), which is part of FWaaS.

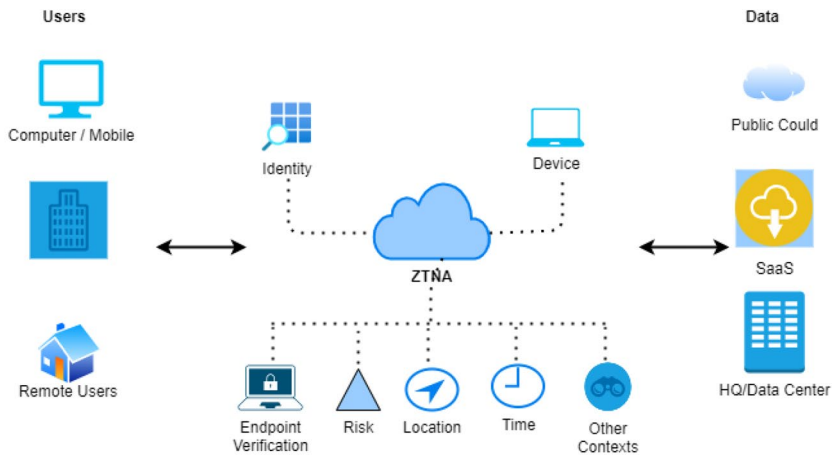

Fig. 5 Zero trust network access (ZTNA). ZTNA is a component of SASE and the ZTNA controller function serves as the SASE point of presence (PoP). PoPs function as entry points to SaaS and cloud services, ensuring efficient network performance irrespective of geographical location or the type of endpoint. ZTNA can be bundled with—next-generation firewall (NGFW), secure web gateway (SWG), anti-malware, and managed extended detection and response (XDR)—and with network services such as SD-WAN, WAN optimization, and a private backbone. XDR collects threat data from endpoints, identity management systems, cloud applications, communication channels, and data stores. When tested, device connected to the SASE PoP, got validated and user is only given access to those applications and sites allowed by the security policy in the SASE next-generation firewall (NGFW).

excels in detecting DNS-based threats and previously unknown, evasive threats, thereby elevating overall security effectiveness.

AI in network visibility and analytics

The improved infrastructure visibility and automated security controls empower network administrators to proactively counter threats and reduce risks, surpassing the capabilities of conventional perimeter security systems [47]. In the context of constructing distributed IT infrastructure, applications, and user environments, it is imperative for organizations to establish comprehensive end-to-end visibility. Eliminating blind spots becomes crucial, as managing what remains unseen is inherently challenging. Conversely, blind spots in certain environments may result in inadequate device patching and upgrades, leaving vulnerabilities and potential exposure to unwelcome threats or attacks 21.

Network visibility empowers AI to meticulously analyze user and device behavior over time. AI models excel at identifying patterns, thereby bolstering the capability to detect insider threats and unauthorized activities. The integration of AI and ML provides precise insights tailored to the network deployment, facilitating swift troubleshooting. One crucial technique is baselining, which involves analyzing network dynamics to extract behavioral patterns that define the 'normal' behavior for a specific network. By comparing actual network performance to this baseline, AI can detect anomalies and pinpoint their root causes, streamlining troubleshooting efforts. Additionally, AI proactively identifies global patterns and deviations, generating system-generated insights.

Given the inherent uniqueness and constant evolution of network environments, AI-powered network analytics continuously collects relevant data from local networks. These data are correlated against an aggregate de-identified dataset, and sophisticated machine learning models create context-specific baselines. These baselines dynamically adapt as network conditions change and the number of devices, users, and applications evolves.

Limitations

While research exploring the impact of AI on Zero Trust Technologies yields valuable insights, it is essential to acknowledge certain constraints. Here are notable limitations:

- *Rapidly evolving threat landscape* The cyber threat landscape undergoes constant transformation, with novel threats and vulnerabilities emerging regularly. This dynamism poses a challenge for research to remain current and relevant. Staying abreast of evolving threats demands continuous vigilance.
- *Variability in implementation* The effectiveness of ZT models varies significantly based on their implementation within an organization. Factors such as organizational context, infrastructure, and operational practices influence outcomes. Consequently, drawing definitive conclusions about overall significance becomes intricate.
- *Limited scope* Some research may focus narrowly on specific aspects of ZTA. While depth is valuable, it may inadvertently overlook other critical dimensions. The comprehensiveness of research can be constrained by such focused scopes.

- *The imperative for ongoing collaboration* Addressing these limitations necessitates ongoing collaboration across academia, industry, and regulatory bodies. Collective efforts enhance our understanding of ZTA and the pivotal role of AI within it.

In summary, despite these limitations, the existing research provides valuable signposts toward more robust and effective security strategies. As we navigate this complex terrain, continued exploration and collaboration remain paramount.

Conclusion

In this comprehensive review, I have explored the pivotal role that AI plays in advancing technologies behind the ZT model. AI empowers technologies to adapt dynamically to changing contexts. By continuously analyzing user behavior, device interactions, and network traffic, AI-driven zero trust technologies (ZTT) can make real-time access decisions. This adaptability aligns seamlessly with the core tenets of ZT, where trust is never assumed, and verification is perpetual. AI augments threat detection capabilities within ZTT. ML models can identify anomalous patterns, detect subtle deviations, and predict potential security breaches. Whether it's identifying unauthorized access attempts or flagging suspicious behavior, AI-driven ZTT enhances incident response and reduces dwell time. AI-driven ZTT automates access controls, reducing reliance on manual rule configuration. Policies tied to user identities, device attributes, and contextual factors become more dynamic and adaptive.

AI techniques enhance encryption methods, optimizing cryptographic algorithms and managing encryption keys. Additionally, AI-powered systems evaluate encrypted traffic, ensuring both privacy and security. As data traverses networks, AI assists in maintaining confidentiality and integrity.

Despite the immense promise of AI, ethical dilemmas persist. AI models may produce false positives (incorrectly flagging benign activities as threats) or false negatives (missing actual threats). Striking the right balance is crucial to avoid unnecessary alerts while ensuring critical incidents are not overlooked. Integrating AI into ZT frameworks demands expertise. Organizations must invest in training, deployment, and ongoing maintenance to harness its potential effectively. AI algorithms can inherit biases from training data. Ensuring fairness and transparency is essential to prevent discriminatory outcomes. Moreover, AI systems consume computational resources. Organizations need to allocate sufficient infrastructure for AI-based security solutions. Organizations must strike a balance between leveraging AI's capabilities and safeguarding individual rights.

This scholarly conclusion underscores the transformative impact of AI within zero trust paradigms, emphasizing the need for ongoing research, ethical considerations, and strategic implementation.

Abbreviations

AI	Artificial intelligence
AMFA	Adaptive multi-factor authentication
CASB	Cloud access security broker
DNS	Domain name system
DPI	Deep packet inspection
EDR	Endpoint detection and response
IAM	Identity access management
IoT	Internet of things

IT	Information technology
ML	Machine learning
MFA	Multi-factor authentication
NGFW	Next-generation firewall
OTP	Onetime password
PAM	Privilege access management
PDP	Policy decision point
PEP	Policy enforcement point
PoP	Point of presence
RBAC	Role-based access control
SaaS	Software as a service
SASE	Secure access service edge
SD-WAN	Software-defined wide area network
SVM	Support vector machines
SWG	Secure web gateway
WAN	Wide area network
ZT	Zero trust
ZTA	Zero trust architecture
ZTM	Zero trust model
ZTMM	Zero trust maturity model
ZTNA	Zero trust network access
ZTT	Zero trust technology

Acknowledgements
The author would like to thank the journal for the opportunity to publish an open access paper, and many thanks to the reviewers for their hard work and feedback.

Author contributions
The author read and approved the final manuscript.

Funding
The author declares that this work was not funded.

Availability of data and materials
No data are used in this paper.

Declarations

Competing interests
The author declare that she has no competing interests.

Received: 25 March 2024 Accepted: 28 July 2024
Published online: 05 August 2024

References

1. Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z (2022) Cyber security in IoT-based cloud computing: a comprehensive survey. Electronics. https://doi.org/10.3390/electronics11010016
2. Ahmed W, Rasool A, Javed AR, Kumar N, Gadekallu TR, Jalil Z, Kryvinska N (2021) Security in next generation mobile payment systems: a comprehensive survey. IEEE Access 9:115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450
3. Ahmad S, Mehfuz S, Mebarek-Oudina F, Beg J (2022) RSM analysis based cloud access security broker: a systematic literature review. Clust Comput 25(5):3733–3763. https://doi.org/10.1007/s10586-022-03598-z
4. Ali T, Kostakos P (2023) HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). arXiv abs/2309.16021. https://doi.org/10.48550/arXiv.2309.16021
5. American Council for Technology-Industry Advisory Council-ACT-IAC (2019) https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf. Accessed 30 July 2023
6. Arohan Y, Yadav A, Pandey A, Churi S, Saxena M, Vaghani A (2020) An introduction to context-aware security and user entity behavior analytics. Int J Adv Res Ideas Innov Technol 6(5):27–33
7. Behera NKS, Behera TK, Nappi M, Bakshi S, Sa PK (2021) Futuristic person re-identification over internet of biometrics things (IoBT): technical potential versus practical reality. Pattern Recognit Lett 151:163–171. https://doi.org/10.1016/j.patrec.2021.08.007
8. Bodepudi A, Reddy M, Gutlapalli SS, Mandapuram M (2019) Voice recognition systems in the cloud networks: has it reached its full potential. Asian J Appl Sci Eng 8(1):51–60
9. Brusilovsky P, Millán E (2007) User models for adaptive hypermedia and adaptive educational systems. In: Brusilovsky P, Kobsa A, Nejdl W (eds) The adaptive web: methods and strategies of web personalization. Springer, Berlin, pp 3–53
10. Campbell M (2020) Beyond zero trust: trust is a vulnerability. Computer 53(10):110–113. https://doi.org/10.1109/MC.2020.3011081

11. Capraro V, Lentsch A, Acemoglu D, Akgün S, Akhmedova A, Bilancini E, Bonnefon J-F, Brañas-Garza P, Butera L, Douglas KM, Everett JAC, Gigerenzer G, Greenhow C, Hashimoto DA, Holt-Lunstad J, Jetten J, Johnson S, Longoni C, Lunn P, Natale S, Rahwan I, Selwyn N, Singh V, Suri S, Sutcliffe J, Tomlinson J, Linden S van der, Lange PAMV, Wall F, Bavel JJV, Viale R (2023) The impact of generative artificial intelligence on socioeconomic inequalities and policy making. ArXiv abs/2401.05377. https://doi.org/10.48550/arXiv.2401.05377
12. Cao Y, Pokhrel SR, Zhu Y, Doss R, Li G (2024) Automation and orchestration of zero trust architecture: potential solutions and challenges. Mach Intell Res 21(2):294–317. https://doi.org/10.1007/s11633-023-1456-2
13. Chen Y, Hu H, Cheng G (2019) Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. Front Inf Technol Electron Eng 20(2):238–252. https://doi.org/10.1631/FITEE.1800516
14. CISA (2023) Zero trust maturity model. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf. Accessed 09 July 2023
15. Cloudflare Zero Trust security | What is a Zero Trust network? https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/. Accessed 23 July 2023
16. Compastié M, Badonnel R, Festor O, He R, Kassi-Lahlou M (2016) A software-defined security strategy for supporting autonomic security enforcement in distributed cloud. In: 2016 IEEE international conference on cloud computing technology and science (CloudCom), pp 464–467. https://doi.org/10.1109/CloudCom.2016.0079
17. Crowdstrike (2023) Zero trust security explained: principles of the zero trust model. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/. Accessed 05 Aug 2023
18. Delinea what is adaptive multi-factor authentication (MFA)? https://delinea.com/blog/adaptive-multi-factor-authentication-mfa-2. Accessed 09 Aug 2023
19. Deshpande A (2021) A study on rapid adoption of zero trust network architectures by global organizations due to COVID-19 pandemic. New Vis Sci Technol 1:26–33. https://doi.org/10.9734/bpi/nvst/v1/3640F
20. DoD (2022) Zero trust reference architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/%28U%29ZT_RA_v2.0%28U%29_Sep22.pdf. Accessed 06 Aug 2023
21. Enterprise Strategy Group (ESG) (2023) The importance of network visibility and analytics for zero trust initiatives. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/esg-importance-network-visibility.pdf. Accessed 27 Aug 2023
22. Forrester (2015) Your best defense: next-generation firewalls enable zero trust security. https://informationsecurity.report/Resources/Whitepapers/93d69295-3527-49f6-90d4-d52a4387282b_Best%20Practices%20For%20Evaluating%20And%20Implementing%20a%20Next%20Gen%20Firewall.pdf. Accessed 20 Aug 2023
23. Frankish K, Ramsey WM (2014) The Cambridge handbook of artificial intelligence. Cambridge University Press
24. Gartner (2023) Gartner forecasts worldwide public cloud end-user spending to reach $679 Billion in 2024. https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240. Accessed 08 July 2023
25. Ghasemshirazi S, Shirvani G, Alipour MA (2023) Zero trust: applications, challenges, and opportunities. arXiv preprint arXiv:230903582. https://doi.org/10.48550/arXiv.2309.03582
26. Global Cybersecurity Alliance (ISA) (2023) Cloud computing and cybersecurity: everything you need to know. https://gca.isa.org/blog/cloud-computing-and-cybersecurity-everything-you-need-to-know. Accessed 08 July 2023
27. Greenberg A (2014) Hacker lexicon: what is end-to-end encryption? Wired, Nov 25
28. Greitzer FL, Purl J, Sticha PJ, Martin CY, Lee JD (2021) Use of expert judgments to inform bayesian models of insider threat risk. J Wirel Mob Netw Ubiquitous Comput Dependable Appl 12(2):3–47. https://doi.org/10.22667/JOWUA.2021.06.30.003
29. He Y, Huang D, Chen L, Ni Y, Ma X (2022) A survey on zero trust architecture: challenges and future trends. Wirel Commun Mob Comput 2022:6476274. https://doi.org/10.1155/2022/6476274
30. Hussain M, Pal S, Jadidi Z, Foo E, Kanhere S (2024) Federated zero trust architecture using artificial intelligence. IEEE Wirel Commun 1(2):30–35. https://doi.org/10.1109/MWC.001.2300405
31. Identity Management Institute (2021) Artificial intelligence and machine learning are transforming Iam. https://identitymanagementinstitute.org/artificial-intelligence-and-machine-learning-are-transforming-iam/. Accessed 12 Aug 2023
32. Jorquera Valero JM, Sánchez Sánchez PM, FernándezMaimó L, HuertasCeldrán A, ArjonaFernández M, De Los Santos Vílchez S, Martínez Pérez G (2018) Improving the security and QoE in mobile devices through an intelligent and adaptive continuous authentication system. Sensors. https://doi.org/10.3390/s18113769
33 Kang H, Liu G, Wang Q, Meng L, Liu J (2023) Theory and application of zero trust security: a brief survey. Entropy. https://doi.org/10.3390/e25121595
34. Karantzas G, Patsakis C (2021) An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. J Cybersecur Priv 1(3):387–421. https://doi.org/10.3390/jcp1030021
35. Kindervag J (2010) Build security into your network's DNA: the zero trust network architecture. Forrester Research Inc, Cambridge, p 27
36. Kindervag J, Balaouras S, Mak K, Blackborow J (2016) No more chewy centers: the zero trust model of information security. Forrester Research Inc, Cambridge
37 Mandapuram M, Gutlapalli SS, Bodepudi A, Reddy M (2018) Investigating the prospects of generative artificial intelligence. Asian J Human Art Lit 5(2):167–174. https://doi.org/10.18034/ajhal.v5i2.659
38. Mohammed IA (2021) The interaction between artificial intelligence and identity and access management: an empirical study. Int J Creat Res Thoughts 3:668–671
39. Moubayed A, Refaey A, Shami A (2019) Software-defined perimeter (SDP): state of the art secure solution for modern networks. IEEE Netw 33(5):226–233. https://doi.org/10.1109/MNET.2019.1800324
40. NIST (2020) Zero trust architecture: NIST Publishes SP 800-207. https://csrc.nist.gov/News/2020/zero-trust-architecture-nist-publishes-sp-800-207. Accessed 09 July 2023
41. NIST (2023) A zero trust architecture model for access control in cloud-native applications in multi-cloud environments. https://csrc.nist.gov/pubs/sp/800/207/a/final. Accessed 09 July 2023

42. Norton (2023a) 23 cloud security risks, threats, and best practices to follow. https://us.norton.com/blog/privacy/cloud-security-risks. Accessed 08 July 2023
43. Norton (2023b) What is facial recognition and how does it work? https://us.norton.com/blog/iot/how-facial-recognition-software-works. Accessed 12 Aug 2023
44. Ramezanpour K, Jagannath J (2022) Intelligent zero trust architecture for 5G/6G networks: principles, challenges, and the role of machine learning in the context of O-RAN. Comput Netw 217:109358. https://doi.org/10.1016/j.comnet.2022.109358
45 Rangaraju S (2023) Secure by intelligence: enhancing products with AI-driven security measures. EPH Int J Sci Eng 9(3):36–41. https://doi.org/10.53555/ephijse.v9i3.212
46. Sans (2023) What is zero trust architecture? https://www.sans.org/blog/what-is-zero-trust-architecture/. Accessed 10 Sept 2023
47 Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H (2022) Security of zero trust networks in cloud computing: a comparative review. Sustainability. https://doi.org/10.3390/su141811213
48. Security Intelligence (2020) When implementing zero trust, context is everything. https://securityintelligence.com/posts/when-implementing-zero-trust-context-is-everything/. Accessed 30 July 2023
49. Shabbir M, Shabbir A, Iwendi C, Javed AR, Rizwan M, Herencsar N, Lin JC-W (2021) Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access 9:8820–8834. https://doi.org/10.1109/ACCESS.2021.3049564
50. Suleski T, Ahmed M, Yang W, Wang E (2023) A review of multi-factor authentication in the Internet of Healthcare Things. Digit Health 9:20552076231177144. https://doi.org/10.1177/20552076231177144
51. Techradar (2022) What is DNS filtering? https://www.techradar.com/features/what-is-dns-filtering. Accessed 20 Aug 2023
52. Techradar (2023) Cloud-based cyberattacks have seen a huge rise. https://www.techradar.com/news/cloud-based-cyberattacks-have-seen-a-huge-rise. Accessed 08 July 2023
53. Techtarget (2023) DEFINITION adaptive multifactor authentication (adaptive MFA). https://www.techtarget.com/whatis/definition/adaptive-multifactor-authentication-adaptive-MFA. Accessed 10 Sept 2023
54. The Register (2023) Miscreants sure do love ransacking cloud networks, more so than before. https://www.theregister.com/2023/01/20/cloud_networks_under_attack/. Accessed 08 July 2023
55. van der Walt S, Venter H (2022) Research gaps and opportunities for secure access service edge, pp 609–619
56. Zukerman I, Albrecht DW (2001) Predictive statistical models for user modeling. User Model User-Adapt Interact 11(1):5–18. https://doi.org/10.1023/A:1011175525451

Publisher's Note