International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Zero trust architecture in IAM with AI integration

Sahil Arora [1,*] and Apoorva Tewari [2]

[1] *Independent Researcher, Staff Product Manager, Twilio Inc.*
[2] *Senior Product Manager, Intuit Inc.*

International Journal of Science and Research Archive, 2023, 08(02), 737–745

Publication history: Received on 13 January 2023; revised on 24 April 2023; accepted on 29 April 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.2.0163

Abstract

ZTA is a new model of enterprise cybersecurity that stands for continuous authentication, strict access control and dynamic verification for data, assets and identities of enterprises in multilayered infrastructures. ZTA ensures that each and every incoming request to access people, devices or applications is constantly compared to the organisation's policy and approved, no matter if it is coming inside or outside a network, unlike a traditional perimeter-based security strategy. In an effort to enhance the compliance standards and lower the attack surface, this article expands on the basic tenets of ZTA, such as adding IAM to regulate access based on the role and permission systems. ZTA is further enhanced by AI that enables the real-time identification of threats, dynamic security access control, and risk estimation. By adopting the AI approach, ZTA can make intelligent decisions, and this makes companies able to counteract the ever-incoming cyber threats. Among the areas where ZTA and AI applications are being adopted are cloud environments, remote workforces, IoT devices, and microservices. Further research prospects are also enumerated in this document, such as developing AI-based behavioural analytics, safeguarding Edge and IoT applications, incorporating improved threat intelligence, and incorporating machine learning in ZTA processes. These developments will keep ZTA as a strong and adaptive cybersecurity framework for any corporate infrastructures and protect them from threats in related modern digital landscapes.

Keywords: Zero Trust Architecture (ZTA); Identity and Access Management (IAM); Artificial Intelligence (AI); Threat Intelligence; Zero Access; Cloud Environments; Secure Access Service Edge (SASE).

1. Introduction

The infrastructure of the average firm has become more sophisticated. A single company may run many internal networks, distant locations with independent local infrastructure, mobile and/or remote workers, and cloud services. a intricate endeavour has resulted in the creation of a novel cybersecurity paradigm called "zero trust" (ZT). Although the primary purpose of a ZT strategy is to protect data and services, it can and ought to be expanded to cover all enterprise assets, including subjects like end users, apps, and nonhuman entities that use resources to obtain information, as well as devices, infrastructure parts, applications, virtual, and cloud components. As a general rule, zero trust security measures include strictly limiting access to resources (including data, compute power, applications, and services) to only those individuals or entities that have been authorised to do so and constantly verifying the identity and security status of every request for access.

ZTAs are enterprise cybersecurity designs that reduce internal lateral movement and work to avoid data breaches. The paper delves into ZTA, its logical components, potential deployment scenarios, and potential dangers, as seen in Figure 1. Additionally, it covers pertinent federal legislation that might affect or affect a zero-trust architecture, and it gives a broad roadmap for organisations looking to transition to such a design approach[1].

* Corresponding author: Sahil Arora

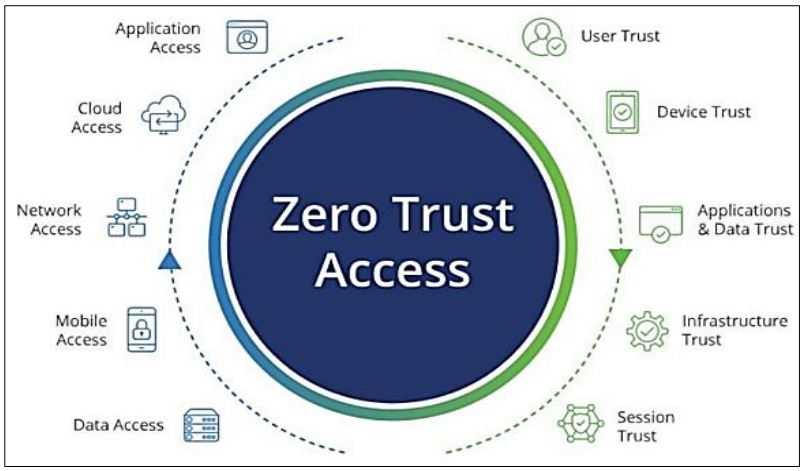

Figure 1 Access to Zero Trust

The aim of IAM is to guarantee that only permitted users may access particular resources for defined reasons and at specific times. The verification technique is a crucial part of any silent authentication system that checks the user's identity and licensing status whenever he attempts to access a service provider system via IAM. Traditional authentication methods are plagued by a multitude of problems and are reliant on several factors. For example, in a password authentication method, the revealed secret phrase (password) of the users is compared with the secret phrase kept in the system[2]. The claimed user's identity is determined using the outcome of this matching process. There are a number of issues with this approach, not to mention the possibility of the keyword being forgeries or stolen[3].

ZTA in IAM, with AI integrated data protection solution, checks the identity of every user and every device in real time before granting access from any location. Compared to traditional perimeter-based security, different solutions of ZTA always use a principle of 'never-trust, always-verify,' which means strict access control is performed for all entry points to the network. AI integration improves this by taking observations from behaviour, distinguishing irregularities, and altering security actions in real time, leading to a more effective way of protecting against new threats. Both ZTA and AI enhance security and flexibility of the contemporary IT environments. The key contribution of this paper is:

- Leading-edge security that regularly verifies people and devices so that the risk of undesirable outcomes such as unauthorised access is significantly reduced in different contexts through the application of Zero Trust.
- Security that can be more proactively engaged due to the AI process that may alter policies as frequently and frequently as user actions and environmental conditions dictate.
- Researching the current approaches for Zero Trust adoption when securing cloud assets and IoT devices with a focus on fine-grained control and constant authentication.
- Documentation on how IAM integrated with ZTA removes user proliferation, simplifies administrative tasks and enhances compliance with security policies ranging from RBAC and automation.
- Investigation into an application of Zero Trust principles in microservices architectures, ensuring secure communications and access between services and APIs while minimising the attack surface.

1.1. Organization of the paper

Here is the outline of the paper: Section II covers the core concepts of zero trust architecture (ZTA). Section III Details IAM in a context of zero trust. Section IV Examines the application for zero trust architecture with AI integration. Section V presents a Literature review, identifies research gaps, and VI offers Recommendations for conclusions and future work.

2. Core Concepts of Zero Trust Architecture (Zta)

As a cybersecurity approach for enterprises, ZTA signifies a radical change based on zero-trust principles. Its main goal is to limit internal lateral progression and prevent data leaks. Zero trust (ZT) is a collection of concepts that may be used in workflow, operations, and design rather than a single architecture.

2.1. Logical Components and Architecture of Zero Trust Security

ZTA usually consists of five main components. However, this might change depending on the needs of an organisation [4]. As shown in Figure 2, these elements include resource, policy enforcement point (PEP), policy administrator (PA), policy engine (PE), and subject [1]. Researchers then started building upon this logical framework with concepts like policy storage and policy information points (PIP).

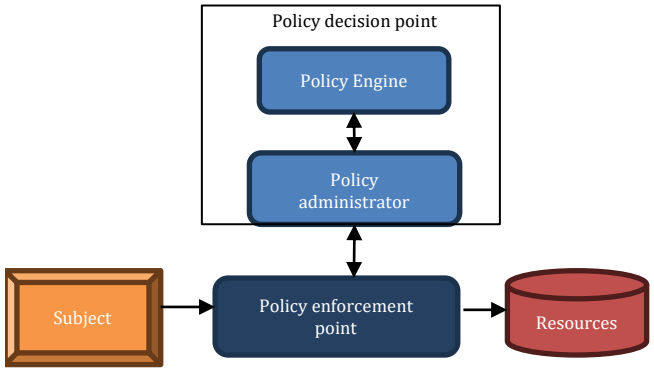

Figure 2 Typical components of the logical structure of zero trust architecture

- **Policy engine (PE):** The PE, a key component of an idea, is in charge of the final, long-term decision on the provision of network or device access. The PE is designed to be programmed to give, refuse, or revoke access to the resource depending on the organisation's internal and external working policies, as well as other external elements like CDM systems, threat information, and activity logs. The PE is accompanied by the component that oversees policy administration. After the policy engine has reached a decision and written it down as approved or refused, the policy administrator carries it out [5].
- **Policy administrator:** In its main role, the policy administrator acts as an executor, monitoring and responding to requests for access or denial of access based on data received from the policy engine. In practice, this means that the PA verifies the identity of users using the credentials or tokens that customers use to access company resources [5].
- **Policy enrollment point:** This component is responsible for carrying out the policy engine's orders, such as enabling, monitoring, and terminating agent-client communication; it also acts as a link between users and the system's resources [5].

It was then that academics started to build upon this logical design by adding concepts like policy storage and PIP. Network participants, PEP, PDP, PIP, PAP, and resources are the six main components of the revised zero trust logic architecture, which are outlined in Figure. 3.

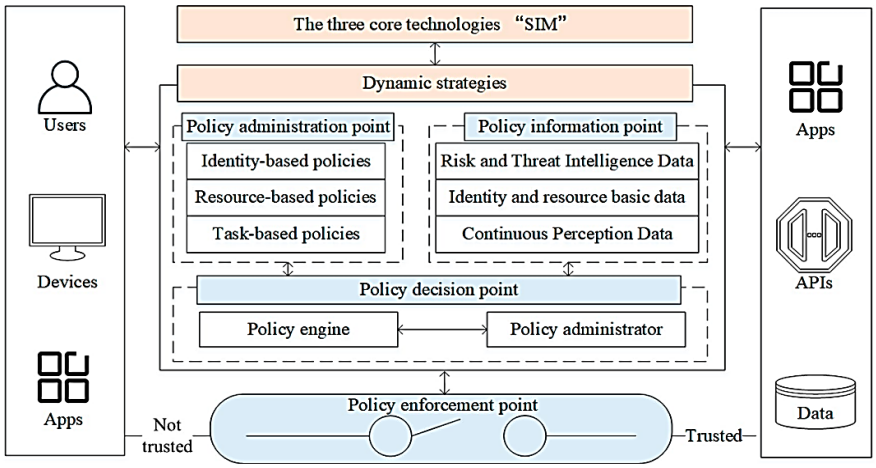

Figure 3 The updated zero trust logic architecture and its key components

The conceptual underpinning of zero trust security is shown in Figure 3. It includes all of the interactions that take place between people, devices, and applications on a network. Additionally, it includes pertinent resources including applications, data, and APIs. Both PE and PA make up the PDP. The PE component is referred to be the "brain" of the ZTA due to its inclusion of the trust algorithm, a crucial decision-making process. It continually assesses the reliability of network users by using data from PAP and PIP, including behavioural patterns, threat intelligence, network traffic, and access controls. Authorisation policy management is done continually by the PA component. The actual implementation of these regulations is the PEP, which facilitates communication among users, devices, applications, and the necessary resources.

- The process starts when a network user initiates a request to the PEP for resource access, following the access flow displayed in Figures 1 and 2.
- The PEP then sends the PDP the information on the request. Subsequently, the PDP's PE component assesses the degree of trust by combining information from many different sources.
- The PA part of the PDP determines the authorisation approach using the PE's prior assessment of the trust value.
- After the access has been allowed, the PDP will provide the PEP instructions on how to set up a secure communication channel.
- The PDP will keep an eye on trust and establish authorisation standards to keep resources safe, updating the PEP as necessary.
- The PEP will then respond to this input by taking the necessary steps to guarantee the resources' security at all times.

2.2. Principle of zero Trust architecture

- **Authenticate users:** Verify a person's identity by analysing their device, location, and activities to determine their level of security. To ensure the user's validity, use appropriate measures, such as multifactor authentication.
- **Authenticate devices:** Device identification and security should impact the rules that govern the use of all devices, whether they are mobile, laptop, bring-your-own-device, public, or company-issued. When it comes to the company's resources, only reliable endpoints are granted access.
- **Restrict access and permissions:** Use a role-based access control approach to resources, granting just the permissions necessary to finish the task at hand, after validating both persons and devices.
- **Adaptive:** A multitude of sources, including people, their equipment, and all related activities, are continuously producing new information. Use ML to create context-sensitive access controls that automatically change and respond to regulations[6].

3. Identity and Access Management (IAM) in The Context of Zero Trust

IAM is a complete framework created to control individuals' digital identities throughout their lives. System administrators and mission-critical assets are among the people and assets in the IT environment whose behaviour and activities are monitored by IAM [7]. IAM includes "identity management" and "access management"[8], including identity management together with the organisational procedures related to authentication and authorisation. Humans, as well as non-human things, may claim identities.

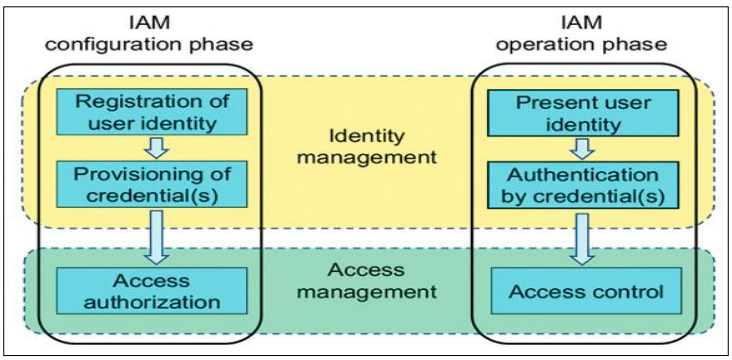

Figure 4 Phases of IAM [9]

Figure 4 presents details on both the IAM setup and operating phases. Permissions control how users may access AWS resources. IAM can help in handling permissions. IAM, sometimes referred to as RBAC, allows cloud users to quickly assign a specific function that is associated with a set of permissions to access data storage, the Internet, and other functions. It may reduce the attack surface of apps and prevent the processing costs associated with unauthorised queries. Business organisations may increase regulatory compliance and assure high-quality security systems manufacturing processes by using IAM. IAM has the power to make conventional usernames and password solutions more flexible[10].

3.1. Key Components of the Process of IAM

IAM specialists need to have a clear understanding of IAM scenarios that meet business needs. All IAM projects ought to progress towards the necessary end state. IAM's constituent parts may be divided into four groups: central user, user management, authentication, and authorisation. Nowadays, a greater number of corporate organisations are concentrating on integrating cloud infrastructure platforms with similar capabilities.

- **Authentication in IAM:** According to the information system's security criteria, authentication's objective is to confirm an entity's identification with recognised threshold trust. When the authentication method offers a mechanism that would result in an implementation without backdoors, it must be reliable [11]. The purpose of authentication in IAM is to verify the user's identity just once during the login process [12]. Intelligent authentication has the potential to be a hyper-method for user-attribute-based contextual authentication, which might be used with user biometric data, other system environment characteristics, and certain business processes. Decision procedures for matching and verifying user traits often make use of intelligent techniques and technologies, such as soft computing[13].
- **User management in IAM:** Manage users in IAM to restrict access to company data, applications, and systems. Ensuring that users have access to the proper resources based on their responsibilities entails creating, editing, and deleting user accounts via a process called user provisioning. This is made easier with role management, which reduces administrative complexity and guarantees compliance with security standards by giving particular access privileges based on user roles.
- **Central user in IAM:** In the context of IAM, a central user is an organisation's one digital identity that unifies authorisation and access across all of the company's systems, apps, and services. A centralised user model streamlines user administration and improves security by allowing a single identity to be handled across all contexts rather than having several user accounts for various platforms.

3.2. Benefits of Identity and Access Management (IAM)

There a benefit of IAM for an enterprise zero trust architecture below:

- **Enhanced security:** IAM solutions help identify and resolve security concerns. You may use IAM to find out who has violated your policies or removed unauthorised access permissions without having to deal with several systems. Further, IAM may be used to check whether security measures are enough to meet audit and regulatory requirements[14].
- **Sharing of information:** An identity and access management system is available with IAM. It is possible that the company's safety regulations will apply to all of the operating systems and devices in use. It is possible to build authentication procedures, permissions, and verification constraints with the aid of IAM platforms, which may prevent "privilege creep."
- **Ease of use:** Registration, sign-in, and user management are all made easier with IAM, which benefits app owners, end users, and system administrators. The user experience is enhanced by IAM's simplification of access delivery and administration. Users may access services based on their assigned roles and permissions via identity and access management[15].
- **Productivity gains:** IAM simplifies access by centralising all access rules. It simplifies authorisation procedures and speeds up the adoption of new apps while allowing for uniform, scalable, and centralised user management. Automated provisioning and Lifecycle Management systems provide identity and access management solutions; instead of randomly assigning passwords and granting access to each application, IT managers may utilise these systems[15]. Instead of needing to request various tools and resources sometimes, users are offered quick access upon onboarding according to their purpose, so there's no need for them to wait in queue. Fewer IT needs and more productivity are the results[14].
- **Reduced IT Costs:** The use of IAM services has the potential to save operating costs. Since federated identity networks eliminate the requirement for local identities for external purposes, application administration becomes simpler with their use. IAM services hosted in the cloud could lessen the need for purchasing and

maintaining local infrastructures. Businesses may gain a competitive advantage by using IAM technology and adhering to related best practices[14].

4. Application for Zero Trust Architecture with AI Integration

There is application for zero-trust architecture with AI integration:

- **Cloud Environments:** The growing popularity of cloud services coupled with Zero Trust provides a strong security foundation for safeguarding data and assets hosted on cloud servers. Zero Trust offers more control over cloud resources and reduces the risks related to cloud security by implementing access rules and continuous verification.
- **Remote Workforce:** Zero Trust is also beneficial when defending employees who connect to corporate assets in ways that are beyond traditional perimeters. Such contrasting behaviour with the devices and networks, which are situated at a distant location, reduces the probability of unauthorised intrusion.
- **Internet of Things (IoT) Security:** Zero trust is essential for protecting IoT devices as the IoT grows in scale. Zero Trust reduces a risk of IoT-related cyber-attacks and prevents an use of IoT devices by unauthorised entities due to strict control of permissions and constant IoT device authentication. This can be achieved by employing AI and analytics techniques, which facilitate ranking of the likely IoT device behaviour risk.
- **Microservices and API Security:** Microservices and APIs are critical components at present while designing applications. APIs can only be accessed by those organisations who are allowed, and Microservices may share information between each other safely through the use of Zero Trust Principal.
- **Secure Access Service Edge (SASE):** The SASE architecture is really complementary to Zero Trust since it integrates cloud security and networking. By successfully deploying Zero Trust, organisations may greatly improve their network security, respond to changing threat environments, and safeguard vital assets from sophisticated cyberattacks. Applying Zero Trust to various domains allows organisations to create a strong security architecture that protects information and assets while promoting confidence in digital operations.

5. Literature Review

This section should include some prior research on IAM-based ZTA. A few authors have dabbled with ZTA in the cloud. One topic covered was the integration of AI with IAM using the ZTA.

Zhang et al. (2022), the ZTA a novel method for evaluating trustworthiness. They introduced the TBTE framework, which integrated the techniques based on criteria and scores. An individual's level of confidence in an access topic, as measured by their actions and the device's security posture, is carefully considered throughout the tag generation process. In contrast to trust score-based evaluations, which make the trust result difficult to understand, and condition-based policies, which make the authorisation process more difficult, a straightforward trust evaluation rule is provided by employing positive and negative features of the tag[16].

Alawneh and Abbadi (2022), concentrate and discrepancies. Our most significant contribution is the application of trusted computing methods to the "Always Verify" notion and the "Never Trust" philosophy via the usage of trust models. To achieve the Zero Trust principles, it is highly recommended to integrate Trusted Computing methods with Trust Models. The Zero Trust concept of "Never Trust/Always Verify" is a cornerstone of developing a long-term strategy to deal with evolving threat environments [17].

Qazi et al. (2022), This article reviews the use of zero trust, as an alternative to standard perimeter security, in network architecture security. A summary of several software programs is also provided for establishing ZTNA-based secure access to programs and services for distant users. There is a change in thinking about resources and the need for a ZTA based on the zero-trust principle. Networks that have adopted zero trust principles make sure that critical data, assets, applications, and services are not vulnerable to a single unsecured API [18].

Song et al. (2022), create a differentiated privacy system that can be integrated into ZTA. In both centralized and local DP scenarios, it maintains a consistent representation of privacy and uses the same noise mechanism. It also manages to find a middle ground between the robustness and flexibility of privacy protections. Confirm experimentally that the algorithm can get the same or higher utility results with the same degree of security as previous approaches by using the maximum expectation estimation method. An important aspect of the industry-wide norm for protecting sensitive data on the Internet is the ZTA[19].

Thakur and Gaikwad (2015), explores the many aspects of an identity management system, including the federated identity manager and access management system, and how they collaborate to regulate access to resources, while also outlining the risks and challenges associated with implementing such a system. One of the most critical and time-consuming aspects of any IT system or user lifecycle control system is ensuring the security of user data. A superset of user provisioning systems, identity management systems make it simple for users and anyone else who needs access to their credentials and personal information to handle this data[8].

Yan and Wang (2021), comprises features for managing identity authentication and access control. By creating an end-to-end dynamic new border based on identity, zero trust technology may genuinely realise the aggregation of security and business, opening up new possibilities for the growth and upgrading of corporate network security architecture. Legitimacy is establishing the user's identity; security is evaluating the machine's security features; and necessary countermeasures are implemented by the access control system [20].

Do Amaral and Gondim (2021), recommends using a ZTA in a network of cyber suppliers. The primary contribution of this research is a structure for organizing controls related to cyber supply chain security in a manner that allows for the use of ZTA principles to enhance cyber supply chain security. The research also includes instructions on how to conduct a gap analysis and ways to display the findings [21].

Table 1 compares and contrasts numerous methodologies, performances, and shortcomings of the studies for the execution of ZTA in IAM. Okay, in fact each of the studies show a different strategy, the problems they faced and the possible ways to tackle the concept of Zero Trust.

Table 1 Comparative related study on Zero Trust Architecture (ZTA) in IAM

References	Methodology	Performance	Limitations & Future Work
[16]	Proposed a new Tag-based Trust Evaluation (TBTE) framework combining score-based and criteria-based approaches.	Improved interpretability of trust results and reduced complexity of authorisation policies compared to other methods.	Future work includes improving scalability and adaptability for diverse environments.
[17]	Integration of Trusted Computing mechanisms with Trust Models to achieve Zero Trust principles.	Enhanced implementation of the "Never Trust/Always Verify" concept, contributing to better adaptability to changes in the threat landscape.	Future research can explore dynamic adjustments to trust models as threat landscapes evolve.
[18]	Reviewed Zero Trust for network security, focusing on Zero Trust Network Access (ZTNA) solutions for remote users.	Demonstrated effectiveness in ensuring secure access without relying on traditional perimeter-based models.	Limitations include addressing API vulnerabilities and ensuring seamless integration with legacy systems.
[19]	Designed a differential privacy scheme for Zero Trust Architecture using maximum expectation estimation method.	The study also details methods for displaying the results and how to carry out a gap analysis.	Further work is needed to refine privacy mechanisms and address practical deployment challenges.
[8]	Overview of Identity Management Systems and challenges in user security, focusing on Federated Identity Manager.	Simplified management of user credentials and identity information, with enhanced lifecycle control.	Challenges remain in securing user data in large, complex environments, and managing federated identities at scale.
[20]	Developed a dynamic access control system based on identity and machine security characteristics.	Enabled end-to-end security aggregation and dynamic boundary creation based on identity.	Future work could focus on automating responses and improving real-time evaluation mechanisms.

[21]	Proposed integration of Zero Trust Architecture in cyber supply chains, with a checklist of security controls.	Enhanced security in cyber supply chains by applying Zero Trust principles and gap analysis.	Future research should explore real-time monitoring and dynamic adaptation of controls for evolving supply chain risks.

6. Conclusion

When it comes to protecting cloud-based and on-premises computing assets, the new ZTA prioritises continuous, dynamic authentication and least privilege access control above the more conventional perimeter-based security methods. IAM integrated with ZTA could help organisations reduce risks associated with unauthorised access, enhance compliance with regulation acts, address user management issues and enhance security. A particular contribution of AI integration to ZTA is real-time threat identification, AC, and predictive risk handling in ZTA. These are AI-enabled features that enable organisations develop the ability to prevent new emerging threats within cyberspace effectively and actively.

Future Scope

Future endeavours in research and development should focus on improving the AI-based behavioural analysing mechanism more strategically for enhanced anomaly and risk identification. IoT and edge computing is another important domain that needs to be secured more and more frequently used in enterprises and being heterogeneous nets. Also, the integration of more enhanced threat intelligence into the ZTA frameworks will enhance the system capacity to address new and early emerging threats comprehensively. Machine learning models can automate components of ZTA for better execution, minimise human dependency and allowed consistency in the policies being implemented. Last but not least, taking ZTA to multi-cloud and hybrid environments will help to keep it future-proof and agile, given that environments enterprises run their applications and services are becoming dynamic and geographically distributed. These advancements will enhance and establish ZTA as the sustainable and flexible security paradigm for future protection.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest is to be disclosed.

References

[1] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," *Security and Communication Networks*. 2021. doi: 10.1155/2021/9947347.

[2] I. A. Mohammed, "Intelligent authentication for identity and access management: a review paper IJMIEII Intelligent authentication for identity and access management: a review paper," *Int. J. Manag. IT Eng.*, 2013.

[3] S. Mulla, "A literature review on the tools for Identity Access Management using AI," vol. 9, no. 10, pp. 33–37, 2022.

[4] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Comput. Secur.*, 2021, doi: 10.1016/j.cose.2021.102436.

[5] O. C. Edo, T. Tenebe, E. Etu, A. Ayuwu, J. Emakhu, and S. Adebiyi, "Zero Trust Architecture: Trend and Impacton Information Security," *Int. J. Emerg. Technol. Adv. Eng.*, 2022, doi: 10.46338/ijetae0722_15.

[6] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wirel. Commun. Mob. Comput.*, 2022, doi: 10.1155/2022/6476274.

[7] A. Caballero, "Information Security Essentials for Information Technology Managers," in *Computer and Information Security Handbook*, 2017. doi: 10.1016/b978-0-12-803843-7.00024-7.

[8] M. A. Thakur and R. Gaikwad, "User identity and access management trends in it infrastructure- An overview," in *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, 2015. doi: 10.1109/PERVASIVE.2015.7086972.

[9] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artif. Intell. Rev.*, 2020, doi: 10.1007/s10462-020-09814-9.

[10] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. K. R. Choo, and Y. H. Park, "Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.2966242.

[11] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A Review on Authentication Methods," *Aust. J. Basic Appl. Sci.*, vol. 7, pp. 95–107, Jun. 2013.

[12] S. Mondal and P. Bours, "A continuous combination of security & forensics for mobile devices," *J. Inf. Secur. Appl.*, 2018, doi: 10.1016/j.jisa.2018.03.001.

[13] A. Karim Abdul-Hassan and I. Hasson Hadi, "Intelligent Authentication for Identity and Access Management: a Review Paper," *Iraqi J. Comput. informatics*, vol. 45, no. 1, pp. 6–10, 2019, doi: 10.25195/2017/4512.

[14] M. K. Hamza, H. Abubakar, and Y. M. Danlami, "Identity and Access Management System: a Web-Based Approach for an Enterprise," *Path Sci.*, vol. 4, no. 11, pp. 2001–2011, 2018, doi: 10.22178/pos.40-1.

[15] T. Martens, "Electronic identity management in Estonia between market and state governance," *Identity Inf. Soc.*, 2010, doi: 10.1007/s12394-010-0044-0.

[16] C. Zhang *et al.*, "Tag-Based Trust Evaluation In Zero Trust Architecture," in *2022 4th International Academic Exchange Conference on Science and Technology Innovation, IAECST 2022*, 2022. doi: 10.1109/IAECST57965.2022.10062213.

[17] M. Alawneh and I. M. Abbadi, "Integrating Trusted Computing Mechanisms with Trust Models to Achieve Zero Trust Principles," in *2022 9th International Conference on Internet of Things, Systems, Management*

[18] F. A. Qazi, "Study of Zero Trust Architecture for Applications and Network Security," in *IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI, HONET 2022*, 2022. doi: 10.1109/HONET56683.2022.10019186.

[19] Y. Song, L. Ding, X. Liu, and M. Du, "Differential Privacy Protection Algorithm Based on Zero Trust Architecture for Industrial Internet," in *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems, ICPICS 2022*, 2022. doi: 10.1109/ICPICS55264.2022.9873739.

[20] Y. G. Wu, W. H. Yan, and J. Z. Wang, "Real identity based access control technology under zero trust architecture," in *Proceedings - 2021 International Conference on Wireless Communications and Smart Grid, ICWCSG 2021*, 2021. doi: 10.1109/ICWCSG53609.2021.00011.

[21] T. M. S. Do Amaral and J. J. C. Gondim, "Integrating Zero Trust in the cyber supply chain security," in *2021 Workshop on Communication Networks and Power Systems, WCNPS 2021*, 2021. doi: 10.1109/WCNPS53648.2021.9626299.