IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions

Vikas Prajapati
Independent Researcher
Prajapati.vikas2707@gmail.com

Abstract: *Modern cloud computing adoption patterns have caused security issues for digital identity protection and resource authorization to become critical problems. IAM functions as a core element of ZTA in cloud security since it channels access management through authentication protocols and continuous verification frameworks that authorize user permissions. NIST explains that ZTA cuts out the requirement of implicit trust and activates rule-based security through device health assessments with dynamic risk evaluation. User identification is another parameter that drives security decisions. The important security concepts ZTNA, RBAC, MFA and LPA operate within IAM to prevent cyber threats and stop unauthorized system access. The implementation of IAM in Zero Trust environments requires addressing four main hurdles: managing complex identities and their integration with old systems and the need for extra staff to manage these systems while addressing scalability requirements across multiple cloud platforms. The article examines several modern security technologies, such as Just-in-Time (JIT) access and behavior-based access control, and password-less authentication, as well as Security Information and Event Management (SIEM). Organizations that implement these security strategies will be able to enforce better protection while optimizing secure access and developing robust Zero Trust security solutions for cloud protection.*

Keywords: Zero Trust Architecture (ZTA), Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Just-In-Time (JIT) Access

I. INTRODUCTION

The majority of human interaction now takes place online. A wide variety of sectors rely on the Internet for their daily operations: healthcare, electronics, the military, business, education, and more [1]. The world would come to a halt if it weren't for the internet. Thus, the growing need for more effective and secure means of communication and network storage of large data has made cloud computing quite well-known in recent years[2]. The storage and analysis of data necessitates significant changes to cloud computing, which in turn increases the computational cost and, thus, the financial burden[3]. The phrase "cloud computing" refers to a model wherein computer and data storage resources are made available to end users on demand without requiring the client to be actively involved. It implies that the end-user has the ability to request the precise quantity of resources needed to fulfill their request[4][5]. The phrase "cloud computing" describes a distributed computing architecture in which users have distant, internet-based access to shared resources and applications [6]. You may classify these offerings in three ways. (3) Infrastructure as a Service (IaaS), (2) Platform as a Service (PaaS), and (1) Software as a Service (SaaS), companies of any size may now maximize efficiency, decrease expenses and increase agility[7]. There are certain problems with cloud computing, especially with security, despite its many advantages. Several vulnerabilities have caused organizations to suffer financial losses and data breaches, including incorrect authentication, phishing efforts, and misconfigurations[8][9].

Organizations need to change their security methods since modern cyber threats continue to develop in sophistication [10]. Traditional perimeter-based security models, which focus on defending a network's perimeter and trusting internal users, have become inadequate in the face of modern threats like insider attacks, APTs, and data breaches[11]. The Zero Trust paradigm has been popular as a solution to these problems; it promotes the idea that no person, device, or

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

application—whether on or off the network—should be trusted by default[12]. Zero Trust models rely on access permissions on rigorous user behavior monitoring and identification verification processes. Multiple internal networks and several external networks, including those of partner organizations and distant offices, may be owned by a single corporation. Both static local hosting and dynamic cloud and storage service execution are viable options for enterprise application hosting[13]. Additionally, businesses are incorporating hyperphysical systems and the IoT[14] into their IT infrastructures; alternative operating strategies, such as WFH and BYOD, may be used. System fragmentation has resulted from the pandemic's impact on the more dispersed infrastructure, which users must traverse quickly to access a huge range of applications and services [15]. A wider variety of devices and geographic regions may now access systems. A wide attack surface is associated with distributed and fragmented systems, and system administration becomes more difficult when home and office computers combine. Additionally, systems with incompatible security paradigms may be aggregated. Simultaneously, assaults have elevated in both sophistication and frequency[16].

Zero Trust security relies on IAM. IAM systems play two critical roles: managing digital identities and controlling resource access when using these user identities. The Zero Trust environment uses IAM as a real-time operation to dynamically control employee authorization provisions so that users can only access resources they need for official work reasons[17]. This study evaluates the pivotal part IAM plays within Zero Trust frameworks, along with methods to implement IAM technologies into these security models that benefit contemporary businesses.

This investigation evaluates all elements of ZTA for cloud security, including components and concepts, and challenges in implementing IAM. The paper delivers comprehensive insights into IAM frameworks as well as their authority in controlling system access and the various obstacles when implementing them in cloud-based environments. This section explains how IAM systems through ZTA achieve security improvements together with their advantageous features. The research contributes its main findings in the following manner:

- The study conducts an in-depth exploration of IAM's relationship with Zero Trust Architecture (ZTA) through its support of Least Privilege Access while also discussing continuous authentication and the access control models RBAC and ABAC.
- The main difficulties revolve around complex identity life cycles and intersection problems between legacy systems, as well as time-intensive administration demands and the scalability problems that appear when deploying across multiple cloud systems.
- The work examines contemporary security solutions, which include Multi-Factor Authentication (MFA) and password-less authentication, and Just-in-Time (JIT) access, and behavior-based dynamic access control for security development.
- Discusses the role of SIEM, EDR, MDM, and ZTNA in improving visibility, monitoring user behavior, and mitigating identity-based cyber threats.
- Proposes strategic recommendations, including AI-driven identity management, automation for identity governance, and compliance strategies to strengthen cloud security in Zero Trust environments.

A. Structure of the study

This paper explores Digital Twin (DT) technology in supply chain management. Section II introduces DT fundamentals; Section III discusses key benefits such as real-time monitoring and predictive maintenance, Section IV examines its applications across various sectors, Section V focuses on DT implementation in supply chain management, Section VI highlights operational advantages, and Section VII reviews related literature.

II. UNDERSTANDING ZERO TRUST ARCHITECTURE (ZTA)

Zero trust and ZTA are defined operationally according to NIST as follows: "Zero trust" is a set of principles that aim to reduce the uncertainty in making exact access choices for every request by treating the network as if it were hacked, while "Strafers" describes the system architecture that will actually make this possible [18]. Figure 1 depicts a simplified view of zero trust access, showing how authentication and authorization work together using Policy Decision/Enforcement Points (PDP/PEP) to manage access for each and every connection request.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Figure 1: Abstract zero trust access control.

Before access is provided to a resource in accordance with the defined rules, the access control depends on the device security posture and maybe other contextual elements that may affect the confidence level[19]. The seven pillars of a ZTA, as defined by NIST, are designed to provide the best possible outcome when ZTA is implemented.

- **Resource** – any computer service or data source.
- **Communication Security** – No matter the location, communication remains secure.
- **Session Security** – Each session is provided access to a different resource, and the same authentication and authorization process for one resource could not work for another.
- **Access Control** – Observable client identification, application, and requesting asset states are part of the dynamic policy that determines resource access.
- **Minimum-Security Posture** – Enterprise takes every precaution to guarantee the highest level of security for all owned and linked devices by constantly monitoring assets.
- **Continuous Authentication** – Dynamic and rigorously enforced authorization and authentication are in place for all resources. Organizations that plan to use ZTA may take extra precautions by implementing an ICAM system and multi-factor authentication (MFA).
- **Information Logging** – In order to fortify its security measures, the organization collects extensive data on the state of the network and communications.

A. ZTA logical components

The implementation of ZTA in an organization involves many interrelated steps. These components may be used either as services in the cloud or as ones hosted on-premises [20][21]. Further on, we'll go into detail about the policy engine and the policy administrator, the two logical components shown in Figure 2 of the policy decision point (PDP). A data plane is used for application data transmission, whereas the ZTA logical components have their own control plane [22].

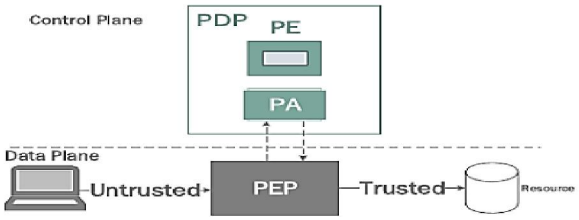

Figure 2: Core logical components of ZT

The component descriptions:

- **Policy engine (PE):** This portion is ultimately responsible for deciding whether or not a certain subject has access to a certain resource. Using company policy and external information, the PE employs a trust algorithm to grant, deny, or revoke access to the resource.
- **Policy administrator (PA):** The operation of opening and closing the channel of communication between a subject and a resource is performed by this component. Tokens and credentials used by clients to access business resources may be generated in this way, as can session-specific authentication.
- **Policy enforcement point (PEP):** Managing the lifespan of subject-to-enterprise resource connections entails starting, monitoring, and eventually terminating connections. The PEP establishes a connection with the PA so that it may receive policy updates and/or relay requests.

B. Key Principles of ZTA for Cloud Security

The following key principles of ZTA for cloud security:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

- **Least Privilege Access** – Users and devices are provided the minimal essential access to fulfill their responsibilities.
- **Micro-Segmentation** – The purpose of dividing cloud environments into smaller, more isolated portions is to restrict lateral movement in the event of a breach.
- **Continuous Authentication and Monitoring** – AI and behavior analytics are used to authenticate, authorize, and continually monitor all access requests.
- **Identity-Centric Security** – The use of multi-factor authentication (MFA) and other stringent IAM standards is strictly enforced.
- **Encryption & Secure Communication** – To ensure that no one else can access the data, it is encrypted both while it is stored and while it is still in transit.
- **Device Trust Verification** – All endpoints accessing the cloud must meet security compliance standards.
- **Assume Breach Mentality** – Security teams operate under the assumption that attackers may already be inside the network, leading to proactive threat detection and response.

C. ZTA Implementation in Cloud Security

The following Implementation of ZTA for cloud security:

- **Cloud Access Security Broker (CASB):** Monitors and controls cloud applications and data access.
- **Identity and Access Management (IAM):** Secures access based on user roles and performs robust authentication.
- **Secure Access Service Edge (SASE):** The cloud service unifies networking and security operations.
- **Endpoint Detection and Response (EDR):** Detects and mitigates threats in real-time.
- **Software-defined perimeter (SDP):** Hides network infrastructure from attackers while allowing authorized users to connect securely.

III. IDENTITY AND ACCESS MANAGEMENT (IAM) IN ZERO TRUST

IAM is an all-inclusive solution that gives users constant control over their digital selves. IDS keeps tabs on mission-critical assets and system administrators as well as other people and things in the IT environment [23][24]. IAM encompasses both "identity management" and "access management," the former of which incorporates the latter and comprises authentication and authorization processes inside an organization. Anything, including humans, is capable of claiming an identity.

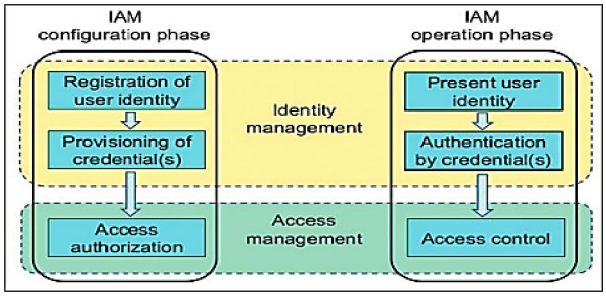

Figure 3: Phases of IAM

Both the initial setup and the operational stages of the IAM are detailed in Figure 3. The way users may access resources on AWS is controlled by permissions. When dealing with permissions, IAM might be useful. IAM, also known as RBAC, facilitates the rapid assignment of a role to a set of permissions that provide access to resources in the cloud, including data storage and the Internet[25][26]. With IAM, businesses can strengthen their compliance with regulations and guarantee the production of high-quality security systems. Additionally, it may make passwords and conventional logins more flexible, which can reduce applications' attack surfaces and prevent processing costs caused by unauthorized requests [27].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

A. Key Components of the Process of IAM

IAM experts must possess a thorough grasp of IAM situations that satisfy business requirements. Every IAM project should advance in the direction of the required final state. Authorization, consent, central user management, and authentication are the four key aspects that make up IAM. Cloud infrastructure systems with comparable capabilities are now the focus of an increasing number of business organizations [28].

- **Authentication in IAM:** The information system's security requirements state that authentication should only be used to confirm an entity's identity with acknowledged threshold trust. Reliability in authentication is ensured when the approach provides a mechanism that eliminates backdoors during implementation [29]. The goal of IAM authentication is to confirm the user's identity just once, at login. Users' biometric data, other components of the system environment, and specific business activities could be a part of intelligent authentication's hyper-method for user-attribute-based contextual authentication[5]. Soft computing is one example of an intelligent approach or technology that is used in decision processes for user characteristic matching and verification.
- **User management in IAM:** Use IAM to control who has access to what in your business. The goal of user provisioning is to assign users the resources they need to do their jobs well by creating, editing, and deleting user accounts. By assigning specific permissions to users according to their assigned responsibilities, role management simplifies administration and ensures compliance with security requirements.
- **Central user in IAM:** In IAM, a central user is an organization's one-stop-shop for all things digital, including its systems, apps, and services. A centralized user model simplifies and strengthens security by allowing a single identity to be handled across all contexts rather than managing several user accounts for various platforms.

B. Benefits of Identity and Access Management (IAM)

Following is an example of how IAM might help an enterprise's zero-trust architecture:

- **Enhanced security:** It is possible to detect and fix security issues with the aid of IAM solutions. With IAM, you may eliminate the need to manage several systems in order to discover who has revoked illegal access rights or broken your regulations. In addition, audit and regulatory bodies may utilize IAM to verify that security measures are sufficient[30]
- **Sharing of information:** The IAM provides a mechanism for managing identities and access. On one hand, the company's safety rules may cover every OS and gadget out there on the other. By using authentication methods, permissions, and verification constraints in conjunction with IAM systems, it may be possible to put an end to "privilege creep."
- **Ease of use:** Software developers, end users, and administrators all get the advantages of IAM's streamlined registration, sign-in, and user management processes. Streamlining access distribution and management is one way in which IAM improves the user experience. With the help of identity and access management, users may get access to services based on their assigned roles and permissions.
- **Productivity gains:** All access rules are centralized using IAM, simplifying access. While enabling consistent, scalable, and centralized user management, it streamlines authorization processes and accelerates the adoption of new applications.
- **Reduced IT Costs:** It may be possible to reduce operational expenses by using IAM services. Federated identity networks make it easier to administer applications by doing away with the need for local identities for external reasons. Cloud-hosted IAM services may reduce the requirement for local infrastructure purchases and upkeep. By implementing IAM technology and following associated best practices, businesses may get a competitive edge.

C. Key Concepts of IAM in Zero Trust for Cloud Security:

The following key concept of IAM in ZTA for cloud security:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

- **Least Privilege Access:** This guiding concept lessens the likelihood of unwanted access and mitigates the possible consequences of security breaches. Permissions are issued according to roles, characteristics, and contextual variables in the widely used frameworks of RBAC and Attribute-Based Access Control (ABAC).
- **Continuous Authentication & Authorization:** MFA ensures that users verify their identity using multiple credentials, adding an extra layer of security.
- **Micro-Segmentation:** Workloads and users are segmented to limit access, preventing lateral movement and reducing the attack surface in case of a breach.
- **Identity Federation & Single Sign-On (SSO):** Identity federation allows users to authenticate securely across multiple cloud platforms using a single identity provider (IdP). Users authenticate securely across multiple platforms using a single identity provider (e.g., Okta, Azure AD, AWS IAM), improving security and convenience.
- **Zero Trust Network Access (ZTNA):** A security weakness stems from traditional VPNs because they offer unrestricted network resource accessibility through Zero Trust Network Access (ZTNA). The secure Zero Trust Network Access (ZTNA) offers application access at a granular level by checking user identification along with device health status and environmental elements in the opposite direction from VPN access models. Such security framework achieves reduced exposure because it requires authentication and authorization of every device and user attempting resource access.
- **Logging & Monitoring:** SIEM tools enable access event tracking as well as anomaly detection which provides instant security event visibility through real-time monitoring. The integration of artificial intelligence into analytics systems allows the detection of suspicious activity through the identification of exceptional behavioral sequences and possible identity-targeted incursions.
- **Endpoint Security & Device Trust:** The system allows authenticated compliant devices to reach cloud resources by implementing Mobile Device Management (MDM) and endpoint detection & response (EDR) solutions for unauthorized access control.

IV. CHALLENGES IN IMPLEMENTING IAM IN ZERO TRUST FOR CLOUD SECURITY

The zero-trust architecture implements network segmentation as an essential feature that prevents vital resources from accessing unauthorized users and systems. The function enhances security breach response by decreasing the number of incidents that affect smaller geographic areas. Network segmentation in ZTA has several advantages, as stated by Yler and Viana. As a means of decreasing the attack surface, the 'never trust, always verify' principle is used to limit access to sensitive data. Improved network performance is another benefit, as is a reduction in traffic volume across the board. This also results in fast response times and little latency. Simplified compliance is another outcome of network segmentation in the zero-trust approach[31].

The security of data in cloud settings is of the utmost importance. ZTA does this by encrypting sensitive data using many methods [32][13]. Chen et al. also performed studies related to this area. Notably, ZTA employs asymmetric as well as symmetric encryption. Despite the speed advantage of symmetric encryption, asymmetric encryption provides much higher security. Should a company happen to misplace or delete its access key, the encrypted data stored in ZTA may still be recovered. In addition to facilitating authentication, encryption aids the network in meeting regulatory requirements. On the whole, it aids businesses in avoiding data breaches and making sure their networks are safe.

A. Challenges and Limitations[33]:

- **Complexity of Identity Management:** The administration of cloud-distributed identity management proves difficult because it dictates ongoing authentication and device verification tasks for all system users.
- **Access Control and Authorization Challenges:** Large organizations face elevated complexity in their efforts to establish correct user access privileges along with permission modifications and accountability tracking.
- **High Administrative Overhead:** High administrative costs accompany the Zero Trust IAM implementation since IT personnel require specialized training and additional workforce support for the extensive work activities.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

- **Continuous Monitoring and Threat Detection:** Cycle-based vigilance and threat discovery capabilities under Zero Trust protocols force organizations to select advanced threat detection tools and hire more employees for security activities.
- **Overload of Security Logs and Data Management:** Zero Trust operations create major operational difficulties when organizations must handle the abundant accumulation of security logs and security event data through powerful analytics and data management solutions.
- **Integration Issues with Legacy Systems:** Current enterprise systems from previous periods lack Zero Trust compliance hence organizations must choose either system replacements or system upgrades due to integration issues.
- **Scalability Challenges in Multi-Cloud Environments:** The implementation of Zero Trust security across distributed cloud systems faces scalability problems because different cloud providers deliver varying degrees of support while providing complex services.
- **Need for Strategic Planning and Resource Allocation:** Strategic planning combined with appropriate resource distribution determines the success of implementing Zero Trust security systems. Rational deployment of IAM within Zero Trust environments requires detailed planning along with adequate resources and funding distributions to produce sustainable security practices.

V. SOLUTIONS AND BEST PRACTICES FOR EFFECTIVE IAM IN ZERO TRUST

Organizations need to implement advanced authentication methods combined with behavior-based security algorithms together with access control methods to deploy IAM within Zero Trust Architecture successfully. Cloud protection strategies can be improved through these important sets of solutions as well as best practices that minimize security risks:

A. Multi-factor authentication (MFA) and Passwordless Authentication

MFA deployments have become essential for securing the SaaS programming environment. MFA delivery across an entire organizational system results in much fewer security events when compared to systems without complete MFA implementation.[34].

MFA effectively reduces the chances of unauthorized system entry even if passwords get stolen. MFA adoption enables SaaS providers to protect their users' information while stopping unauthorized account entries and meeting security requirements thus creating a stronger secure user experience[35]. MFA technical implementation uses three authentication elements including passwords as knowledge-based factors alongside security tokens for possession-based authentication and biometric authentications as inherence factors. The current MFA systems use risk-based authentication approaches to create time-sensitive security requirements through contextual risk evaluation mechanisms.

MFA with biometrics or hardware tokens operates as additional verification along with password-less authentication under zero-trust setups. Two password-less authentication systems are the biometric technology and FIDO2 design[36][37]. The technology defends against phishing attacks by using biometric information and encryption methods to prevent password theft. Compared to conventional password systems, password-less authentication provides organizations with a stronger defense against password theft as well as phishing attempts. For instance, FIDO2 may streamline operations by eliminating the need for one-of-a-kind biometric data storage and reducing the number of steps involved in each activity. Financial services and healthcare, which have stringent security standards, will devote more resources to ensuring customer privacy[38][39][40]. Thus, password-less technology will most certainly replace the old-fashioned Password method.

B. Continuous Authentication and Behavior Analytics

The security system relies on user behavior analysis and trust, and it features a continuous authentication process that uses known users.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

- **The Trust:** Trust is an abstract idea that expresses faith in another person's honesty or genuineness. Trust is a universal human trait that is closely linked to an individual's reputation, perception, and knowledge. We, humans, base our perception of another person's trustworthiness on their actions and reputation; trust is not a fixed quality that can be bestowed upon an individual; rather, it is not a black-and-white concept that can be measured and graded.
- **The attribution of Initial Trust:** The user's current action, location, time of conduct, and behavior history may be used to determine the initial trust heuristic.
- **The Uncertainty:** The system verifies the degree of confidence uncertainty, which is expressed as: If (Bj) = 1 - (mC + mD) = I (3) If (Bj) = i is the level of user-assigned uncertainty about the behavior Bj. If the user's behavior falls within the range of values between the initial minimal diffidence (mD) and the initial minimal trust (mC), then the system will utilize this evidence to decide whether to trust the user.
- **The attribution of the subsequent trust:** Two phases make up the system's assignment of trust. Initially, the system records the conduct in its database and gives it a low degree of confidence due to its lack of understanding of the behavior. Finally, it accounts for and saves the information that was recorded.

A person's behavior analysis may be supported by rules that examine the factors that impact human behavior. Understanding and isolating the components of an event is the first step in scientifically analyzing human behavior. Next, they need to identify the features and dimensions of the context in which the behavior takes place, and finally, they need to describe the changes that occurred as a result of interactions with the surrounding environment, space, time, and opportunities [41]. Accordingly, the environment and the physical and virtual spaces provide the circumstances for certain behaviors. Human behavior is determined by contextual knowledge, past behavioral history, prior reinforcement of behavior, and the individual's conduct.

C. Least Privilege Access and Just-In-Time (JIT) Access

The temporal dimension of least privilege should be considered. Temporary access granted to a user principal is often considered more secure than permanent access granted to the same principal for the same authorization. By limiting your access to an action's execution to only the moment it's required, you may adhere to the principle of least privilege. Figure 4 illustrates how a JIT approach to permissions and the concurrent improvement of superfluous permissions get us closer to the least privilege. However, keep in mind that not every organization may find JIT to be a good match due to the cost of maintaining temporary access and the productivity cost of having to ask every time[42].

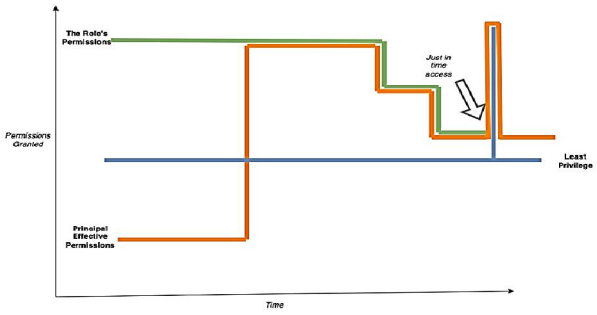

Figure 4: Just-in-time Least Privilege Model

A Privileged Access Management (PAM) system is similar to this JIT method; with PAM, users may "check out" and "check-in" credentials that provide them access to a shared and often sensitive system. Still, the JIT method lets the actor check out authorization to be authorized to execute the action rather than a credential. The JIT method, on the other hand, may enable the principal to verify if a role can be assumed with the required authorization to carry out the activity. Additionally, it is important to continuously improve the permissions given for that JIT access.

VI. LITERATURE OF REVIEW

This section highlights the IAM in zero trust architecture for cloud security with the analysis of significance and key findings. Also, provide a summary in Table I:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Iordache, Dragomir and Marian (2022) pave the way for biometric multi-factor authentication to be standard practice for strengthening the cyber defenses of government agencies. A more granular approach to data and network security might be achieved by rethinking network design to support a ZTA methodology, which would occur in line with the widespread adoption of this solution. Furthermore, the proposed system would adhere to the present standards and limitations of the GDPR [43].

Vai et al. (2023) detail a method for developing mission-critical embedded systems' survivability using ZTA. Functionality, performance, and survivability are being co-designed with security and resilience characteristics by using the ZTA principle of "never trust, always verify" throughout the design process. In addition to outlining the ZTA method, the article provides a design example of a tiny drone with an emphasis on survival[44].

Sajid (2023) presents a risk-based method to apply zero-trust security concepts to 5G system core networks. It begins by discussing the issues the 5G network has in adopting a typical security strategy and the 3GPP and allied entities' study on NIST's Zero trust tenets. This study showed promise and will guide enterprises adopting private 5G to leverage their enterprise security controls and maintain zero trust security. It will also provide wireless standard bodies like 3GPP and GSMA with recommendations for the next release[45].

Xu, Di and Song (2024) established a cloud-edge-gateway collaborative ZTA based on the distributed ZTA, named CEGC-ZTA, for smart factories. They design the workflow of CEGC-ZTA based on the software-defined perimeter (SDP) model. An implementation case of CEGC-ZTA is given in a smart factory scenario. Simulations and theoretical analysis show that CEGC-ZTA has a superior performance in terms of both security and efficiency[46].

Rajasekar et al. (2024) focus on the implementation of DLT for data protection applications that are based on a solid dataset and decentralized security procedures in cloud environments. Moreover, DLT also does IAMs in a way that is decentralized, data sharing in a manner that is secure, and compliance with regulatory frameworks. The proposed architecture is genuinely a big jump toward protecting cloud security from centralized control interruptions and, thus, enhancing resilience and stability in cloud computing[47].

Singh, Kuzminykh and Ghita (2024) try to summarize, from the beneficiaries' point of view, the existing perception of and security concerns with IAM solutions. Default settings, inadequate handling of non-human identities (e.g., service accounts), bad certificate management, improper API setup, and a lack of comprehensive log analysis were the primary obstacles faced by cloud-based identity and access management systems. The survey also found that 41% of people still think on-premises solutions are more secure than cloud-based ones, even though cloud-based IAM solutions are becoming better all the time [48].

Table 1: Literature of review based on IAM in Zero Trust Architecture for Cloud Security

Author(s) & Year	Focus Area	Key Contributions	Security Aspects Covered	Implementation Scenario	Limitations	Future Work
Iordache, Dragomir & Marian (2022)	Multi-factor authentication (MFA) in Public Institutions	Proposes biometric MFA for enhancing ZTA-based cybersecurity in public networks.	MFA, GDPR Compliance, Granular Access Control	Public Institution Security	Does not address implementation complexity.	Exploring AI-driven adaptive authentication methods.
Vai et al. (2023)	ZTA for Mission-Critical Embedded Systems	Uses ZTA as a tool for security and resilience in embedded system design.	Identity Verification, Access Control, System Resilience	Small Drone for Survivability	Limited to embedded systems applications.	Applying ZTA in broader IoT and industrial systems.
Sajid et al.	Risk-Based	Applies ZTA	5G Security,	5G Core	Requires	Real-world

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

(2023)	ZTA for 5G Networks	principles to secure 5G core networks; proposes attack vector analysis.	Network Hardening, Policy Enforcement	Network & Private 5G Enterprises	validation for large-scale telecom adoption.	implementation and testing in telecom networks.
Xu, Di & Song (2024)	Cloud-Edge-Gateway Collaborative ZTA (CEGC-ZTA)	Introduces SDP-based ZTA model for improved security and efficiency in smart factories.	Access Control, SDP Model, Cloud-Edge Security	Smart Factory Security	Focused on industrial use; lacks cloud-specific discussion.	Extending to multi-cloud and hybrid cloud environments.
Rajasekar et al. (2024)	Decentralized Identity & Access Management (IAM) using DLT	Proposes IAM using Distributed Ledger Technology (DLT) to improve cloud security.	Decentralized IAM, Data Sharing Security, Compliance	Cloud Computing Environments	Implementation complexity in real-world cloud infrastructures.	Optimizing DLT-based IAM for high-performance computing.
Singh, Kuzminykh and Ghita (2024)	Security Issues in IAM Solutions	Identifies challenges in cloud-based IAM (e.g., poor API config, log analysis gaps).	Default Configurations, Non-Human Identity Management, Compliance	Cloud IAM Solutions	41% of respondents preferred on-premise IAM over cloud IAM.	Developing automated IAM security monitoring tools.

VII. CONCLUSION

The adoption of Identity and Access Management (IAM) in Zero Trust Architecture (ZTA) is crucial for securing cloud environments by eliminating implicit trust and enforcing dynamic, context-aware access controls. This review highlights how IAM enhances security through principles such as least-privilege access, continuous authentication, micro-segmentation, and identity-based security. Despite challenges like high administrative overhead, integration with legacy systems, and scalability in multi-cloud environments, solutions such as Multi-Factor Authentication (MFA), Just-in-Time (JIT) access, Zero Trust Network Access (ZTNA), and AI-driven behavior analytics help organizations strengthen security while minimizing risks. The successful establishment of Zero Trust cloud security depends on enterprises utilizing progressive identity authentication systems, real-time watch procedures and adjustable access systems. Future studies need to concentrate on AI threat evaluation of identities, distributed identity mechanisms, and robotic access management to make zero-trust platforms more efficient.

REFERENCES

[1] S. Murri, S. Chinta, S. Jain, and T. Adimulam, "Advancing Cloud Data Architectures: A Deep Dive into Scalability, Security, and Intelligent Data Management for Next-Generation Applications," Well Test. J., vol. 33, no. 2, pp. 619–644, 2024.

[2] B. Boddu, "Securing and Managing Cloud Databases for Business - Critical Applications," J. Eng. Appl. Sci. Technol., 2025.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

[3] M. Gopalsamy, S. Cyber, and S. Specialist, "Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection," IJRAR, vol. 8, no. 1, pp. 187–192, 2021.
[4] D. Gangwani, H. A. Sanghvi, V. Parmar, R. H. Patel, and A. S. Pandya, "A Comprehensive Review on Cloud Security Using Machine Learning Techniques," Intell. Syst. Ref. Libr., vol. 240, no. January 2024, pp. 1–24, 2023, doi: 10.1007/978-3-031-28581-3_1.
[5] S. R. Thota, S. Arora, and S. Gupta, "Hybrid Machine Learning Models for Predictive Maintenance in Cloud-Based Infrastructure for SaaS Applications," 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691295.
[6] A. Goyal, "Optimising Cloud-Based CI / CD Pipelines : Techniques for Rapid Software Deployment," TIJER, vol. 11, no. 11, pp. 896–904, 2024.
[7] K. Rajchandar, M. Ramesh, A. Tyagi, S. Prabhu, D. S. Babu, and A. Roniboss, "Edge Computing in Network-based Systems: Enhancing Latency-Sensitive Applications," in 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), 2024, pp. 462–467. doi: 10.1109/IC3I61595.2024.10828607.
[8] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," Electron., 2024, doi: 10.3390/electronics13050865.
[9] N. P. Hirenkumar Mistry Kumar Shukla, "Securing the Cloud: Strategies and Innovations in Network Security for Modern Computing Environments," Int. Res. J. Eng. Technol., vol. 11, no. 04, p. 11, 2024.
[10] S. S. S. Neeli, "A Hands-on Guide to Data Integrity and Privacy for Database Administrators," Int. J. Sci. Res. Eng. Manag., vol. 6, no. 09, p. 7, 2022.
[11] Qi An Xin and Gartner, "Zero Trust Architecture and Solutions," Gartner, 2020.
[12] M. Ahmed and K. Petrova, "A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments," in Workshop on Information Security and Privacy (WISP), 2020.
[13] Pranav Khare and Abhishek, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.
[14] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, 2021, doi: DOI: 10.48175/IJARSCT-6268B.
[15] E. B. Fernandez and A. Brazhuk, "A critical analysis of Zero Trust Architecture (ZTA)," Comput. Stand. Interfaces, vol. 89, 2024, doi: 10.1016/j.csi.2024.103832.
[16] D. P and S. S. A, "A Zero Trust Framework Security to Prevent Data Breaches and Mitigate the Cloud Network Attacks," Int. J. Res. Appl. Sci. Eng. Technol., 2022, doi: 10.22214/ijraset.2022.42976.
[17] R. Johnny, "Identity and Access Management in Zero Trust Frameworks," no. January, 2019.
[18] H. Sinha, "The Identification of Network Intrusions with Generative Artificial Intelligence Approach for Cybersecurity," J. Web Appl. Cyber Secur., vol. 2, no. 2, pp. 20–29, Oct. 2024, doi: 10.48001/jowacs.2024.2220-29.
[19] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," 2022. doi: 10.1109/ACCESS.2022.3174679.
[20] Vashudhar Sai Thokala, "Scalable Cloud Deployment and Automation for E-Commerce Platforms Using AWS, Heroku, and Ruby on Rails," Int. J. Adv. Res. Sci. Commun. Technol., pp. 349–362, Oct. 2023, doi: 10.48175/IJARSCT-13555A.
[21] N. Patel, "Quantum Cryptography In Healthcare Information Systems: Enhancing Security In Medical Data Storage And Communication," J. Emerg. Technol. Innov. Res., vol. 9, no. 8, pp. g193–g202, 2022.
[22] S. Rose and O. Borchert, "Zero Trust Architecture," Control. Priv. Use Data Assets, pp. 127–134, 2022, doi: 10.1201/9781003189664-11.
[23] A. Caballero, Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems. Elsevier Inc., 2017. doi: 10.1016/B978-0-12-803843-7.00024-7.
[24] R. K. Arora, A. Tiwari, and Mohd.Muqeem, "Advanced Blockchain-Enabled Deep Quantum Computing Model for Secured Machine-to-Machine Communication," Sep. 2024. doi: 10.21203/rs.3.rs-5165842/v1.
[25] V. S. Thokala, I. Researcher, S. Pillai, and I. Researcher, "Optimising Web Application Development Using Ruby on Rails , Python, and Cloud-Based Architectures," vol. 9, no. 12, pp. 630–639, 2024.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

[26] B. Boddu, "Ensuring Data Integrity and Privacy: A Guide for Database Administrators," https://www.ijfmr.com/research-paper.php?id=10880, vol. 4, no. 6, p. 6, 2022.
[27] S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," Int. J. Curr. Eng. Technol., vol. 12, no. 6, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.11.
[28] S. Murri, "Data Security Environments Challenges and Solutions in Big Data," Int. J. Curr. Eng. Technol., vol. 12, no. 6, pp. 565–574, 2022.
[29] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A Review on Authentication Methods - Archive ouverte HAL," Aust. J. Basic Appl. Sci., no. August 2015, pp. 95–107, 2013.
[30] 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.
[31] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," J. Eng. Res. Reports, vol. 26, no. 2, pp. 215–228, 2024, doi: 10.9734/jerr/2024/v26i21083.
[32] V. S. Thokala, "A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications," Int. J. Res. Anal. Rev., vol. 8, no. 4, pp. 383–389, 2021.
[33] H. Sharma, "Zero Trust in the Cloud : Implementing Zero Trust Architecture for Enhanced Zero Trust in the Cloud : Implementing Zero Trust Architecture for Enhanced Cloud Security," no. September, 2024, doi: 10.56472/25832646/JETA-V2I2P110.
[34] M. Manoharan, "Multi-Factor Authentication and Passwordless Authentication : The Future of SAAS Security," vol. 8, no. 1, pp. 509–547, 2025.
[35] T. K. K. and S. Rongala, "Implementing AI-Driven Secure Cloud Data Pipelines in Azure with Databricks," Nanotechnol. Perceptions, vol. 20, no. 15, pp. 3063–3075, 2024, doi: https://doi.org/10.62441/nano-ntp.vi.4439.
[36] Y. L. Maxine, "Analysis of Multi-factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State , Challenges , and Future Trends," vol. 186, no. 57, pp. 30–36, 2024.
[37] M. H. A. S. Ashish Shiwlani, Sooraj Kumar, Samesh Kumar, Syed Umer Hasan, "Transforming Healthcare Economics: Machine Learning Impact on Cost Effectiveness and Value-Based Care," Pakistan J. Life Soc. Sci., 2024.
[38] M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.
[39] Sagar Bharat Shah, "Improving Financial Fraud Detection System with Advanced Machine Learning for Predictive Analysis and Prevention," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 10, no. 6, pp. 2451–2463, Nov. 2024, doi: 10.32628/CSEIT24861147.
[40] R. Arora, S. Gera, and M. Saxena, "Impact of Cloud Computing Services and Application in Healthcare Sector and to provide improved quality patient care," IEEE Int. Conf. Cloud Comput. Emerg. Mark. (CCEM), NJ, USA, 2021, pp. 45–47, 2021.
[41] I. Brosso, A. La Neve, G. Bressan, and W. V. Ruggiero, "A Continuous Authentication System Based On User Behavior Analysis," ARES 2010 - 5th Int. Conf. Availability, Reliab. Secur., pp. 380–385, 2010, doi: 10.1109/ARES.2010.63.
[42] M. K. Carter, "Techniques To Approach Least Privilege," IDPro Body Knowl., vol. 1, no. 9, 2022, doi: 10.55621/idpro.88.
[43] C. A. Iordache, A. V. Dragomir, and C. V. Marian, "Public Institutions Updated Enhanced Biometric Security, Zero Trust Architecture and Multi-Factor Authentification," in 2022 International Symposium on Electronics and Telecommunications (ISETC), 2022, pp. 1–4. doi: 10.1109/ISETC56213.2022.10010127.
[44] M. Vai et al., "Zero Trust Architecture Approach for Developing Mission Critical Embedded Systems," in 2023 IEEE High Performance Extreme Computing Conference, HPEC 2023, 2023. doi: 10.1109/HPEC58863.2023.10363531.
[45] T. Sajid, "Securing 5G Cloud Native NFV Architecture with Zero Trust Security," in 2023 IEEE Future Networks World Forum (FNWF), 2023, pp. 1–5. doi: 10.1109/FNWF58287.2023.10520441.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

[46] Z. Xu, B. Di, and L. Song, "Design of Cloud-Edge-Gateway Collaborative Zero-Trust Architecture and Workflow for Smart Factories," in 2024 IEEE International Workshop on Radio Frequency and Antenna Technologies (iWRF&AT), 2024, pp. 335–339. doi: 10.1109/iWRFAT61200.2024.10594530.
[47] P. Rajasekar, K. Kalaiselvi, R. Shanmugam, S. Tamilselvan, and A. P. Pandian, "Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments," in 2024 Second International Conference on Advances in Information Technology (ICAIT), 2024, pp. 1–6. doi: 10.1109/ICAIT61638.2024.10690718.
[48] A. P. Singh, I. Kuzminykh, and B. Ghita, "Industry Perception of Security Challenges with Identity Access Management Solutions," in 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2024, pp. 312–315. doi: 10.1109/BlackSeaCom61746.2024.10646296.