International Journal of Scientific Engineering and Science
Volume 10, Issue 5, pp. 14-17, 2026. ISSN (Online): 2456-7361

An Integrated Approach to Identity and Access Management and Zero Trust for Security and Compliance

Djanilda Fortes[1], Ludmila Gomes[1], Marcelo Correia[1], Fredson Bandeira[1], Romário Dias[1], Hugo Barbosa[2]
[1]Master's Student in Cybersecurity, Department of Computer Engineering, Mindelo University, São Vicente, Cape Verde
[2]Assistant Professor, Department of Computer Engineering, School of Management and Technology - ESTG/IPP, Porto, Portugal

Abstract —*The rapid evolution of digital environments, driven by cloud computing, remote work, and increasingly sophisticated cyber threats, has rendered traditional perimeter-based security models insufficient. Identity and Access Management (IAM), combined with Zero Trust Architecture (ZTA), has emerged as a fundamental paradigm for securing modern systems. This paper provides a comprehensive review of the digital identity lifecycle, IAM governance, Zero Trust principles, and their role in ensuring compliance with the General Data Protection Regulation (GDPR). The study identifies key challenges, including weak authentication mechanisms, excessive access privileges, and insufficient monitoring practices. Furthermore, the paper highlights that the integration of IAM governance, Zero Trust principles, and passwordless authentication can significantly enhance security posture and organizational resilience. However, implementation challenges related to complexity, integration, and user experience remain significant.*

Keywords— *Cloud Security; Digital Identity; GDPR; IAM; Zero Trust*

I. INTRODUCTION

The rapid advancement of digital technologies has fundamentally reshaped organizational infrastructures, particularly with the adoption of cloud computing, mobile access, and remote work environments [1], [2]. These changes have significantly expanded the attack surface and increased system complexity, creating new challenges for securing information systems and managing access to critical resources.

In addition to technological evolution, organizations are increasingly dependent on interconnected systems and third-party services, which further complicate the security landscape. The proliferation of devices, including personal and IoT devices, has introduced additional entry points for potential attacks, making traditional security approaches less effective in mitigating modern threats.

Traditional perimeter-based security models are no longer sufficient in distributed environments, where users and devices operate beyond organizational boundaries [3]. In such contexts, access to resources can occur from multiple locations and devices, requiring a shift toward identity-driven security models.

Identity and Access Management (IAM) plays a central role in controlling access to digital resources by ensuring that only authenticated and authorized entities can interact with critical systems. Modern IAM solutions support advanced capabilities such as multi-factor authentication and adaptive access control, enhancing security in dynamic infrastructures. They also enable access decisions based on identity, context, and risk [4].

At the same time, regulatory frameworks such as the General Data Protection Regulation (GDPR) impose strict requirements on data protection and accountability [5]. Organizations are required to implement robust access control mechanisms, ensure traceability of user actions, and protect sensitive data from unauthorized access.

Zero Trust Architecture (ZTA) introduces a paradigm shift by eliminating implicit trust and enforcing dynamic validation of identity and context [3], [6]. Unlike traditional models, Zero Trust assumes that threats may exist both inside and outside the network, requiring continuous evaluation of users, devices, and activities.

Furthermore, the convergence of IAM and Zero Trust represents a comprehensive strategy for addressing modern cybersecurity challenges. By combining identity governance, adaptive authentication, and context-aware access control, organizations can build resilient security architectures capable of adapting to evolving threats and complex environments.

This paper contributes by presenting an integrated identity-centric security framework that combines IAM and Zero Trust principles, highlighting their complementary roles in enhancing security and ensuring regulatory compliance. In addition, the increasing regulatory pressure and the growing sophistication of cyber threats require organizations to adopt proactive and adaptive security strategies. This reinforces the need for a unified approach that integrates identity governance, continuous risk assessment, and advanced access control mechanisms.

This evolving landscape further highlights the importance of adopting flexible and scalable identity-driven security strategies capable of ensuring consistent protection across diverse and highly interconnected digital environments.

II. THEORETICAL BACKGROUND

A. Digital Identity and Lifecycle

http://ijses.com/
All rights reserved

Digital identity represents the unique digital representation of an entity, composed of attributes such as credentials, personal data, and behavioral characteristics [7]. This concept extends beyond simple user identification, encompassing a wide range of elements that collectively define how an entity is recognized and authenticated within digital systems.

These attributes may include both biographical and biometric data, which are essential for modern authentication mechanisms [8]. Biographical data refers to static information such as names and identification numbers, while biometric data includes unique physical or behavioral characteristics such as fingerprints or typing patterns. The integration of these attributes enhances the reliability of authentication processes.

Modern digital identity systems increasingly incorporate contextual and behavioral data, such as login patterns, device usage, and geographic location. These additional layers allow systems to build more accurate identity profiles and detect anomalies that may indicate potential security threats.

The lifecycle of digital identity includes stages such as creation, identity proofing, authentication, maintenance, and deactivation [9]. Each stage plays a critical role in ensuring the security and integrity of identity management systems. Failure to properly manage this lifecycle can result in vulnerabilities such as orphaned accounts or unauthorized persistence [10].

Dynamic authentication mechanisms enable continuous identity evaluation based on real-time contextual factors [11]. This approach reflects the evolution of identity management from static verification to adaptive and risk-based models.

B. Identity and Access Management (IAM) and Governance

IAM is a framework that manages digital identities and enforces access control across systems [4]. It provides a structured approach to ensuring that only authorized users, devices, and services can access specific systems and data.

IAM systems manage identity provisioning, credential management, and access revocation, ensuring alignment between access rights and organizational roles. By automating these processes, IAM reduces human error and improves consistency in access control policies.

IAM is based on authentication, authorization, and auditing (AAA), ensuring secure and traceable access control [12]. Authentication verifies identity, authorization determines access levels, and auditing provides visibility through activity logging.

Modern IAM systems extend to distributed environments, supporting users, devices, and services across cloud and hybrid infrastructures [1], [13]. Capabilities such as single sign-on (SSO), federated identity, and multi-factor authentication improve both security and usability.

IAM governance introduces mechanisms such as role-based access control (RBAC), least privilege, and segregation of duties [14]. These principles reduce the risk of unauthorized access and ensure that permissions align with job responsibilities.

However, challenges such as excessive access rights and limited visibility into access activities remain significant risks [15]. Without proper oversight, organizations may struggle to detect anomalies or respond effectively to security incidents.

C. Zero Trust Architecture

Zero Trust Architecture is based on the principle of "never trust, always verify," requiring dynamic validation of identity, device posture, and contextual factors [3], [6]. It assumes that threats may exist both inside and outside the network.

Access decisions are evaluated dynamically based on identity, device health, and risk level. This enables organizations to implement adaptive security policies and reduce the likelihood of unauthorized access.

Key principles include ongoing authentication, least privilege enforcement, and real-time monitoring [16]. Ongoing authentication mechanisms ensure that users are continuously validated throughout sessions, allowing early detection of anomalies.

Micro-segmentation further enhances security by dividing networks into smaller segments, limiting lateral movement within systems.

Despite its advantages, Zero Trust implementation presents challenges related to complexity, integration, and user experience [17]. Organizations must balance strong security controls with usability to avoid operational friction.

D. IAM, Zero Trust, and GDPR Compliance

In the context of GDPR compliance, identity governance mechanisms play a crucial role in ensuring controlled and auditable access to personal data [5]. These mechanisms support accountability, traceability, and data protection.

Organizations are required to implement technical and organizational measures such as access control, monitoring, and encryption [5], [18]. These measures align with GDPR principles, including data minimization and confidentiality.

Zero Trust enhances compliance by enforcing continuous evaluation of access conditions and minimizing unauthorized access [3], [6]. The combination of identity governance and adaptive access control enables fine-grained protection of sensitive data.

However, compliance requires continuous evaluation and improvement. Organizations must regularly review policies, update security controls, and ensure user awareness.

E. Emerging Trends: Cloud IAM and Passwordless Authentication

Cloud computing has increased the demand for scalable IAM solutions that support distributed environments [1], [2]. Identity management now extends beyond human users to include devices and services.

Cloud IAM enables centralized policy enforcement, improving visibility and reducing administrative complexity. This is essential in cloud-based ecosystems where access control must remain consistent across platforms.

Passwordless authentication has emerged as a secure alternative to traditional methods, using biometrics and cryptographic authentication [19]. This reduces vulnerabilities associated with password-based systems.

Although adoption challenges remain, these technologies significantly enhance both security and user experience. Taken together, these theoretical foundations highlight the increasing convergence between identity management, adaptive security models, and regulatory requirements. The evolution of IAM

http://ijses.com/
All rights reserved

and Zero Trust reflects a broader shift toward identity-centric security, where access decisions are no longer static but continuously influenced by contextual and risk-based factors. This convergence reinforces the need for integrated frameworks capable of supporting secure, scalable, and compliant operations in distributed and cloud-based environments.

III. Analysis and Discussion

The analysis reveals a significant gap between theoretical security frameworks and their practical implementation within organizations. While Identity and Access Management (IAM) and Zero Trust Architecture (ZTA) are widely recognized as best practices in modern cybersecurity, many organizations continue to rely on weak authentication mechanisms and outdated practices that do not adequately address current threat landscapes [15], [20]. This discrepancy highlights the difficulty of translating well-established theoretical models into effective operational strategies.

One of the most critical issues identified is the persistence of traditional authentication methods, particularly password-based systems, which remain highly vulnerable to attacks such as phishing, credential stuffing, and brute force [20]. Despite the availability of more secure alternatives, such as multi-factor and passwordless authentication, organizations often delay adoption due to cost, complexity, or resistance to change. This results in a security posture that does not reflect the capabilities of modern identity-centric frameworks.

Excessive privilege allocation and lack of monitoring remain critical issues, increasing vulnerability to cyberattacks [15]. In many organizations, users accumulate access rights over time, leading to privilege creep, where permissions exceed actual job requirements. This creates opportunities for attackers to exploit compromised accounts and escalate privileges within systems. Furthermore, insufficient monitoring of access activities limits the ability to detect anomalies or respond promptly to potential threats.

Another important observation is the lack of integration between IAM and broader security strategies, such as Zero Trust. Their combined implementation enables more adaptive and resilient security strategies, where IAM serves as the operational foundation for identity governance, while Zero Trust enhances these capabilities through dynamic and context-aware access control.

This integration also has measurable organizational impact. Industry reports highlight the financial and operational impact of poor identity governance, reinforcing the need for stronger IAM strategies [21]. Data breaches resulting from compromised credentials or excessive privileges can lead to significant financial losses, reputational damage, and regulatory penalties. These consequences emphasize the importance of investing in robust identity management and governance frameworks.

In addition to technological challenges, organizational factors play a crucial role in the effectiveness of IAM and Zero Trust implementations. The successful adoption of these frameworks requires a cultural shift within organizations, where security is treated as a shared responsibility rather than solely an IT concern. This includes user awareness, employee training, and clear definition of roles and responsibilities.

The successful implementation of IAM and Zero Trust requires not only technological solutions but also organizational commitment, user awareness, and continuous improvement [17]. Continuous evaluation of access policies, regular audits, and the use of identity analytics are essential for maintaining an effective security posture. Organizations must also adopt a proactive approach, anticipating potential threats and adapting their security strategies accordingly.

Furthermore, the increasing adoption of cloud computing and distributed systems has intensified the need for identity-centric security approaches. As traditional network boundaries disappear, identity becomes the primary control point for securing access to resources. This reinforces the importance of integrating IAM, Zero Trust, and advanced authentication mechanisms into a unified security strategy.

Overall, the analysis demonstrates that while IAM and Zero Trust provide a strong theoretical foundation for modern cybersecurity, their effectiveness depends on proper implementation, integration, and continuous adaptation. Organizations that successfully address these challenges will be better positioned to mitigate risks, enhance security, and comply with regulatory requirements.

These observations also indicate that organizations must strengthen the integration between security governance and operational practices to ensure consistent enforcement of access policies. The alignment of identity management processes with real-time monitoring and risk assessment mechanisms is essential to improve decision-making and reduce exposure to evolving threats. This approach enables a more resilient and proactive security posture.

Table 1 summarizes the proposed integrated IAM and Zero Trust framework, highlighting the key components and their roles in enforcing secure and compliant access to organizational resources. The table provides a structured overview of how identity governance, continuous validation, and monitoring mechanisms interact to support a unified security approach.

Table I. Summary of Integrated IAM and Zero Trust Framework

Component	**Role**
Entities	Sources of access (users, devices, apps)
IAM	Identity management and access control
Zero Trust	Continuous and context-aware validation
Context & Risk	Evaluation of device, behavior, and risk
Monitoring	Logging, detection, and compliance
Resources	Protected systems, data, and services

As shown in Table 1, the integration of IAM and Zero Trust enables a layered and adaptive security model, where access decisions are continuously evaluated based on identity, context, and risk factors. These findings also suggest that organizations must move beyond isolated security controls and adopt integrated, identity-centric strategies that combine

http://ijses.com/
All rights reserved

governance, continuous risk assessment, and adaptive access mechanisms. The effective alignment of IAM and Zero Trust principles not only strengthens access control but also enhances visibility, accountability, and incident response capabilities. As threat landscapes continue to evolve, the ability to dynamically evaluate access conditions and respond to emerging risks will become a critical requirement for sustainable cybersecurity practices.

These findings demonstrate that addressing current security challenges requires a coordinated approach that combines governance, continuous risk evaluation, and adaptive access control. Organizations must align technical capabilities with strategic objectives to ensure that security measures remain effective, scalable, and responsive to evolving threats.

IV. CONCLUSION

Identity-driven security models are essential in modern cybersecurity. The integration of IAM, Zero Trust Architecture, and GDPR compliance provides a comprehensive framework for protecting digital assets [3], [5].

While these frameworks offer strong theoretical foundations, their effectiveness depends on proper implementation, governance, and continuous monitoring.

Future developments are expected to focus on decentralized identity, artificial intelligence-driven authentication, and improved interoperability between identity systems [11], [19]. Ultimately, the integration of IAM and Zero Trust represents a critical step toward building resilient, adaptive, and identity-driven security architectures capable of addressing the challenges of modern digital environments.

Moreover, the growing complexity of digital ecosystems and the increasing interconnection of systems highlight the urgency of adopting scalable and interoperable security solutions. Future research should also explore the integration of artificial intelligence and machine learning techniques to enhance identity analytics, automate access decisions, and improve threat detection capabilities. In this context, the continuous evolution of identity-centric security frameworks will play a crucial role in enabling organizations to effectively manage risk, ensure compliance, and maintain trust in increasingly dynamic and distributed environments.

REFERENCES

[1] A. Sabahi, “Cloud Computing Security Threats and Responses,” IEEE 3rd International Conference on Communication Software and Networks, pp. 245–249, 2011.
[2] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” IEEE International Conference on Cloud Computing Technology and Science, pp. 693–702, 2010.
[3] S. Rose, O. Borchert, M. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST SP 800-207, National Institute of Standards and Technology, 2020.
[4] D. Ferraiolo, D. Kuhn, and R. Chandramouli, Role-Based Access Control, Artech House, 2007.
[5] European Parliament and Council, “General Data Protection Regulation (EU) 2016/679,” Official Journal of the European Union, 2016.
[6] Forrester Research, “The Zero Trust eXtended Ecosystem,” 2020.
[7] K. Cameron, “The Laws of Identity,” Microsoft Corporation, 2005.
[8] National Institute of Standards and Technology, “Digital Identity Guidelines,” NIST SP 800-63-3, 2017.
[9] IDPro, “Identity Management Body of Knowledge,” 2022.
[10] World Bank, “Digital Identity Toolkit,” 2019.
[11] M. Sporny et al., “Verifiable Credentials Data Model 1.0,” W3C Recommendation, 2021.
[12] V. C. Hu et al., “Assessment of Access Control Systems,” NIST Report, 2006.
[13] Microsoft, “Identity Fundamentals,” Microsoft Learn, 2025.
[14] ENISA, “Digital Identity and Trust Services,” 2023.
[15] Gartner, “Market Guide for Identity Governance and Administration,” 2023.
[16] Microsoft, “Zero Trust Security Model,” Microsoft Learn, 2025.
[17] Chinamanagonda, S., “Zero Trust in Cloud Environments,” 2022.
[18] ISO/IEC, “ISO/IEC 27001: Information Security Management Systems,” 2013.
[19] FIDO Alliance, “FIDO2: Moving Beyond Passwords,” 2019.
[20] D. Florêncio and C. Herley, “A Large-Scale Study of Web Password Habits,” WWW Conference, 2007.
[21] IBM Security, “Cost of a Data Breach Report,” 2023.
[22] S. Mushtaq et al., “A Systematic Literature Review on the Implementation and Evaluation of Zero Trust Architecture,” Sensors, vol. 25, no. 19, 2025.
[23] A. Soni et al., “A Comprehensive Review and Comparative Analysis of Zero Trust Architecture: Evolution, Implementation Strategies, and Key Challenges,” Journal of Information Security, 2025.
[24] Y. Akharchaf, “Zero Trust Architecture in Cloud Security: Challenges and Implementation,” 2025.
[25] D. Guha, “A Practical Implementation of Zero Trust Architecture for Secure Cloud Systems,” IEEE Conference, 2025.
[26] K. Denzel, “A Survey of Security in Zero Trust Network Architectures,” GSC Advanced Research and Reviews, 2025.

http://ijses.com/
All rights reserved