American Research Journal of Computer Science and Information Technology

Volume 8, Issue 1, 6-11 Pages
Research Article | Open Access
ISSN (Online)- 2572-2921
DOI : 10.21694/2572-2921.25002

Redefining the High-Level Framework for Identity and Access Management in Cyber Security

Sandeep Singh

Senior System and Infrastructure Engineer Information Security, Bentonville, USA.

ABSTRACT

The article discusses approaches to improving identity and access management, adapted to modern challenges related to technology development. The research is aimed at identifying the problems of traditional methods and developing solutions based on modern tools, including artificial intelligence, cloud services, and the concept of complete abandonment of trust.

The article also analyzes the transformation of the architecture of identity and access management systems (hereinafter - IAM) in the context of technological changes. IAM components adapt to the challenges posed by the introduction of new solutions and technologies.

Technological development, including cloud platforms, artificial intelligence algorithms, and innovative systems, has changed the architecture of IAM. It began to adapt to distributed environments, cyber threats, and new attack scenarios. In turn, the creation of platforms with flexibility, security, and adaptability helps organizations protect information resources, confront new threats, and maintain sustainability in the digital world.

The results of the study confirm the ability of the proposed methods to ensure data protection, minimize the likelihood of attacks, and comply with regulatory requirements. The materials are intended for cybersecurity specialists, access control system developers, and employees working with digital transformation.

The conclusion focuses on the effectiveness of the proposed approaches to the organization of access control that meet modern requirements of the digital environment, strengthen information protection, and facilitate adaptation to new challenges.

KEYWORDS: *identity and Access Management, IAM Framework, Identity Security, Cybersecurity, Digital Transformation.*

INTRODUCTION

Modern digitalization necessitates a reevaluation of approaches to information security, emphasizing identity management and access control. The development of cloud technologies, the proliferation of remote work formats, and the increasing complexity of digital infrastructures expand the volume of processed data and create new challenges for data protection. Outdated access management architectures often prove ineffective against emerging threats. IAM platform architectures represent adaptive structures that enhance information security through centralized account management.

Scientific studies highlight the importance of addressing account-targeted attacks and unauthorized information access. Statistical data confirm that issues related to identification processes constitute a significant portion of security threats. The application of technologies such as automated analysis and distributed ledgers offers opportunities to improve security levels. However, their implementation requires a systematic approach tailored to specific tasks.

Organizations transitioning to digital technologies under the influence of global changes are adopting cloud-based IAM platforms. Despite ongoing concerns regarding confidentiality, these solutions mitigate risks by employing stringent control mechanisms.

This article examines current methods of organizing identification processes, identifies their weaknesses, and provides recommendations for designing flexible access management systems. The proposed approaches aim to enhance security reliability, optimize processes, and meet contemporary requirements amid active digital transformation.

MATERIALS AND METHODS

Contemporary research in identity and access management encompasses a wide range of directions. Topics include conceptual approaches, risk analysis methods, countermeasures against attacks, technological advancements for enhancing security, the human factor in IAM systems, specialized applications, and infrastructural solutions.

In the study by Devlekar S. and Ramteke V. [1], a conceptual framework was presented for assessing the security level of identification systems. The authors highlighted aspects such as authentication, authorization, and data management. Pöhn D. and Hommel W. [3] refined the taxonomy of threats, contributing to a better understanding of vulnerabilities and approaches to mitigate them.

A. Talabi et al. [2] examined biometric systems utilizing multifactor authentication, demonstrating their effectiveness in risk management. Fragkos G., Johnson J., and Tsiropoulou E. E. [7] proposed a role-based access control model applicable to smart energy grids, emphasizing adaptive approaches to security provision.

Blockchain technologies and artificial intelligence find applications in IAM. Ghaffari F. et al. [6] analyzed blockchain usage in identification processes, focusing on the advantages of distributed systems. Alomari M. K. et al. [4] reviewed AI-based platforms that optimize the accuracy and reliability of identification processes.

The human factor was explored in the work of Hilowle M. et al. [5], which studied the perception of security and usability in national digital identification systems, emphasizing the importance of these characteristics for technology adoption.

In the study by S. N et al. [8], threat analysis methods using machine learning algorithms were investigated. The authors suggested applying classification and clustering approaches for predicting attacks and assessing vulnerabilities in information systems. These methods enhance forecasting accuracy and minimize false alarms.

The article by Domínguez-Dorado M. et al. [9] introduced a novel approach to asset protection organization. The proposed model addresses both tactical and operational levels, focusing on asset accounting and protection under cyber threat conditions. Integrating risk management and asset protection processes was found to enhance security in complex tasks.

Specialized topics cover various aspects. Eichelberg M., Kleber K., and Kämmerer M. [10] examined cybersecurity challenges in medical PACS systems, proposing specific protection methods. Kraus K., Kraus N., and Shtepa O. [11] explored the relationship between security and financial inclusion at different levels. Pinto R. F. M. [12] described the use of infrastructure codes for training cybersecurity professionals.

Statistical data illustrating the number of user identification breaches from 2020 to 2024 were examined using sources [13-16], with data available on platforms such as rg.ru, www.ptsecurity.com, and securelist.ru.

Scientific studies highlight contradictions in the assessment of biometric and blockchain systems. Some researchers emphasize their resilience to threats, while others identify associated risks. Issues related to interdisciplinary approaches, combining technological and social aspects, and the scalability of systems remain underexplored.

The methodology was based on analyzing scientific publications and studying statistical data.

RESULTS AND DISCUSSION

Methods of attacks targeting the use of personal data remain dominant in the field of digital security threats. These methods expose vulnerabilities in organizations lacking effective access management and user identification mechanisms. Statistical analysis confirms the importance of such systems in ensuring protection against attacks and reducing potential losses. The number of hacks at the user identification level from 2020 to 2024 is shown in Figure 1.

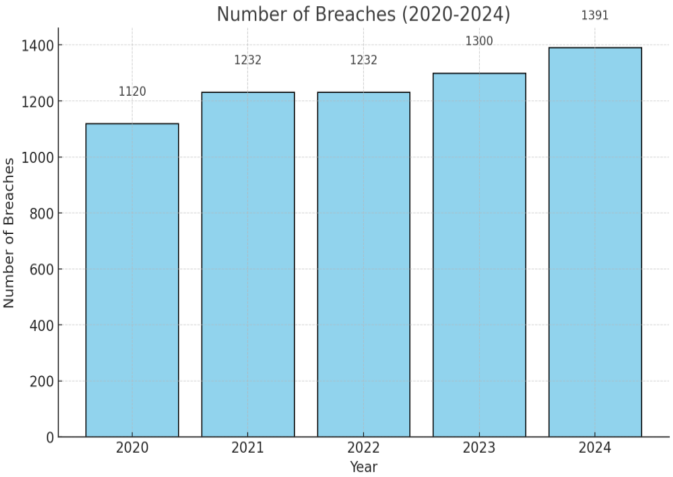

Figure 1. The number of hacks at the user identification level in 2020-2024 [13-15]

Cyberattacks aimed at user identification continue to pose significant threats to information security in 2024. The data presented emphasizes the need to address this issue:

- Account data compromise. In the first quarter of the current year, information on more than 102 million users, including passwords of over 19 million individuals, was disclosed. The level of data leaks has exceeded the figures of the previous year several times over [13].

- Professional services: The number of reports regarding database leaks and ransomware attacks has increased by 15% compared to 2023, with 351 incidents registered compared to 334 [14].

- Engineering and construction remained constant targets for cyberattacks in the first half of 2023 and 2024. In the first half of 2024, the United States bore the brunt of cyberattacks, with the number of incidents increasing by 46.15% compared to 2023 [14].

Identity and Access Management (IAM) systems encompass rules, technological tools, and methods that provide control over employee access to resources. Their implementation aids in data protection, regulatory compliance, and process optimization. The key components of IAM systems are detailed below:

- Identification. Determining the identity of a user or object using unique identifiers, such as logins or codes.

- Authentication. Verifying identity-based on passwords, biometric characteristics, or other multifactor verification methods.

- Authorization. Allocating access rights to resources based on predefined rules, such as role-based models.

- Account management. Managing the creation, modification, and deletion of account data throughout their lifecycle.

- Audit and activity logging. Monitoring user activity and recording actions to analyze compliance and detect anomalies [1].

The components of the IAM system are presented in Figure 2.

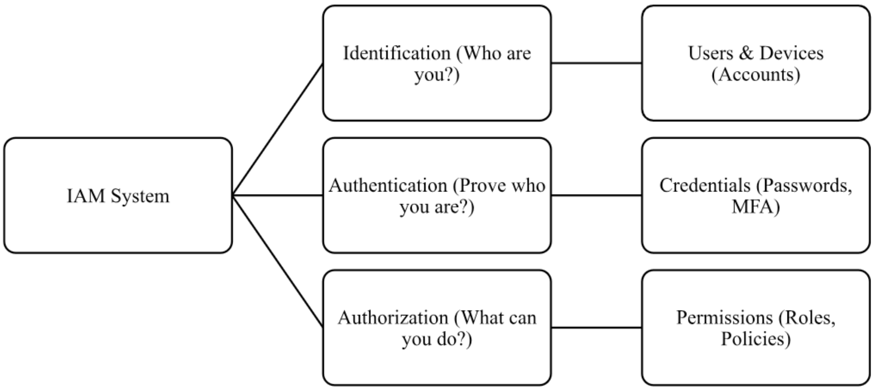
IAM System
Identification (Who are you?)
Authentication (Prove who you are?)
Authorization (What can you do?)
Users & Devices (Accounts)
Credentials (Passwords, MFA)
Permissions (Roles, Policies)

Figure 2. Components of the IAM system (compiled by the author)

Thus, implementing an IAM system enables access control, ensuring information security and management process stability. The advantages and disadvantages of IAM are detailed in Table 1.

Table 1: Advantages and disadvantages of IAM (compiled by the author)

Advantages	Disadvantages
Enhanced security. IAM ensures that only authorized users can access confidential resources.	Technical complexities during implementation. Deploying systems requires an understanding of the infrastructure where various platforms, programs, and users interact. Integration with legacy elements that do not support modern technologies complicates the process. Implementation takes significant time for design, testing, and configuration.
Compliance with regulatory standards. Standards such as GDPR, HIPAA, and ISO are met, ensuring controlled access.	Financial burden. High licensing costs, the need for specialized training for system use, and ongoing maintenance for infrastructure updates impose a significant financial strain.
Efficiency. Automated processes save time and prevent errors caused by human factors.	Configuration errors. Incorrectly defined parameters lead to access management issues. Ambiguous settings create difficulties in determining acceptable levels of permissions for different users.
Improved user experience. Enabled through single sign-on functionality.	Security threats. Centralized systems are vulnerable because, in the event of a compromise, attackers gain access to a wide range of data. Complex policies cannot protect against human errors or social engineering attacks. Dependence on external providers introduces risks related to vendor vulnerabilities.

Identity management systems include AWS IAM, Azure Active Directory, Okta, SailPoint Identity Security cloud, Saviynt IGA, Oracle Cloud Infrastructure (OCI) IAM, Ping Identity and Privileged Access Management (PAM) solutions (e.g., Delinea Secret Server, CyberArk, BeyondTrust). For instance, in a PAM setup, Manage Privileged Access by monitoring, detecting, and preventing unauthorized access to allow the organization to protect their applications, infrastructure, and maintain confidential data and essential infrastructure. Emergency access accounts can be created within the "Emergency Access Accounts" division, such as Privileged accounts managed through tools like Delinea Secret Server, CyberArk, or BeyondTrust. A dedicated group of security administrators is granted the authority to enable, disable, unlock, and reset passwords for these accounts.

SailPoint Identity Security cloud Implementation Example: In managing access to corporate cloud applications, SailPoint integrates with employee account management systems. For instance, within the "Financial Reporting" application, access roles are configured to match job functions: the "Financial Analyst" role provides view-only access to reports, while the "Chief Accountant" role enables data editing. All changes to access permissions are automatically approved through workflow processes.

Oracle Cloud Infrastructure Implementation Example: In OCI, role-based access control governs permissions for cloud resources. For a web application development project, roles such as "Developer" and "System Administrator" are created. Access policies automatically regulate user rights, while activity logs and authentication records are collected to enhance security.

Technologies are integrated throughout the organizational lifecycle, from initial data processing to eventual system decommissioning. Mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) regulate access based on predefined role models and attribute data. Key components include user data storage and access rights management tools.

Modern identity management platforms emphasize automation through the implementation of the following:

- OAuth: A standard that allows applications to access resources hosted by another application on behalf of a user without requiring their password. Users authenticate via a third-party service (e.g., Google, Facebook), and the system issues an access token granting permissions.

- SAML: An open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP). Users authenticate with the IdP, which sends an assertion to the SP verifying their identity.

- Automated Access Reviews: Facilitate the regular review of group memberships, enterprise application access, and role assignments. The system automatically initiates periodic access reviews, enabling responsible parties to confirm or adjust user access levels.

- Employee Self-Service Access Requests: Allow employees to directly request access to specific applications or personal information through a self-service portal. Requests are routed to the appropriate manager or responsible individual for approval.

- Onboarding-Offboarding Automation: Ensures timely provisioning and deprovisioning of access. New employees are automatically granted necessary accounts and permissions, while access is revoked, and accounts are deleted upon offboarding.

- Birthright Provisioning: Assigns default permissions based on an individual's organizational role or position, providing limited access aligned with their responsibilities.

- Separation of Duties (SoD): Ensures no single user has full control over sensitive systems, processes, or activities. Systems enforce SoD policies by automatically restricting conflicting roles in critical business processes.

- Synchronization programs. Programs such as SCIM facilitate seamless data updates, eliminate unnecessary permissions, and establish baseline access levels.

- Birthright Provisioning. Provisioning strategy that assigns default permissions based on an individual's role or position within the organization.

- RBAC and ABAC usage. These provide flexibility in access management, enabling permissions tailored to risk and user behavior.

- Adaptive MFA. Configure MFA for devices,VPN,OWA and cloud applications for enhanced security.

- Enterprise SSO. Allow end users to log in to multiple applications with a single set of credentials.

- Zero Trust principles. These principles mitigate risks, safeguard data, and identify potential threats.

- SCIM tools. These standardize processes, reduce errors and support integration within hybrid systems.

- Monitoring and automated checks. These identify deviations and propose methods to address inconsistencies.

Analytical models streamline workflows, accelerate processing, and help prevent recurrence of issues [7]. Artificial intelligence technologies transform data protection methods, creating adaptable platforms responsive to evolving conditions. Such systems analyze data, detect anomalies in user behavior, eliminate vulnerabilities, and maintain reliability.

Contemporary platforms adapt to various scenarios by analyzing user actions, device attributes, geographic locations, and time-based parameters. This reduces errors and mitigates risks associated with unauthorized access attempts.

Technology integration eliminates manual access management. Platforms optimize role assignments, remove redundant permissions, and ensure settings remain current. Detection of atypical behavior prevents threats, restricts suspicious actions, and safeguards data.

Platforms monitor activity changes, analyze anomalous events, and take preventive measures against incidents. Automation tools reduce response delays, enhance stability, and ensure timely risk mitigation.

Automated management reduces unnecessary expenses, eliminates errors, reallocates functional access, and improves system performance. Integration reduces time spent on routine tasks, thereby increasing productivity.

Platforms track configuration changes, log actions, generate audit reports, and assist in compliance with internal policies. This transparency enhances trust among partners, regulators, and clients.

Systems integrate with other security tools, forming a unified ecosystem that reduces the likelihood of errors. These solutions are well-suited for managing connected devices within complex digital infrastructures.

The application of artificial intelligence transforms access management approaches by creating universal platforms that integrate seamlessly into digital infrastructures, maintain stability, simplify administration, and protect data [4].

Thus, the updated IAM platform incorporates artificial intelligence algorithms, identity protection technologies, and SCIM standards, creating a system designed for digital ecosystems. Automation of workflows, enhanced threat protection, and the introduction of adaptive access control mechanisms align with organizational requirements. The system ensures data security, optimizes process management, complies with regulatory standards, and addresses emerging challenges. This technological model meets business needs while accounting for technological advancements.

CONCLUSION

The research highlighted the necessity of revising approaches to identity and access management to adapt to the demands of the digital environment. Analysis of authentication methods, authorization processes, account data management, and activity auditing confirmed their importance in protecting information and preventing threats. Technologies such as artificial intelligence algorithms, distributed ledgers, and zero-trust concepts demonstrated their effectiveness in enhancing system functionality.

Centralized management platforms were emphasized for their ability to simplify operations, eliminate redundancies, and improve transparency. Access management approaches, including role-based models and adaptive strategies, enable systems to be tailored to different threat scenarios. Automation reduces the likelihood of human error and optimizes resource allocation.

The findings underline the importance of developing identity management systems that are resilient to changes in the digital landscape. The proposed solutions ensure compliance with regulatory requirements and information security, making them valuable across various industries. This analysis lays the foundation for further refinement of management concepts, incorporating advanced technologies and expanding functional capabilities.

REFERENCES

1. Devlekar S., Ramteke V. Identity and Access Management: High-level Conceptual Framework //Revista geintec-gestao inovacao e tecnologias, vol. 11. No. 4, 2021, pp. 4885-4897.
2. Talabi et al. Cybersecurity Risk Management in Identity Systems using Biometric-based Multimodal Authentication. // Proceedings of the 28th iSTEAMS Multidisciplinary & Inter-tertial Research Conference, 2021, pp.61-86
3. Pöhn D., Hommel W. Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems //Security and Communication Networks, No. 1, 2023, pp. 5573310.
4. Alomari M. K. et al. Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control //Security and Communication Networks, No. 1, 2021, pp. 8686469.
5. Hilowle M. et al. Users' adoption of national digital identity systems: Human-centric cybersecurity review //Journal of Computer Information Systems, vol. 63. No. 5, 2023, pp. 1264-1279.
6. Ghaffari F. et al. Identity and access management using distributed ledger technology: A survey //International Journal of Network Management, vol. 32. No. 2, 2022, p. e2180.
7. Fragkos G., Johnson J., Tsiropoulou E. E. Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach //IEEE Transactions on Human-Machine Systems, vol. 52. No. 4, 2022, pp. 761-773.
8. S. N et al. Cybersecurity Analysis Using Machine Learning // International journal of scientific research in Engineering and management , Vol. 7(1), 2023, pp. 1-8
9. Domínguez-Dorado M. et al. CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels // IEEE Access, vol. 10, 2022, pp. 122454-122485.
10. Eichelberg M., Kleber K., Kämmerer M. Cybersecurity protection for PACS and medical imaging: deployment considerations and practical problems //Academic radiology, Vol. 28 No. 12, 2021, pp. 1761-1774.
11. Kraus K., Kraus N., Shtepa O. Practice of the implementation of cyber security and financial inclusion at the micro-, macro- and global levels of the economy // VUZF review, vol. 7. No. 2, 2022, pp. 25-40.
12. Pinto R. F. M. Infrastructure as Code for Cybersecurity Training, 2023
13. Phishing Attacks Double in 2024. - URL: https://www.infosecurity-magazine.com/news/2024-phishing-attacks-double/

14. Cyber threats that shaped the first half of 2024. - URL: https://www.helpnetsecurity.com/2024/08/30/cyber-threat-intelligence-report-key-threats/
15. Number of user accounts exposed worldwide from 1st quarter 2020 to 3rd quarter 2024. - URL: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

Citation: Sandeep Singh, "Redefining the High-Level Framework for Identity and Access Management in Cyber Security", American Research Journal of Computer Science and Information Technology, Vol 8, no. 1, 2025, pp. 6-11.