International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 2, Mar-Apr 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Identity Management

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Identity management refers to how an organization identifies and authenticates individuals for access to its networks or applications. The process ensures that individuals and groups have the right access, rights, and restrictions with established identities for the organizational resources while keeping their assets and data secure. Controlling who has access to these resources can be challenging without effective identity management. Identity management is important because it aids in preventing security events like data leaks and illegal access. From logging into email and collaboration platforms to accessing corporate resources, identity management plays a pivotal role in daily interactions online. In this paper, we will explore the role of identity management solutions in securing users and devices.

KEYWORDS: *identity, identity management, digital identity management, law, legal industry*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Identity Management" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-2, April 2025, pp.788-796, URL: www.ijtsrd.com/papers/ijtsrd78579.pdf

IJTSRD78579

INTRODUCTION

With digital transformation gaining even more momentum, their protection is an absolute must. In the era of digital transformation, digital identity management emerges as a key enabler for organizations seeking to enhance cybersecurity, strengthen customer trust, and comply with regulatory requirements.

Today, data is the most valuable commodity in the world. This is reflected by the ever-increasing number of cyberattacks. Evolving cyber threats have increased the risk of online identities becoming compromised. As a result, traditional user authentication methods (using username and password, biometrics, etc.) have proven to be lacking. Many businesses face challenges in ensuring identity protection and data security, particularly with remote and hybrid work environments becoming more common. Identity management emerged as a solution to the limitations of traditional identity verification methods. It refers to the processes and technologies used to manage and secure information about the identity of individuals or entities within a digital system. It is the organizational process for ensuring individuals have the appropriate access to technology resources. It ensures the right individuals to access the appropriate resources at the right times for the right reasons. Identity management solutions can help you protect your organization by authenticating users and devices seamlessly without compromising security.

Organizations of all sizes rely on a variety of tools and technologies to function and compete in today's digital world. Identity management encompasses the processes involved in securing and overseeing unique digital representations of people and devices. For them to protect their systems, data, and resources, identity management best practices are essential. By adhering to these best practices, organizations can make sure that their identity management systems are efficient at safeguarding their resources, data, and systems while also preserving the confidence of their clients and other stakeholders.

WHAT IS A DIGITAL IDENTITY?

An identity is the collection of unique characteristics that define a person, organization, resource or a service in conjunction with any optional additional

information. A digital identity is the information and data that identifies an individual in the digital world. It consists of a set of attributes and credentials, such as name, date of birth, e-mail address, and biometrics, as well as certificates, passwords, or other cryptographic keys. Digital identities are typically stored in a central database or directory, which acts as a source of truth. We all have some sort of digital presence, social media, e-mail, etc. which can all be described as our individual digital identities. Within the corporate world, it is the organizational identity which matters and therefore forms the core of the identities of users within the infrastructure.

Digital identities have become a core element of a company's DNA. An employee ID allows the workforce of a company to access the internal network and enables organizations to manage permissions. A consumer ID provides online shoppers with increased security while allowing providers to gather insights into user preferences and demographics. An e-banking ID (a special form of consumer ID) can be used to access online banking services, view account information, and make transactions. A citizen ID offers secure 24/7 access to government services online, encouraging digital use and reducing the need for office [1]. Figure 1 shows these forms of ID [1].

WHAT IS IDENTITY MANAGEMENT?

Identity management (IDM) is an identity security framework that works to authenticate and authorize user access to resources such as applications, data, systems, and cloud platforms. It is a framework for policies and technologies that ensure the secure management of digital identities, focusing on identifying, authenticating, and authorizing users and applications to access internal resources. It is a method of verifying the identities of network entities and the level of access for enterprise network resources. Its main goal is to ensure only authenticated users are granted access to the specific applications, systems or IT environments for which they are authorized. At the core of an identity management system are policies defining which devices and users are allowed on the network and what a user can accomplish, depending on device type, location, and other factors.

Identity management systems must enable companies to automatically manage multiple users in different situations and computing environments in real time. They include software, hardware, and procedures used to identify and authorize a person or persons that need access to applications, systems, networks, or physical locations. They encompass the tools, protocols, and practices used to establish, validate, and maintain digital identities. This is done by first ensuring that the right person or persons are identified, and then verifying that those persons are authorized to access the item or resource in question. Identity management aids in ensuring compliance with laws and industry standards pertaining to data protection and privacy. Figure 2 shows a representation of identity management [1].

There are a number of identity management systems available today that perform a few key functions. They are displayed in Figure 3 [2] and briefly explained as follows [2]:

- Validation – Is the identity data real and authentic?
- Verification – This verifies the identity of users through credentials or other means. Is the validated identity data associated with a specific person?
- Authentication – This involves verifying the identity of users or entities attempting to access a system. Does the person or persons have permission to access what they are attempting to access?

A driver's license is an example of identity data. Other examples may include biometric data (fingerprints, facial recognition, selfies, etc.), documents (passports or government-issued ID), challenge questions, or even behavioral signals. Organizations may use a variety of these methods within their identity management process. Figure 4 shows various means of identifying a person [3].

IDENTITY AND ACCESS MANAGEMENT

In addition to managing employees, use of identity management along with access management enables businesses to manage customer, partner, supplier, and device access to their systems while ensuring security. The terms "identity management" and "access management" are often used interchangeably or in combination. But a distinction does exist between the two concepts. Identity management focuses on *managing* the attributes related to the user, group of users, devices, or other network entities that require access to resources. In contrast, access management focuses on *evaluating* user or device attributes based on an organization's existing policies and governance. Identity access management (IAM) is an umbrella term that encompasses all of the processes involved in identifying people inside a system and restricts access to such information to only authorized users [4]. IAM systems fall under the overarching umbrellas of IT security and data management. Identity and access management (IAM) ensures that the right people (identity) can access the

right resources at the right times, for the right reasons (access management). The purpose of IAM is to stop hackers while allowing authorized users to easily do everything they need to do. Organizations of all sizes need IAM solutions to make sure that only authorized people have access to the systems. Figure 5 represents identity and access management [3], while Figure 6 presents some IAM tools [5]. A typical IAM system has a database or a directory of users.

Thanks to IAM, users can use their digital identity to gain access to different systems. Any corporation that wants to safeguard its resources, data, and systems must have a strong IAM strategy. Unauthorized access, data breaches, and other security problems can all be avoided with the help of an efficient IAM approach. Implementing appropriate security measures to guard against data breaches and other security threats is another critical component of an IAM strategy.

There are two types of IAM, centralized and decentralized identity management models [6]:

- *Centralized identity and access management (IAM)* is a framework for storing and managing users' identity data in a single location. It consolidates the storage and exchange of users' login credentials and privileges. It provides a secure process for identifying, authenticating, and authorizing users who have permission to access a company's digital assets. With centralized IAM, users can access all the resources and applications they need to do their jobs by entering only one set of login credentials. Critics of a centralized approach often cite the single identity store as the most troubling issue. Relying on a single set of credentials creates a single point of failure.
- *Distributed identity management* (also known as decentralized authentication), allows users access applications individually using a different set of credentials for each. This model distributes users' identities across the network, as each application must store and handle its own user data. Decentralized identity management gives users more control but offers companies less visibility. It eliminates single point of failure by distributing data and increasing trust. Decentralized IAM relies on nascent Web3 technologies—specifically blockchain and user-owned, decentralized identifiers (DID). DIDs allow users to control their data and offer a convenient way to authenticate with a wide range of applications.

Since there is no need for consensus across a large network, decentralized solutions are typically less expensive.

APPLICATIONS OF IDENTITY MANAGEMENT

Identity management (IDM) in essence refers to the management or administration of individual identities within a system, such as a company or network. It encompasses a variety of components and practices, including authentication, authorization, and identity governance. Innovations in the user identity management space have been a trend in the past couple of years. Specific applications of identity management include the following [7]:

- *Biometric Authentication*: Biometric authentication ensures a seamless and convenient user experience while minimizing the risk of unauthorized access. New techniques in biometric authentication include advanced methods such as vein pattern recognition, gait analysis, and behavioral biometrics (such as typing patterns or mouse movements) to enhance security and usability. Digital identity management will also witness advancements in biometric authentication, leveraging unique biological traits for secure verification. Technologies like facial recognition, iris scanning, and fingerprint authentication are already prevalent.
- *Blockchain Technology:* Blockchain provides a decentralized and tamper-proof ledger, ensuring that each user's identity information is stored in a block that's cryptographically linked to the previous one. This decentralised approach makes data breaches much more difficult.
- *Two-Factor Authentication:* Two-factor authentication (2FA) adds an extra layer of security by requiring users to provide two different forms of identification, like a PIN code or QR code sent to the user's registered phone. Multi-factor authentication (MFA) requires users to provide two or more authentication factors to prove their identities. Combined with multifactor authentication and enforceable security policies, enterprises can lower the risk of security breaches.
- *Zero Trust Architecture:* This assumes that no user or device can be trusted by default, regardless of their location. It enforces strict access controls, continuous monitoring, and least privilege principles. Identity is not only the most important element in Zero Trust; identity is the new perimeter.
- *Encryption:* Digital identity systems employ robust encryption with a public and private key cryptographic authentication system, preventing unauthorized access to networks and data as only

the intended user has the private key used to decrypt the message.

- *IDM in the Workplace:* Identity governance and administration (IGA) solutions ensure that all identities in an organization get the right access to the right resources. Organizations with simpler needs choose light IGA solutions with a subset of IGA features to reduce cost and deployment time. Light IGA solutions often focus on identity administration features.
- *Single sign-on (SSO):* SSO allows users to access multiple apps and services with one set of login credentials. The SSO portal authenticates the user and generates a certificate or token that acts as a security key for other resources. SSO systems use open protocols like Security Assertion Markup Language (SAML) to share keys freely between different service providers. Features like SSO and adaptive access allow users to authenticate with minimal friction while protecting vital assets.
- *Cloud Identity Management:* This is the subsequent step of identity and access management (IAM) solutions. However, it is a lot more than merely a straightforward web app single sign-on (SSO) solution. Identity management in cloud computing incorporates all categories of user-base who can operate in diverse scenarios and with specific devices. Identity management in cloud computing is highly critical to an organization. This next generation of IAM solution is a holistic move of the identity provider right to the cloud. Cloud IAM solutions provide a clean and single access control interface. Figure 7 shows the representation of cloud IDM [8].

BENEFITS

A major benefit of identity management is the ability to efficiently carry out transactions and complete tasks like document signing. Users can effortlessly access various online services without the need to remember different passwords or usernames. Identity management is indispensable for maintaining security, ensuring user trust, and meeting regulatory standards in today's digital landscape. Embracing it can significantly improve the security of your organization and optimize workflow while keeping your mission-critical data secure. Other benefits include the following [1]:

- *Automation:* Many key IAM workflows are hard or outright impossible to do manually. Instead, organizations rely on technology tools to automate IAM processes. Modern IDM and IAM systems frequently have automated features that help ensure controls are in place to manage these risks. These systems also help to manage compliance with an ever-changing ecosystem of regulations that ensure users only have access to authorized data, and that data lives in the right place.
- *Competitive Advantage:* In a fast-paced business environment, being able to quickly adapt and integrate advanced identity management solutions can provide a competitive edge, improving security, operational efficiency, and customer trust.
- *Identity Governance:* This is the process of tracking what users do with access rights. Identity governance provides oversight and monitoring, helping organizations track and manage who has access to specific resources and why. IAM systems monitor users to ensure that they do not abuse their privileges and to catch hackers who may have snuck into the network. Identity governance is important for regulatory compliance.
- *Less Reliance on Physical Documents*: Traditional identity systems rely on physical documents (e.g., driver's licenses, passports) for verification. Digital identity management eliminates the need for physical documents, reducing the risk of theft or loss.
- *Cybersecurity:* A reason that IAM is important is that cybercriminals are evolving their methods daily. Identity management plays a vital role in protecting organizations against breaches. By implementing stringent access controls and continuously monitoring identity activities, organizations can mitigate the risk of cyberattacks and data leaks. This not only protects the organization's assets but also upholds its reputation and trustworthiness. While perfect protection unfortunately is not possible, IAM solutions are an excellent way to prevent and minimize the impact of attacks. While no security system is infallible, using IAM technology significantly reduces your risk of data breaches.
- *Cost Efficiency:* While initial setup may be expensive, managing digital identities in-house can lead to long-term cost savings by reducing reliance on third-party services.
- *Productivity:* Identity management can improve employee productivity. This is especially important when onboarding new employees or changing authorizations for accessing different systems when an employee's function changes. As tempting as it might be to implement a complicated security system to prevent breaches, having multiple barriers to productivity like

multiple logins and passwords is a frustrating user experience.

- *Delegation:* Delegation enables local administrators or supervisors to perform system modifications without a global administrator or for one user to allow another to perform actions on their behalf. For example, a user could delegate the right to manage office-related information.
- *Improved Collaboration:* Seamless collaboration between employees, vendors, contractors, and suppliers is essential to keeping up with the pace of modern work. IAM enables this collaboration by making sure that not only is collaboration secure, it is also fast and easy.

CHALLENGES

Identity management comes with numerous challenges affecting all levels of an organization. Merging modern IAM technology with existing legacy infrastructures is not always easy. People are tired of creating and managing all of their user ID and password combinations. Other challenges include the following [1]:

- *Password Management:* One of the top challenges in implementing identity management is password management. IT professionals should invest in techniques that reduce the impact of password issues in their companies. They must enforce strong password policies and manage password resets. Employees often cannot remember and maintain multiple secure passwords to access the resources they need to get their jobs done. By streamlining communication processes and access control, identity management not only improves IT security, it improves the user experience as well.
- *Resource Shortages:* When it comes to identity management, two types of resources can lead to problems if there is a shortage of them. Firstly, human resources are an issue, as securely managing digital identities requires a broad range of qualified professionals which are hard to find. Secondly, financial resources play a key role. Smaller companies or those with limited IT budgets may struggle to allocate sufficient funds for hiring, training, and retaining IAM professionals or investing in necessary technologies.
- *Complexity:* The complexity of identity management consists of several interrelated factors further emphasizing the need for highly skilled employees. Identity management needs to be integrated across a variety of systems, applications, and platforms, each with its own requirements and protocols. To meet the complex use cases of modern enterprises, IAM platforms must integrate with a wide variety of systems.
- *Security:* Protecting against a wide range of security threats, such as phishing, brute force attacks, and insider threats, requires advanced security measures and continuous vigilance. With new technologies and vulnerabilities, new attack vectors emerge. Quickly implementing updated security measures helps organizations stay ahead of these threats. In-house management ensures that all identity processes align with the latest global data privacy and security regulations.
- *Scalability:* Ensuring that the identity management system can scale to accommodate growth, additional users, and increased data without compromising performance or security adds another layer of complexity. As a company grows, it might struggle to scale their systems efficiently, leading to performance issues and operational bottlenecks. Standard solutions are built to scale according to the needs of the business, allowing for easy adjustments as the company grows or changes.
- *Interoperability:* Achieving interoperability between different identity management solutions and standards involves careful planning and implementation.
- *Regulatory Compliance:* Keeping up with evolving regulations and industry standards can be difficult, increasing the risk of non-compliance and potential legal penalties. Regulations and compliance standards are frequently updated to address new security concerns and protect user data. Companies must adapt quickly to meet these evolving requirements and avoid legal penalties. Ensuring that identity management practices comply with ever increasing regulations involves ongoing monitoring, auditing, and reporting.
- *Access Control:* Users expect easy and quick access. This can conflict with the need for robust security measures, which is also increasingly a hard requirement for most users. Defining and enforcing granular access control policies necessitates detailed planning and constant updates.
- *Flexibility:* With emerging methodologies, business requirements are changing rapidly, adapting to market trends, responding to customer needs, and necessitating an update of the IT strategy. Therefore, identity management systems

need to be flexible to accommodate new projects, technologies, or organizational changes.

- *Data Privacy:* One major concern with identity management is data privacy. Keeping data secure and private is not easy. Customers demand that the companies they do business with not only make their personal experiences enjoyable, but that those companies keep their data safe from breaches and protect their privacy. Fragmented global data and privacy regulation is creating compliance challenges. As a result of the growing list of breaches, violations of customer privacy, and increasing consumer dissatisfaction, there has been an explosion of regulations related to data security and privacy.
- *Cost:* Managing digital identities requires significant investment in technology and infrastructure, which can strain the limited resources of smaller companies.
- *Lack of Expertise:* There may be a lack of the specialized knowledge required to effectively manage digital identities, leading to potential misconfigurations, security gaps, and operational inefficiencies.

CONCLUSION

Identity management (IDM) essentially refers to the management or administration of individual identities within a system, such as a company or network. Today, the importance of an effective IDM strategy cannot be overstated. In the digital age, where digital interactions are everywhere, users must be able to trust that their identities and personal information are protected. Effective digital identity management provides this assurance by verifying that users are who they claim to be through strong authentication methods. For those who want to master or speed up digital transformation, the key is to thoroughly manage and protect digital identities on all levels. IDM can and should be a key component of a business's security and productivity strategies [9]. By falling short on IAM best practices, organizations unknowingly risk their own security, along with that of their customers and shareholders. More information on identity management is available from the books in [10-20].

REFERENCES

[1] "What is digital identity management and how do you master it?" https://www.adnovum.com/blog/digital-identity-management

[2] "Identity management," Unknown Source.

[3] T. Watson, "What is identity management – Its characteristics & benefits," August 2020, https://skywell.software/blog/identity-management-characteristics-benefits/

[4] "What is identity management (ID management)?" https://www.techtarget.com/searchsecurity/definition/identity-management-ID-management

[5] E. Wisniowska, "Top 10 best IAM tools – Identity access management (pros cons)," November 2022, https://infrasos.com/top-10-best-iam-tools-identity-access-management/

[6] S. Brown, "Centralized and decentralized identity management explained," https://www.strongdm.com/blog/centralized-decentralized-identity-management

[7] R. Villano, "Digital identity management: How it's revolutionising user and device authentication," May 2024, https://www.globalsign.com/en/blog/sg/digital-identity-management-how-its-revolutionizing-user-and-device-authentication

[8] R. Soni, "Identity management in cloud computing," January 2021, https://www.loginradius.com/blog/identity/identity-management-in-cloud-computing/

[9] J. Barton, "Identity management – What you need to know," June 2015, https://www.univention.com/blog-en/2015/06/identity-management-what-you-need-to-know/

[10] M. Bryght, *Identity and Access Management: from Zero to Hero: Learn all you need about Identity and Access Management (IAM) (Identity in Cybersecurity).* Independently Published, 2024.

[11] M. Chapple, *Access Control and Identity Management (Information Systems Security & Assurance).* Jones & Bartlett Learning, 3rd edition, 2020.

[12] A. Zulejhic, *Identity and Access Management: Fundamentals.* Independently Published, 2022.

[13] E. Sergeev, *Identity Management Crisis: Solving IAM's Biggest Challenges.* Independently Published, 2025.

[14] M. J. Haber and D. Rolls, *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. Apress, 2019.

[15] Y. Wilson and A. Hingnikar, *Solving Identity Management in Modern Applications:*

Demystifying OAuth 2, OpenID Connect, and SAML 2. Apress, 2nd edition, 2022.

[16] J. Nickel, *Mastering Identity and Access Management with Microsoft Azure.* Packt Publishing, 2nd edition, 2019.

[17] M. Laurent and S. Bouzefrane, *Digital Identity Management.* ISTE Press - Elsevier, 2015. ·

[18] E. Bertino and K. Takahashi, *Identity Management: Concepts, Technologies, and Systems*. Artech House, 2010.

[19] K. Spaulding et al., *Identity Management: A Primer.* MC Press Online, LLC. 2009.

[20] D. G. W. Birch (ed.), *Digital Identity Management: Perspectives on the Technological, Business and Social Implications*. Gower, 2007.

Figure 1 Some forms of ID [1].

Figure 2 A representation of identity management [1].

Figure 3 Key functions of identity management systems [2].

Figure 4 Various means of identifying a person [3].

Figure 5 Representation of identity and access management [3].

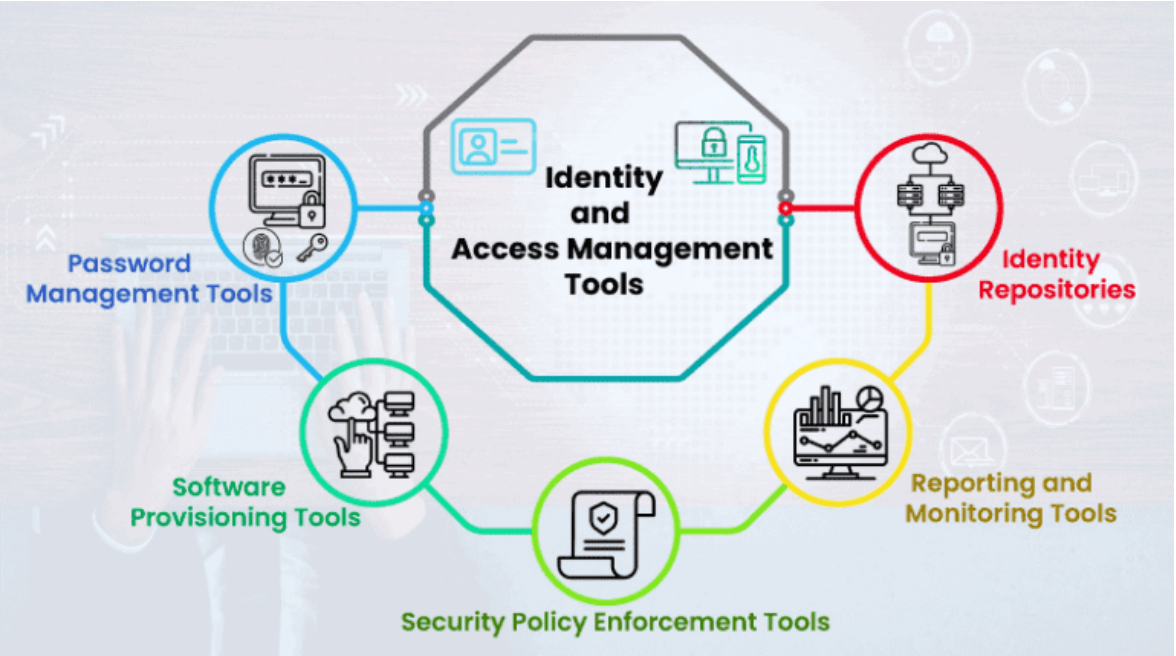

Figure 6 Some IAM tools [5].

Figure 7 Representation of cloud IDM [8].