International Journal of Advanced and Innovative Research (2278-7844)/

Volume 1 Issue 4

Identity and Access Management System: a Web-Based Approach for an Enterprise

Ishaq Azhar Mohammed

Sr. IAM Engineer & Department of Information Technology

Hyderabad, India

ishaqazhar14@gmail.com

Abstract:

The main purpose of this paper is to explore how identity and access management systems provide important benefits in various enterprises. One of the biggest problems confronting computers worldwide is establishing digital identities and access management for corporate users and services. Incorporating enterprise-wide identity and access management (IAM) into business operations, processes, and technology settings facilitates corporate identity and access management (IAM) [1]. As long as the business has implemented an IAM framework, IT administrators can regulate who has access to important information from within the company. Many companies are now confronting the difficult task of maintaining multiple identities and credentials across the organization's technological infrastructure. Previously limited to the data warehouse, the challenge has now expanded externally, and now affects companies of all sizes. Also, in dispersed IT systems, many big companies are still unable to successfully manage user identities and network access. While during the past few years, IT organizations have created system administration (SA) divisions to handle the many servers, databases, and desktops that organizations utilize, system administrators have become more important in the way organizations manage their technology [1]. Despite the establishment of SA groups, it's difficult to control who has access to the organization's activities. Even with this growth, human resource management and manual procedures are often unable to meet the challenges of managing the massive numbers of user IDs and significant administrative overhead required to do so [2].

Keywords: Identity and Access Management (IAM), Identity Management strategy, Access management, IAM enterprise, IT systems

I. INTRODUCTION

Businesses historically install and put their software programs within their internal information systems. This enables the development of a "trust area," which is just a designated entity that is governed by certain rules, which are supervised and regulated by the specialists of the IT office. Almost all of the time, the “trust area” encompasses the company's in-house systems, infrastructure, and services, all of which are placed in a data center [3]. A conventional approach has several systems deployed at the network layer, which connect directly to the organization's digital information.

Current regulations increase the number of internal controls and external reviews to get access. Major corporations give people access in the most granular fashion possible, making it necessary for management to find which particular permissions are required to complete a task. While the term identity and access management (IAM) is becoming widely accepted in the business sector, this does not mean that no other interpretations are being used [4].

Rather, it is simply the case that different groups of users, vendors, and consultants all have their interpretations of IAM, and the very nature of the business, product, or expert they are affiliated with. That so, the fundamental assumption remains unchanged [5]. The identity management solution is being used to secure user access, user accounts, verify credentials, and ensure that only the appropriate people have access to the organizations' resources. A wide range of authentication methods is used, including passwords, biometrics, tokens, and certificates. The greater the size of the company, the greater the risk, expense, and administrative resources needed to maintain identities. Every company should have a comprehensive identity management system for handling its identities effectively. It reduces the costs associated with identity management while also reducing the time and expense needed to meet employee requirements [5]. Cloud-based services require access control mechanisms for authorization. To decide if the appropriate individual has access to resources with established access rules, we utilize the access control mechanism. This method is intended to allow resources to be secure and private. Effective access control mechanisms guard against illegal network access. There are various access management systems and approaches, all of which are distinct. The same cloud is utilized by many companies with varying security standards, leading to the risk of unauthorized individuals accessing resources [5,6]. A means of controlling user access to the resources or applications, known as access management, is tied to a system that manages a user's identification, often known as identity management. An access management system that has been in place for some time in an enterprise offers various functions and advantages.

In addition to managing access to digital resources, IAM covers the process, tools, and rules for identifying and deciding what identity access and permission are needed. An individual user will deal with many tasks with the introduction of IAM. An application's user account may be created, modified, or deleted. Additionally, users have a method of verification to substantiate their identification. Authentication methods may vary from single-factor authentication (e.g. login and password) to multi-factor authentication (combining many factors, including tokens, biometrics, and/or a smartcard) [6]. Concerning companies, IAM is utilized very extensively because it is often employed to address a situation where many users have various digital resources to use. The longer this process takes, the more user accounts need to be propagated and greater monitoring and audit capabilities are required. Most identity and access management frameworks/architectures/models focus on providing an end-to-end solution [7]. However, the current methods do not have a complete assessment from the initial conceptualization to the execution stage, and they are thus impractical and inaccurate solutions. In this research work, IAM will be explored to understand how it is beneficial to enterprises. A literature review will be provided to understand various scenarios and the benefits of IAM to businesses and organizations.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to understand how identity and access management can be beneficial to enterprises. Any economic crisis exposes the company to significant threats. Staff who are worried about downsizing may be motivated to obtain unauthorized access to critical information housed across apps, while temporary workers would be less committed and user authentication procedures for full-time workers may be bypassed, leaving the company vulnerable. In other words, this helps to explain why security experts place such importance on identity and access management (IAM) [7,8]. Developers can address these issues: providing centralized monitoring and enforcement of application access rules, together with new role-based access control technologies that allow for consistent temporary worker access, and robust and efficient disengagement. Incremental improvements in IAM may be gained by supporting SaaS apps utilizing federated user account provisioning and hosted IAM provider services.

III. LITERATURE REVIEW

A. How Identity and Access Management Works

With today's increasing computing complexity and increased security concerns, users no longer feel safe even with a secure login and password. Identity management systems nowadays typically include biometric information, artificial intelligence, and machine learning, as well as risk authentication [8]. IT administrators can grant or deny access to information inside their companies using an IAM platform. Identity and access management solutions provide the ability of system managers to restrict access to a computer system or networks based on the activities of user accounts in the business. In this case, access refers to a user's capacity to execute a particular activity, such as viewing, creating, or modifying a file. Throughout an organization, roles are classified based on job expertise, authority, and accountability. Numerous solutions exist to make the security system and other elements of IAM easier [9]. Depending on the kind of IAM program that is implemented, there are many sorts of approaches that are often employed:

Single Sign-On (SSO): This is a user authenticating authorization and login platform that supports people to access all the applications, systems, and data they request before having to log in separately in each one of such domains.

Multi-Factor Authentication: Such a system authenticates people and grants their authorization by combining something the user knows (– for example, a password), what the user already possesses (– for example, a security token), and also something the user is (– for example, a fingerprint) [9].

Privileged Access Management: Such a framework combines the database of workers and pre-defined work roles to identify and give access to individuals to their tasks.

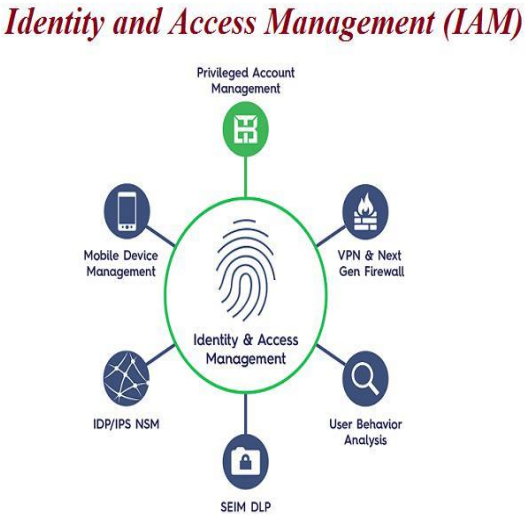

Fig I: Identity and access management

B. Why IAM is crucial for enterprises

Business leaders and information and communication services are being expanded to safeguard access to company resources via regulatory and organizational pressures. As a consequence, they no longer have the power to issue and monitor user rights on manual and mistaken procedures. The IAM simplifies these processes and allows the management of granularity access and auditing on-site and in a cloud of all business assets [9,10]. The IAM, which has a growing range of capabilities, such as biometrics, computational intelligence, and AI, is ideally adjusted to the changing security landscape's requirements. In highly dispersed and dynamic settings, for instance, the close IAM management of resource access is aligned with the shift from firewalls to zero-confidence paradigm and with IoT's security needs [9,10]. Although IAM may be seen to be for bigger businesses with more resources, the platform is available to enterprises of all sizes.

C. Fundamental IAM components

An IAM framework allows IT to monitor access permissions inside its enterprises to valuable information. IAM solutions provide role-based access management, enabling system administrators to restrict system or network entry depending on the activities of specific users in the company. In this

respect, accessibility is a user's ability to execute a certain activity, like seeing, producing, or altering a file. Functions inside the company should be determined through work, authority, and responsibility [11]. The following must be done to IAM systems: collect and store user login data, maintain the company user IDs databases, and coordinate permissions for assigning and cancellation.

This implies that technologies employed by IAM offer supervision and control of all elements of the user community of the business to a centralized metadata repository. Not only do people have digital identities; IAM may also monitor the digital identities of computers and software to build confidence. IAM may be managed in the cloud platform via the use of authentication as a service or identity as a service (IDaaS) [11]. For both instances, the role of authentication and certifying consumers is shared by a third-party service provider as well as their management.

D. Benefits of Identity and Access Management for enterprises

1. Enhanced security

IAM solutions assist detect security issues and address them. You may utilize IAM to detect policy breaches or eliminate inappropriate access rights without exploring multiple dispersed platforms. One may also use IAM to verify that security measures are in place to satisfy demands for regulation and audit [12].

2. Sharing of information

IAM offers single access and identity information framework. Every operating system and device that the business is using may be subject to the same safety policies. IAM platforms may help you implement authentication processes, permissions, and verification restrictions and ensure "privilege creep."

3. Ease of use

IAM makes things simpler for app owners, end-users, and system administrators when it comes to registration, sign-in, and user management. IAM simplifies access delivery and management, which improves user experience. Identity and access management allows the user to access services depending on their given roles and permissions. However, IAM also provides custom access depending on the experience of a person, the vulnerabilities, and the environment in which they seek the access [12,13].

4. Productivity gains

By integrating all access rules into a single system, IAM minimizes access complexity. It allows user management to be centralized, uniform, and scalable and simplifies authorization, and accelerates the adoption of new applications. IT administrators may use automated provisioning and Lifecycle Management systems that provide identity and access management solutions, rather than continuously changing passwords and giving access to all applications [13]. As a result, users do not have to queue since they get immediate access to whatever it is they want as soon as they are onboarded, based on their function, rather than requiring various tools and resources on an ad hoc basis. This implies fewer IT requirements and ultimately more productivity.

5. Reduced IT Costs

IAM services may help to reduce operational expenses. Utilizing federated identity networks makes it simpler to administer applications since local identities are no longer needed for external purposes. The demand for buying and maintaining local infrastructures may be reduced by cloud-based IAM services. By adopting IAM technologies and following associated best practices, companies may obtain a comparative edge. For instance, IAM technology allows businesses to access their networks via mobile apps, on-site applications, and SaaS to people outside the company – like customers, associates, contractors, and suppliers – without compromising on security. This allows improved cooperation, improved production, greater efficiency, and lower operational expenses.

E. IAM implementation challenges and risks

While IAM protects everything in a network, it doesn't cover everything. One problem is how the

rules for "birthright access" develop. When new employees start to work at a business, they are granted such access privileges. The choices for granting this access to new workers, contractors, and partners encompass many departments, and assigning this to the correct persons and management has become a problem [13]. IAM systems ought to be capable of automatically detecting changes to access permissions, but they frequently don't.

This level of uncertainty becomes critical when considering automated onboarding and offboarding of clients, user self-service, and ongoing verification of compliance. It is not possible for dozens or hundreds of users to manually adapt access rights and restrictions. For instance, it virtually guarantees that unnecessary permissions of access have not been totally removed without computerized "exit" procedures, or periodically audited. This cannot be accomplished using Excel spreadsheets or other manual methods, but the fundamental complexities of user onboarding have remained constant over time, even though IAM solutions have improved at managing workflows and business operations [13].

Another problem is that, although zero-trust platforms are quite popular right now, the challenge is being able to constantly verify these trust connections when innovations are introduced to a company's IT system architecture. One must monitor everyone once they log in, looking for behavioral benchmarks. Then there has to be properly managed IAM and Single-sign relationship on (SSO) [14,15]. The objective is to reach an integrated SSO system per user group that can manage access to all the apps the company utilizes. Because each company may have its reasons for utilizing different SSO tools, this doesn't imply that every organization will be using the same SSO solution.

Apart from that, the integration of identity and access management with customer-centric identity and access management has evolved. As long as security experts view these as two distinct initiatives, IAM is constantly catching up. Furthermore, IAM teams must be aware of many cloud solutions. Consider IAM security recommended standards from Amazon, Google Cloud, as well as Microsoft Azure Web Services (AWS) [16]. Addressing the loopholes across cloud service providers can become difficult, and combining such procedures with a company's network and applications architecture will be complicated. Finally, IT administrators must include identity management into modern innovations from the outset. To successfully pilot any IAM and identity governance initiatives, it is important to carefully identify a target application that can be used as a model and subsequently expanded to additional applications throughout the business.

IV. FUTURE OF IAM IN VARIOUS SECTORS

Identity and Access Management (IAM) is destined to become an increasingly important aspect of many corporate and personal activities in the United States as the technological and organizational environment continues to quickly evolve. In the coming years, innovative methods for identity and access management will probably be developed owing to the changing technologies. IAM (identity and access management) methods that are mainly reliant on passwords to authenticate users will not be able to keep up with the reality of the future where a large number of devices will be interconnected [17]. From a business perspective, a decentralized and secure identity model will be embraced by every item, application, and platform. One may have many identities, yet still, be identified as the individual and also be identified with smart things. Increasingly powerful identities mean that global identity service providers must authenticate identities and monitor identification registries. Due to growing complexity, many U.S. businesses no longer have the internal capacity to successfully handle identity and access management (IAM) problems they face [17,18]. Adopting new techniques to strengthen your position in the identity verification industry, building better management skills, and minimizing the dangers of a growing remote workforce will be essential for organizations trying to keep up with changes in the IAM environment.

V. IAM INTEGRATION SERVICES IN THE UNITED STATES

The number of industries integrating IAM solutions in its businesses will grow as the operations and security of companies becomes more complex in the United States. Identity and access management will be deployed in biometric analysis, facial recognition, speech recognition among other factors [18]. Artificial Intelligence integrated into the future IAM solutions will be capable of learning about the user for access control and user actions will be evaluated and abnormalities will be detected automatically. IAM services offer sophisticated services to allow service providers to better meet large-scale customer needs, commanding larger transaction volumes, and establishing themselves in a growing industry with substantial long-term development. Those who can assist clients progress in their IAM maturity, while also delivering strong value, will find themselves in a highly valued market position. Several new product developments have arisen because of the recent embrace of new technology [18]. As a result, the software has been enhanced and better effectiveness has been realized. Not only for corporate headquarters but for other important sectors as well, identity and access management solutions are needed. This system not only keeps track of workers' identities but also helps a company follow international regulatory guidelines and standards.

VI. CONCLUSION

This research paper study addressed how identity and access management benefit enterprises. The conclusions made from this research demonstrate that as a business evolves, the number of end utilities and consumers who utilize different apps and platforms from multiple devices increases. To mitigate cybersecurity threats, businesses may use Identity and Access Management — a framework that makes use of services such as multifactor authentication, Single Sign-On (SSO), and privileged access management. IAM provides businesses with control over their user access to vital data. Many companies today are grappling with the perplexing issue of managing identities and credentials for their digital resources. A long-standing, well-defined problem used to be a straightforward affair limited to the data center's walls, but that is no longer the case. Now, the problem is bigger and more difficult to deal with, and it's affecting many companies of all kinds. For instance, companies that have hundreds or thousands of users have trouble managing the user identities and access rights they give. The overall aim of IAM is to guarantee that every person, organization, or device has access to the resources they need, and in the appropriate context. Since the late 1990s, the IAM industry has seen strong competition. Companies are spending more in the IAM industry because of the immense value it has in many industrial sectors. This increased investment in IAM will contribute to market growth.

REFERENCES

[1] K. Chow, K. Choy and W. Lee, "Design of a knowledge-based logistics management system: a case-based RFID approach", *International Journal of Enterprise Network Management*, vol. 1, no. 1, p. 5, 2006.

[2] J. González, M. Rodríguez, M. Nistal and L. Rifón, "Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems", *Computers & Security*, vol. 28, no. 8, pp. 843-856, 2009.

[3] J. Balmer and S. Greyser, "Managing the Multiple Identities of the Corporation", *California Management Review*, vol. 44, no. 3, pp. 72-86, 2002.

[4] L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", *Information Systems Security*, vol. 16, no. 1, pp. 9-14, 2007.

[5] E. Zavadskas, A. Kaklauskas, M. Gikys and N. Lepkova, "A multiple criteria decision support web-based system for facilities management", *International Journal of Internet and Enterprise Management*, vol. 2, no. 1, p. 30, 2004.

[6] E. Damiani, S. De Capitani diVimercati and P. Samarati, "Managing multiple and dependable

identities", *IEEE Internet Computing*, vol. 7, no. 6, pp. 29-37, 2003.

[7] K. Flieder, "Identity- und Access-Management mit EAI-Konzepten und -Technologien", *Datenschutz und Datensicherheit - DuD*, vol. 32, no. 8, pp. 532-536, 2008.

[8] G. Goth, "Identity management, access specs are rolling along", *IEEE Internet Computing*, vol. 9, no. 1, pp. 9-11, 2005.

[9] Å. Grönlund, "Electronic identity management in Sweden: governance of a market approach", *Identity in the Information Society*, vol. 3, no. 1, pp. 195-211, 2010.

[10] K. An, K. Lee and M. Chung, "Design and Implementation of an RFID-based Enterprise Application Framework based on Abstract BP and Kerberos", *Journal of Information Processing Systems*, vol. 2, no. 3, pp. 170-177, 2006.

[11] D. Bates, "The Athens Access Management System", *SSRN Electronic Journal*, 2001.

[12] G. Larson and G. Pepper, "Strategies For Managing Multiple Organizational Identifications", *Management Communication Quarterly*, vol. 16, no. 4, pp. 528-557, 2003.

[13] T. Martens, "Electronic identity management in Estonia between market and state governance", *Identity in the Information Society*, vol. 3, no. 1, pp. 213-233, 2010.

[14] R. Easty and N. Nikolov, "Client-side integration of life science literature resources", *Bioinformatics*, vol. 25, no. 23, pp. 3194-3196, 2009.

[15] M. Velicanu, "Identity Management in University System", *SSRN Electronic Journal*, 2009.

[16] J. Wang, X. Li and Z. Feng, "Enterprise application integration framework based on multi-agent system", *Journal of Computer Applications*, vol. 29, no. 4, pp. 1151-1154, 2009.

[17] C. Zang, Y. Fan and R. Liu, "Architecture, implementation and application of complex event processing in enterprise information systems based on RFID", *Information Systems Frontiers*, vol. 10, no. 5, pp. 543-553, 2008.

[18] R. Scherer and G. Cheney, "Rhetoric in an Organizational Society: Managing Multiple Identities", *Sociological Analysis*, vol. 53, no. 1, p. 111, 1992.