ISSN No:-2456-2165

A Survey on Identity and Access Management

Zeel Hiren Shah
NMIMS's MPSTME

Abstract:- Different architectural issues related to Identity and Access Management (IAM) are arising for the successful deployment of applications in the context of digital entitlement. Data management solutions should include effective access control methods and choose the best configuration among the numerous and intricate approaches to offering access control services. The IAM features can be used to implement Web Single Sign-on (SSO), federated identities, password synchronisation, and service granularity, allowing the system to address and resolve the majority of current access management concerns. This paper gives you the general idea of what is IAM (Identity Access Management), How it is related to Cybersecurity, Its Functional Areas and its role in Cybersecurity and in Information Security for a better understanding.

I. INTRODUCTION

Traditionally, Software applications are typically deployed and deployed inside the boundaries of an organization's information system. As a result, the company has a "confidential area" that is determined by static procedures and is overseen and managed by the IT department's expertise. The "confidential area" typically refers to the central organisational network, as well as internal systems and applications, which are arranged in the shape of a data centre. The data centre can either be maintained by professionals from within the company or it can be contracted out to an outside service provider (in which case the company typically retains the right to control and last say over how security rules are developed and enforced). In a "conventional" paradigm, a number of specialised technologies that are implemented at the network level secure access to the organization's operational resources.

Nowadays, maintaining identities and credentials for their technological resources is a challenging issue that many enterprises must deal with. What began as a straightforward problem contained within the boundaries of the data centre has evolved into a huge and enormously complicated issue that affects businesses of all kinds. In particular in remote IT systems, many major firms are unable to efficiently control the identities and access permissions assigned to users. System administration (SA) teams have been developed by IT departments during the past few years to handle the organization's numerous servers, databases, and workstations. Nevertheless, managing access to the organization's resources continues to be difficult even with the introduction of SA groups. Even with this increase, manual procedures and human resources occasionally fall short of the demanding workloads and high administrative costs required to manage user IDs inside the business.

Identity and access management (IAM) refers to the products, processes, and policies that are employed to manage user identities and regulate user access within an organisation. It makes reference to the IT security discipline, foundation, and digital identity management solutions. Identity management includes identification provisioning and de-provisioning, identification security and authentication, and authorization to access resources and/or perform specific actions. IAM's overriding goal is to ensure that any given identity has access to the appropriate resources (applications, datasets, networks, etc.) and context.

Identity management systems are used to secure user access, manage users, perform credential verifications, and determine whether the right people are accessing the services' resources. Users are authenticated in a variety of ways, including passwords, biometrics, tokens, and certificates. In most organisations, the risk, cost, and effort required to manage identity grows in tandem with the organization's size. This assists the organisation in lowering the risk associated with identity management, as well as the cost and time required to meet the identity and access needs of the employees.

II. RELATED WORKS

This chapter explores existing studies works on Identity and Access Management in an organisation, outlining work's strengths and flaws of each work. To address the various types of authentication and authorization issues, several researchers have proposed various approaches and models.

- A new architecture for managing identity and controlling access to resources in a multi-tier cloud infrastructure was proposed in the article [1]. The architecture is made up of two major components: middleware and centralised IAM for managing user and infrastructure data. While the repository handles database operations, middleware sits in front of a resource provider and manages time-consuming decision making such as authorization and authentication. The architecture was tested on the Canadian SAVI testbed. The system is built on a multi-tier infrastructure IAM solution, such as the SAVI testbed. However, the proposed work necessitates a significant amount of effort to define and assign roles.

- An integrated identity and attribute-based access management system for cloud web services was proposed in the paper [2]. The hybrid architecture for authentication and attribute based control (ABAC) for authentication were used in the proposed integrated approach. Identity Management and Access Management models are included. To access cloud web services, the user must first authenticate via an identity system from the initiated

ISSN No:-2456-2165

application, which is Identity Management. There is a process in place to verify the access token with the identity system and perform cloud authorization. This work, on the other hand, only provides and demonstrates a theoretical framework.

- The authors [3] proposed an identity and access management as a service (IAMaaS) framework that focuses on authentication, authorization, identity administration, and auditing. It is also concerned with identity verification and granting correct access to resources that are protected in the cloud environment. When a user logs in, his or her credentials are validated and a token is generated, which is then passed to the private cloud's protected resources, such as devices, data, and application servers. The framework, however, has yet to be integrated into SECaaS and has only demonstrated a proof-of-concept (POC).

III. FUNCTIONAL AREAS

An IAM Framework can be divided into four major areas:

- *Authentication:* This refers to the procedure by which a user gives appropriate credentials to get access to an application system or a specific resource for the first time. Once a user is authorised, a session is generated and used throughout the user's interaction with the application system until the user logs out or the session is ended in some other way (e.g. timeout).

- *Authorization:* Once a user has been authenticated, authorization handles the rest of an organization's identity and access management processes. Users are granted permissions based on their role within an organisation. Authorizations determine a role's network resources and level of access.

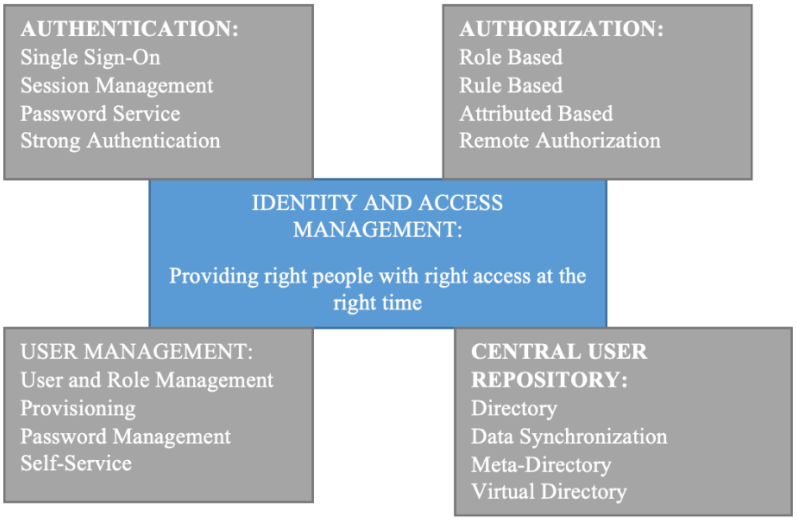

Fig 1:- Functional Areas of IAM

- *User Management:* This category includes user administration, strong passwords, role/group management, and user/group provisioning. It defines a collection of administrative duties such as identity generation, propagation, and the management of user identities and privileges. One of its components is user life cycle management, which allows a company to control the lifecycle of a user account from provisioning through de-provisioning. Some user management functions should be centralised, while others must be outsourced to end users. Delegated management allows an organisation to allocate duty directly to user departments. Delegation may also increase system data accuracy by entrusting updating responsibilities to those who are most acquainted with the situation and data..

- *Central User Repository:* The Central User Repository maintains and distributes identification information to other systems, as well as verifies customer credentials. The Central User Repository aggregates or logically organises an enterprise's identities. To handle different identity data from several systems and application user repositories, both a meta-directory and a virtual directory can be employed. By collecting data from numerous identity sources, a meta-directory often gives an aggregate collection of identity data. To maintain the data in sync with other identity sources, it often incorporates a two-way data synchronisation service.

A. Role of IAM in Cybersecurity

Effective IAM infrastructure and solutions assist enterprises in establishing secure, productive, and efficient access to technology resources across these disparate systems, while also providing several important key benefits:

- *Enhanced Data Security:* Business and IT personnel receive a streamlined and uniform manner of controlling user access across an organization's identity lifecycle by unifying both authentication and authorization capabilities on a single centralised platform. When employees leave a firm, for example, a centralised IAM solution enables IT managers to revoke their access with assurance that the revocation will take effect quickly throughout all business-critical systems and assets that are linked with the centralised IAM solutions.

ISSN No:-2456-2165

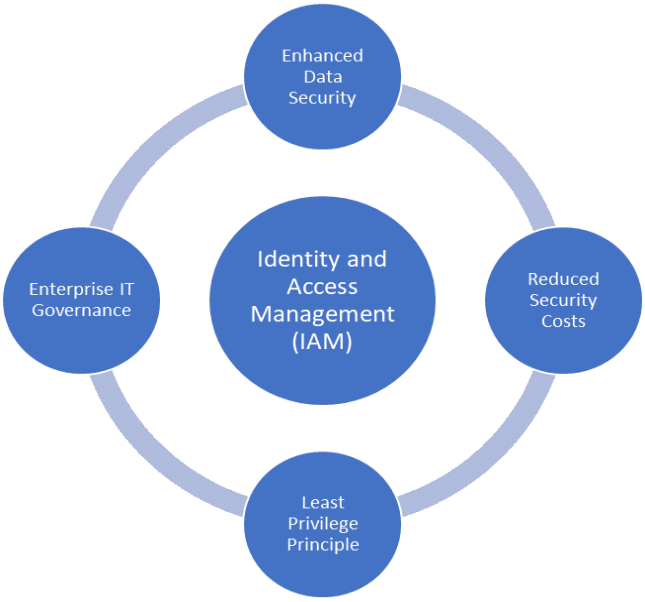

Fig 2 A:- Role of IAM in Cybersecurity

- *Reduced Security Costs:* Having a centralised IAM platform in an organisation to manage all users and their access enables IT to work more efficiently. As part of their job in today's world, every employee has access to thousands of systems and resources. An effective centralised IAM solution can address this challenge diligently, resulting in significant time and money savings for the company.

- *Least Privilege Principle:* The principle of least privilege is an important practise in computer and information security for limiting access privileges for users to the bare minimum necessary to perform their job duties. With an insider being involved in 77% of data breaches, it is critical to ensure that access to all corporate resources is secured and granted using the least privilege principle.

- *Enterprise IT Governance:* Taking global compliance regulations such as HIPPA, SOX, and the upcoming EU GDPR (General Data Protection Regulation) into account, a lack of effective identity and access management poses significant compliance risks. Through automated governance controls, modern IAM solutions and products can enforce user access policies such as separation-of-duty (SoD) and establish consistent governance controls, eliminating access violations or over-entitled users. This will ensure that businesses adhere to business and government compliance and regulatory standards.

B. Role of IAM in Information Security

One of the three main pillars of information security is the role of identity, which is responsible for cataloguing users within a system so that everyone who has access to it can be properly authenticated. It is critical for better access control that the roles of identities are clear and that the individual who wishes to access them can be easily identified.

It is critical for information security that a specific user has control over what he can access. The ideal is to appeal to the maxim of "minimum privileges," in which a person receives authorization and sees only what has been allowed on his screen through the management of permission groups.

Fig 2 B:- Role of IAM in Information Security

IV. CHALLENEGES AND RISKS OF IMPLEMENTING IAM

Despite the fact that IAM is present at all levels of an organization's information security architecture, it does not cover all bases. The evolution of users' "birth right access" rules is one issue [5, 6]. These are the access rights granted to new users on their first day of employment at a company. When it comes to granting access to new employees, contractors, and partners, the options are numerous and cover a wide range of departments. According to Steve Brazen, research director at the European Medicines Agency, who wrote about it in a blog post, this level of automation becomes critical when considering automated onboarding and compliance management of users, user self-service, and ongoing verification of compliance. Manually changing access rights and restrictions for hundreds or thousands of users at the same time is not possible [6]. Having no automatic "leave" procedures (and failing to review them on a regular basis) virtually guarantees that unnecessary access privileges will not be completely removed.

Another issue is that, while zero-trust networks are popular right now, it is difficult to constantly monitor these trust connections when new applications are introduced into a corporation's IT system architecture. We must examine the baselines of behaviour and monitor what individuals do after logging in. Many false positive scenarios exist, such as when a user breaks their finger, which can destabilise these trust connections. The relationship between identity and access management (IAM) and single sign-on (SSO) must then be properly managed [7, 8]. Okta's acquisition of Auth0 [8] demonstrates that the integration of identity and access management with customer-centric identity and access management has begun. Because security experts will continue to treat these initiatives separately, IAM will be constantly playing catch-up.

Following that, IAM personnel should be acquainted with a wide range of cloud architectures. The following sections [8] provide examples of IAM security best business practises for Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure. It will be difficult to integrate these practises into an organization's network and application infrastructure, and it will be even more difficult to close the security gaps that exist between different cloud providers.

Finally, IT administrators must incorporate identity management into the design of all new apps from the start. To successfully pilot any IAM and identity governance initiatives, choose a target app carefully that can be used as a template and then expanded to other applications throughout the business.

V. HOW ARTIFICAL INTELLIGENCE ADDRESS IAM CHALLENGES

Despite the fact that this is a fairly common occurrence in many businesses, it is not necessary to stay in this state. Artificial intelligence (AI) could be a huge help in achieving successful IAM, alleviating a lot of stress. Businesses will be able to transition from overly technical access management to access management that is understandable at all levels of the organisation as a result of these technologies [9]. Analytics combined with artificial intelligence will provide insights into focus and discourse, allowing both technical and non-technical employees to work for extended periods of time while remaining productive. Using cutting-edge technology, new insights can be gained, and procedures can be automated, allowing for a significant speedup in current IAM compliance controls. They will detect anomalies and potential threats without the need for a large team of security experts to do the same. This provides technical and non-technical employees with the information they need to make the best decisions possible. The need for such development is critical, particularly in anti-money laundering and known security vulnerabilities, but also in countering business executive risks [9]. It paves the way for a future transition from reactive access management to preventive or even corrective access management. As a result of their efforts, businesses are always up to date and secure.

VI. CONCLUSION

In this paper, we saw that IAM system provides a strong identity and access management system to an enterprise being it on-premise or on cloud web related services. To assist enterprises in meeting today's business challenges, Identity and Access Management (IAM) has emerged. IAM combines business processes, security policies, and technologies to assist organisations in managing digital identities (user attributes that describe who users are, how they prove their identity, and the resources they can access) and controlling resource access. Any enterprise should implement an identity and access management system:

- with a large number of employees where users are provisioned frequently and frequently; -where there is a need to monitor who accessed what and to what extent;
- where their application and users are not on a single repository;
- where Single Sign-On is a priority among diverse applications an enterprise or organisation.

This research evaluated how artificial intelligence (AI) is being used in identity and access management, as well as the difficulties that have been encountered and the industry's future.

Because it acts as a barrier between users and sensitive company assets, identity and access management is a critical component of any business information security. It helps to prevent the use of stolen usernames and passwords, as well as easily cracked passwords, which are common network entry points for malicious attackers looking to plant malware or steal data.

REFERENCES

[1]. Faraji, M., Kang, J.-M., Bannazadeh, H., & Leon-Garcia, A. (2014). Identity access management for Multi-tier cloud infrastructures. 2014 IEEE Network Operations and Management Symposium (NOMS). doi: 10.1109/noms.2014.6838229
[2]. Indu, I., & Anand, P. M. R. (2015). Identity and access management for cloud web services. 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS). doi: 10.1109/raics.2015.7488450
[3]. Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and Access Management as Security-as-aService from Clouds. Procedia Computer Science, 79, 170–174. doi: 10.1016/j.procs.2016.03.117
[4]. Bresz, F., Renshaw, T., Jeffrey R., & Torpey, W. (2007, November). Identity and Access Management. Retrieved from https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%209%20-%20Identity%20and%20Access%20Management.pdf
[5]. M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security", Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 150-156, 2015.
[6]. I. Aguiló, L. Valverde and M. Escrig, Artificial intelligence research and development. Amsterdam: Tokyo, 2003
[7]. R. Lee, Software engineering, artificial intelligence, networking and parallel/distributed computing. Cham : Springer International Publishing : Imprint : Springer, 2015.
[8]. S. Phon-Amnuaisuk, S. Ang and S. Lee, Multi-disciplinary Trends in Artificial Intelligence. Cham, Switzerland: Cham, Switzerland : Springer, 2017.
[9]. J. Sołdek and L. Drobiazgiewicz, Artificial intelligence and security in computing systems. [Place of publication not identified]: Springer, 2013.
[10]. https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system