Identity and Access Management as Security-as-a-Service from Clouds

Ishaq Azhar Mohammed

Data Scientist & Department of Information Technology

Dubai, UAE

Abstract- *This paper provides a systematic review of identity and access management as a security as a service from clouds with particular attention on identity-as-a-service. IAM as a service (IAMaaS) offers a safe, scalable, and functional cloud-based IAM platform that protects enterprises from the cost and hassle of managing their network. IAM Managed Services handle the Identity and Access Management (IAM) system in a seamless, end-to-end way whether on-site or remotely. Researchers from all over the world are bringing new elements and capabilities to the cloud computing architecture, which is still in its infancy and fast-growing. Cloud computing is based on vast cloud applications. It's an expansion to the grid, distributed computing, and parallel computing [1]. As with the digitalization of industry in the industrial era, the emergence of cloud computing can be compared to the rise of the information age. The coming future organizations, for their computational resources, will easily connect to the cloud (computer grid).*

Keywords: *Identity and access management, security as a service, cloud computing, identity, and access management, information technology, information security, identity management systems*

I. INTRODUCTION

One of the main benefits of the IAM platform is its flexibility. IT decision-makers wish to be able to expand the technology using plug-in application programming interfaces (APIs), hooks, and associated applications to add and change features, such as authentication methods, for customers and partners. As a result, enterprises need technological ecosystems which provide an extensive network of connections that are prefabricated, tested, verified, and regularly updated. For successful business results, companies need to be equipped with well-designed, strong IAM systems with defaults covering the majority of usage cases and extending these capabilities. Cloud computing is a young and fast-changing concept, with new features and capabilities introduced regularly by researchers worldwide. The origins of cloud computing can be traced back to large-scale distributed technological advances. It is generally a combination of the grid, distributed, and parallel computing [1]. The security-as-a-service theory relies on cloud-based encryption rather than on-premise software applications. By integrating with current on-premise installations as part of a hybrid model, the security-as-a-service approach improves their capabilities. Identity and Access Management (IAM) is a method used for managing resource access. This is accomplished by confirming an entity's identification, after identity verification access is allowed under the protected resource policies at the appropriate level [3]. This paper looks at the methodology of Identity and Access Management as a Service (IAMaaaS) in improving the security of cloud services. In particular, this IAMaaS is a mobile on-demand pay-per-use strategy. The article deals with numerous security challenges as a cloud platform. This paper deals with the following problems in different sections.

II. PROBLEM STATEMENT

The main problem that this paper will try to solve is to review how identity and access management is important in information security especially in cloud solutions. It is not a simple undertaking to maintain a secure system. A model of efficient and effective IAMaas especially in cloud systems one of the key elements for solving security concerns. In this paradigm, only authorized users are allowed permissions. Three basic elements include a model of access control: the subject, the objective, and the rules. The subject involves users of the system requesting access to the network. Rules are used to decide whether to give or refuse access [3,4]. The primary aim of user authentication is to deprive intruders of a given device and minimize the task of authorized users. Additionally, it inhibits the activity that could result in a security breach. One of the primary difficulties for the implementation of this model is to establish a suitable risk assessment technique to produce precise and effective risk values to ascertain the easy option for each access request. This research, therefore, provides a risk assessment methodology that combines Identity and Access Management as Security-as-a-Service to analyze safety concerns and solutions in Clouds services.

III. LITERATURE REVIEW

A. An Overview of IAM as a Service

Identity and access management as a service (IDaaS or IAMaaS) relates to web-based solutions that enable the creation and maintenance of individual system access. It, therefore, is among forms of cloud-based services currently provided by cloud service providers. There is a growing trend in the contemporary IT industry toward moving away from on-premises infrastructure and toward cloud-based SaaS-based applications [4]. Almost every area of information technology now offers cloud-based applications as a service. Although cloud computing has seized over in the majority of cases, there are still certain areas that have been sluggish to transition. An excellent illustration is the Identity and Access Management (IAM) sector. This has been remedied, however, by the introduction of an entirely new generation of IAMaaS systems [4]. IDaas relies on the fundamental concept of software as a service (SaaS), which gained popularity in recent years when companies realized they could successfully "stream" services via the Web instead of offering them as licensed software packages on CDs or inboxes. Providers expanded their provision of cloud-based SaaS solutions, including platform as

a service (PaaS), communications as a service (CaaS), as well as infrastructure as a service (IaaS) [4]. The digitalization of networks and the simplification of hardware into logical tools have both contributed to the acceleration of this advancement. In today's complicated world, IAMaaS enables businesses to establish bespoke layers of safety for their IT infrastructure, either in its whole or in segments. The underlying concept is whether a third-party provider establishes access privileges and defines the capabilities of these particular users inside a platform [5]. As with traditional identity and access management solutions, these services operate by tracking and identifying specific system and user activities, followed by the creation of a network monitoring of credentials for each. IAMaaS is much more relevant to businesses that enable workers to work from home or utilize their personal computers. Often, the usage of various devices necessitates increased security to safeguard private data as well as other sensitive data. The advantage of IAMaaS for the sector is that businesses may create a blanket system for the whole design or a specific component [5]. Some IT professionals warn companies that would like to offer IAMaaS just for cloud-related solutions, while the "old apps" already in place lack the same modicum of flexibility. Such critics assert that, in certain instances, keeping any of those locations largely unprotected may result in significant risks [6]. Fortunately, the majority of these adjustments have been beneficial. Nevertheless, to fully appreciate the advantages of a new cloud-based identity and access management system, we must first examine the previous approach. Following that, we'll talk about what's changed.

B. Identity and Access Management in the Past

Historically, the identity provider (IdP) category has been on-premises and usually provided through software controlled by the IT department. Microsoft Active Directory® has been the preferred choice for the majority of businesses (AD) [7]. For the most part, we are all aware that AD has dominated the IAM area for over two decades, for better or worse. AD is a directory services platform for information technology resources that are running on Microsoft Windows®. It was originally launched in 2000 as a directory service solution for the then-common implementations of Windows systems and services. Everything was Windows-based at the time. Users accessed the on-premises email, apps, and data servers they used regularly via their endpoints. The basic fact was that if you want computer capacity, you turned to Microsoft and controlled it via Active Directory. With AD at its heart, the IAM industry evolved into a plethora of subcategories [8]. Numerous others addressed AD's flaws, such as its lack of device management capabilities for non-Windows systems, and have evolved into SaaS solutions that companies may use in addition to AD. None of them, however, were built to provide a fully complete Directory-as-a-Service® in the cloud [8,9,10].

C. Identity and Access Management as a Service

For some time now, options for identity-as-a-service (IDaaS) have been available. Numerous web application Single Sign-On (SSO) solutions exist that may be considered first-generation IDaaS solutions [10]. However, when we use the term IAMaaS (a.k.a. Identity and Access Management as a Service), we mean a solution that sits at the heart of identity management (rather than as an add-on to an on-premises IAM instance such as Active Directory) – all provided as a service from the cloud. IAMaaS's real purpose is to serve as an organization's centralized, cloud-based directory service. The contemporary IAMaaS platform, as a cloud identity management platform, securely maintains and links employee identities to the IT resources they need [11]. These resources may include Windows, Mac, or Linux operating systems, Windows or Linux servers hosted in the cloud or on-premises at AWS or elsewhere, online or on-premises apps, physical or virtual storage, and wired or wireless networks. Almost everything a person needs to connect to is enabled through the cloud and as a service by the current IAMaaS solution. Directory-as-a-Service refers to this approach to IAMaaS [11].

D. IDaaS

Identity-as-a-Service (IDaaS) is a term that refers to identity management. IDaaS is a term that refers to cloud-based Identity and Access Management (IAM) capabilities and services (Software-as-a-Service managed by a third party). As a result, Gartner also refers to IDaaS as SaaS-delivered IAM or simply IAM as a service [12]. To provide context, IAM is a broad word that encompasses the management of digital identities (whether they be those of people, organizations, or objects), as well as security, authentication, and user roles and privileges inside corporate networks, applications, and digital services. IAM is used to verify that users are who they say they are and that they have secure privileged access to just the apps, services, and resources to which they are authorized. As is the case with IAM, the phrase IDaaS encompasses both internal and external system identities (workforce IAM) (CIAM or Customer IAM) [13]. Therefore, let's examine some critical issues about IDaaS for cloud IAM and CIAM scenarios – including identity service features, adoption factors, and reasons why organizations may select this Software-as-a-Service Identity & Access Management approach.

E. IAM functionalities offered by IDaaS

IDaaS offers a variety of identity management options and generally involves standardized elements such as basic user logins, Single Sign-On (SSO), authentication multi-factor (MFA), and self-service online account managing. This may enable it easier for current digital identities validated by third-party IDPs like banks, national IDs and other identity schemes to be used as robust means of verification and authentication [13]. It is possible to provide seamless "sign in with..." authentication techniques using other Identity Providers such as Google, Facebook, LinkedIn, among others. In summary, IDaaS must enable the usage of digital identities in business directories as authentication mechanisms, such as Active Directory, LDAP, HR, and ERP systems. In other words, an organization using IDaaS does not have to worry about handling implementation, encryption, setting, and management in-house [13,14]. Managing in-house IAM systems may be complex and costly, with the advantages of the SaaS IAM method more to be taken into consideration - infrastructure, networking, software, and pricey expertise expenses.

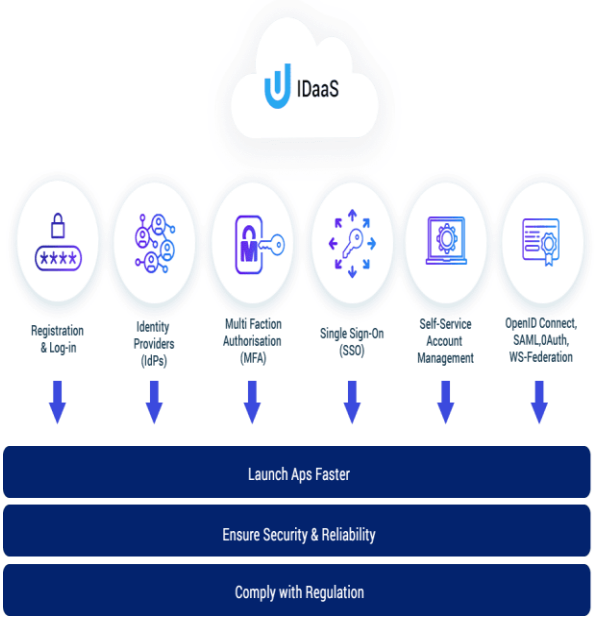

Fig i: Flow process of IDaas

IDaaS provides Registry & Login, Identity Provider Identity Verification, MFA, SSO, User Directories, and other basic IAM features as one-service capabilities [13]. IDaaS is an excellent option for rapidly marketing an app/service and building customer and user confidence without sacrificing the safety of user identity management features. Some organizations' identity management requirements may exceed the capabilities of SaaS IAM. Ubisecure, for instance, provides a complete identity application with IAM installation targeted offers between identity as a service and private cloud (Platform as a service), through IAM software installation locally in the local user directory of the organization's data center (s) [14].

F. Benefits of IDaaS

1. IDaaS safeguards against data breaches

The critical purpose of IDaas is to improve the security and use of digital signature data and tokens, as well as to control access to the relevant individuals. Security applies to both internal users such as remote staff and external users such as client identities, partners, and contractors. Most intrusions are caused by online fraud, unapproved usage, or poor access control. In addition to implementing credential management rules, IDaaS introduces higher degrees of adaptive authentication when the situation warrants it [14]. Data privacy has been (and will be) a highly debated subject lately, with daily news headlines by data violations. Data breach incidents wreak havoc on an organization's image, regardless of its size, pulling away businesses and resulting in massive regulatory penalties especially for the GDPR non-compliance). To guarantee that users are who they claim to be, IDaaS protects systems utilizing access control and authentication [14]. For example, IDaaS solutions should include identity verification and identity testing processes when a user registers for a service and then utilize Multi-Factor Authentication (TOTP), biometrical, or other similar passwordless authentication, such as TOTP for the licensed users. In addition to these identity services, the application may also employ simplified access management to minimize needless risk (e.g. single sign-on/sso), which can enable users to log in and participate with various services in a strong identity.

2. IDaaS enables regulatory compliance.

Regulation non-compliance may be caused by a variety of factors, not only breaches. Organizations must guarantee that their data practices remain credible and that users have authority over their data – another capability enabled by Software-as-a-Service IAM capabilities like self-service account management [15].

3. IDaaS enhances user experience

IDaaS's advantages do not just reflect the objectives of the cybersecurity team; they include usability (UX) and customer experience, which may fall within the competence of various departments, like advertising. For instance, it may be used to provide the simplest registration procedures possible for customer-facing apps — a critical step in turning visitors into subscribers – by providing straightforward sign-up and authentication features, like access to new digital identities. Identity provider capabilities will differ across SaaS Identity and Access Management systems. Once a client is enrolled, they may bounce between linked apps that use the same identity without having to authenticate each time. This is enabled via Single Sign-On (SSO), which is another fundamental IAM / CIAM feature [15].

4. IDaaS expertise on demand

IAM is a complicated issue based on several requirements, for instance, OpenID Connect, OAuth, and WS-Federation. Furthermore, addition, requirements and their application are continuously changing. This implies significant costs for the organization that is attempting to maintain its position. Integrating IAM features into any project using IAM implies that the software developers should not have to come up with something new achieving what the IAM providers have already done for many clients effectively [16]. This significantly lowers time and costs on infrastructure development and the chance of mistakes. In recent years, SaaS has fueled development in numerous sectors by this 'demand expertise,' and identification is no exception. Gartner predicts that Software as a Service IAM (IDaaS by another name) is expected to increase or replace 60 percent of IAM installations supplied worldwide, up from 20 percent now, and the delivery model selected for over 80 percent of global secure access management buying [17].

G. Overview of the market

Identity and access management as a service is one of several cloud services that cloud providers provide that relate to web-based services that establish and regulate individual user access levels. In this situation, identity and access management as a service enable businesses to establish customized levels of protection in whole or in part for an IT infrastructure [17]. The fundamental concept of identity and access management as a service platform is that a third-party service provider establishes user IDs and decides what each user may do in a system.

H. IAMaaS Market: Drivers and Challenges

The main drivers of identity and access management as a services industry are the growing demand to increase mobile security, business needs to improve operational efficiency, and the extensive use of cloud-based apps. Many companies have adopted their device idea or are developing it, so that workers may use their own mobile devices or take them to various places for a seamless connection. To guarantee mobile security, these businesses require their identity and access management systems in place. Cloud-based platforms are also on the increase to replace on-site applications and save small and medium-sized businesses on costs. It is thus essential to

have a robust identity and access management as a service platform for such businesses [17].

IV. FUTURE IN THE UNITED STATES

The Cloud and as a Service is the future of Identity and Access Management. Many businesses in the United States have historically installed and used information asset management applications and solutions on-premises. In recent years, as the number of identities running across cloud and digital services has increased, companies have begun to offer IAMaaS solutions to help with the increasing complexity and resulting security problem [17]. Because of its simplicity of use and cloud-native connections, the IDaaS industry is slowly but steadily gaining ground on the on-premises IAM market. While IDaaS offers several advantages over traditional on-premise solutions in terms of flexibility, security, and scalability, a third alternative is becoming more popular. IDaaS is created by a third-party integrator to provide an IAM solution tailored to functional and financial needs, utilizing the best race identity elements, and maybe also managed by the integrator when the client wants to. Directory-as-a-Service is redefining what identity and access management may look like in the cloud era by rethinking what it can look like [17]. Active Directory on the cloud wasn't the goal, and it wasn't even close to being sufficient. User identities are securely managed and connected to the IT resources that users need, comprising systems (Windows, Mac, Linux), servers (on-premises and in the cloud), applications (web-based and local), networks (wired and WiFi), independent of platform, protocol, service provider, or location [17,18]. All companies' information and authentication strategies have been affected by forced remote working, and this will continue to be the case for the foreseeable future. It seems inevitable that remote working, or a hybrid combination of remote and other work arrangements, will become more popular. It will continue to have a significant effect on companies' cybersecurity, highlighting the need for a long-term identity and access management plan, as well as a Zero-Trust Strategy, which says "Never Trust, Always Verify." The Zero-Trust Strategy, which is more comprehensive than the IAM strategy, begins with a visualization of your strengths and possibilities, to reach and exceed your company's objectives [18]. Many workers are now working outside of their typical working hours, from exotic places, and/or need access to systems that they would normally only be able to access while they were in the office, among other things.

V. ECONOMIC BENEFITS TO THE U.S

As security problems continue to grow in importance, more technical needs will be beneficial for the United States information technology sector. The United States presently dominates the IAMaaS industry, owing to widespread use of cloud apps and the bring your device idea, as well as compliance regulations and conventional mobility practices. Numerous industrial sectors, including the civil service, industrial production, and petroleum & gas, place a premium on identity management solutions [18]. Because of the increasing use of cloud computing and mobility, the IAMaas market is expected to expand at a stable rate in the foreseeable future. Manufacturing firms will contribute to the growth of the United States economy via the shipping of technical gadgets that are made possible by IAMaas. IBM Corporation, Oracle Corporation, Microsoft Corporation, Dell Inc., and Centrify Corporation are just a few of the businesses that operate in IAMaaS industry, among others. A number of these businesses have deliberately purchased a few technological startups over the years to extend their service portfolio, and they are constantly upgrading their products and service portfolios [18]. The continued growth of the Internet economy in the United States is dependent on the proper management of online identification information. As a result of the increased need for secure identification and access management services, the area will be able to strengthen its hold on the identity and access management market share in the future years.

VI. CONCLUSION

This paper discussed identity and access management as a service in clouds. The findings from this research demonstrate that digital transformation is a crucial corporate necessity especially when it comes to cloud solutions. Cloud IAM services and technologies have the potential to substantially increase the speed with which innovation and corporate development occur. However, security teams frequently struggle to define the appropriate cloud identity and access management strategy that not only meets cloud-first objectives, but also considers internal policy compliance and security, architecture constraints, and the customization requirements of their processes and workflows, among other factors. For a succinct summary, identity and access management (IAM) solutions are critical in ensuring security in the cloud environment via sophisticated methods of authentication and permission management. It is feasible to offer clients a solution that is continuously up to date, automatically adjusts its capacity, and has the greatest possible level of availability. In addition to manufacturing lines, there is also test- and play-areas accessible for use. Furthermore, IAMaaS offers the advantage of not requiring the service to be run at the same location as the real application, which is a significant benefit.

References

[1] C. Everett, "Identity and Access Management: the second wave", Computer Fraud & Security, vol. 2011, no. 5, pp. 11-13, 2011.

[2] C. Gunter, D. Liebovitz and B. Malin, "Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems", IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 48-55, 2011.

[3] B. Li, J. Li, L. Liu and C. Zhou, "Toward a flexible and fine-grained access control framework for infrastructure as a service clouds", Security and Communication Networks, vol. 9, no. 15, pp. 2730-2743, 2015.

[4] M. Hummer, M. Kunz, M. Netter, L. Fuchs and G. Pernul, "Adaptive identity and access management—contextual data based policies", EURASIP Journal on Information Security, vol. 2016, no. 1, 2016.

[5] H. Liu and M. Liang, "Efficient identity-based hierarchical access authentication protocol for mobile network", Security and Communication Networks, vol. 6, no. 12, pp. 1509-1521, 2012.

[6] 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.

[7] D. Sharma, C. Dhote and M. Potey, "Identity and Access Management as Security-as-a-Service from Clouds", Procedia Computer Science, vol. 79, pp. 170-174, 2016.

[8] 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.

[9] J. Nickel, Mastering Identity and Access Management with Microsoft Azure. Birmingham, UK: Packt Publishing, 2016.

[10] D. Young, "Human Resources have a vital role to play within employee identity and access management", Network Security, vol. 2004, no. 11, pp. 5-7, 2004.

[11] J. Hong and G. Linden, "Protecting against data breaches; living with mistakes", Communications of the ACM, vol. 55, no. 6, pp. 10-11, 2012.

[12] D. H.Sharma, C. A Dhote and M. M. Potey, "Security-as-a-Service from Clouds: A Comprehensive Analysis", International Journal of Computer Applications, vol. 67, no. 3, pp. 15-18, 2013.

[13] B. Ludwig and S. Coetzee, "Implications of security mechanisms and Service Level Agreements (SLAs) of Platform as a Service (PaaS) clouds for geoprocessing services", Applied Geomatics, vol. 5, no. 1, pp. 25-32, 2012.
[14] M. Madan and M. Mathur, "Cloud Network Management Model - A Novel Approach to Manage Cloud Traffic", International Journal on Cloud Computing: Services and Architecture, vol. 4, no. 5, pp. 9-20, 2014.
[15] T. Mather, S. Kumaraswamy and S. Latif, Cloud security and privacy. Farnham: O'Reilly, 2009.
[16] K. Pathak, N. Vaskevicius and A. Birk, "Uncertainty analysis for optimum plane extraction from noisy 3D range-sensor point-clouds", Intelligent Service Robotics, vol. 3, no. 1, pp. 37-48, 2009.
[17] D. Sharma, C. Dhote and M. Potey, "Identity and Access Management as Security-as-a-Service from Clouds", Procedia Computer Science, vol. 79, pp. 170-174, 2016.
[18] M. Thomas and K. Sekaran, "Agent-based approach for identity and access management in the inter-cloud environments", International Journal of Trust Management in Computing and Communications, vol. 2, no. 2, p. 125, 2014.