A COMPREHENSIVE APPROACH OF IMPLEMENTATING IAM IN AN ORGANIZATION

Santripti Bhujel
Student
Master of Computer Application
Jain (Deemed-to-be University)
Bangalore, India
santriptib@gmail.com

Priya N
Assistant Professor
Master of Computer Application
Jain (Deemed-to-be University)
Bangalore, India
n.priya@jainuniversity.ac.in

Abstract*— nowadays, the Internet is the most widely used medium to maintain communication with family, friends, work colleagues, and people worldwide. Internet is the means through which every individual exchange information with just a click of few buttons in a fraction of seconds. With this ease of communication comes one of the greatest challenges of managing digital identities and access control for users and applications. As the use of the internet grows rapidly so do the users or people who use the internet and access and exchange the data using the internet in the organization and outside the organization increases. User Data security is a monotonous and significant piece of the IT framework and its user or employee lifecycle control framework. As a result of this, the user's information security is consistently considered while planning security frameworks for an organization. Subsequently, the majority of organizations use Identity and Access Management Systems to keep track of employees and records of the employee's access to accounts and applications on day to day basis. Identity and Access Management System protects access everywhere with a security technique that authenticates every user and device and smartly limits access to applications as per each user's roles and responsibility within an organization. This paper gives an overview of the Identity Management Systems Access Management System and how they are implemented in an organization to manage user security throughout the employee lifecycle.

***Keywords*— Identity and Access Management, IDaaS, SSO, Federated Identity Management System, MFA.**

I. INTRODUCTION

In this day and age, all the individual and business information is being shared on computer networks each day. So because of this security become the most fundamental part of systems administration. An organization's security framework relies on layers of information protection and their various segments that are connected to the organization. This join programming or assembled segments work to expand the general security of the computer network. Because of protection and security, the new technology are accessible over the long run as the strategy for both attack and defence that grows day by day. The network security of an company is predominantly handle by the network administrator who monitor network to safeguard it from unwanted individuals and the resource or application access from unauthorized user who want to access the resource on network. The utilization of Internet is developing quick and each user need the fast result of request, so because of this the exhibition of organization and computers is requiring more because of which the IT security becomes so complex to handle and due to which many organizations are encountering with the challenges of assigning their employees with the right level of access to the right resources at the right time. Hence, an organization adopt IAM solution to automate the IT on boarding and off boarding and also to manage each and every employee's life cycle within an organization in a more effective and efficient way as compared to traditional approach of managing identity within an organization.

Identity and Access Management (IAM) allows every single people within an organization to securely and safely access data and also provides internal security team of a company with a dashboard giving information about current risks and enterprise-wide activity that should be flagged or monitored IAM solutions provides features like Multi-factor Authentication, Single Sign On, User Management, Login Management, Role Management, Services Management, Group Management, Policy Management, Adoption policy, Identity policy, Password Policy, Provisioning Policy within an organization to automate the task of the IT team. The main reason why we adapt Identity and Access Management is reduction in help work area calls for IT support on password resets, permits administrator to computerize IAM and save time costs upgrade administration conveyance, helps IT groups to characterize access approaches for whom and which information to be given admittance, and better control of client access lessens inner and outside breaks. . Modern IAM solutions are mostly cloud-based, and mobile-friendly that gives an organization a flexible solution that's simple to execute for small to large companies.

II. EXISTING SYSTEM

The Architecture is designed to enhance the security of the cloud web index by using a new verification framework. The validation process is done by using multiple factors like the secret key that is created depending on advanced encryption for standard calculation. Each client or customer sends the requirements of the services to the cloud service provider. Calculated precision contract net protocol is used to find a probable agent for user requirements. Review and analyze data storage methods that are most commonly used to storing information of IdP sessions. Create and deploy a browser extension for managing the use of active IdP sessions. The main aim is to find a solution to reduce the vulnerabilities of the single sign-on method. The mentioned system is not hard to implement and if implemented will remove the risk of unauthorized access to valuable information. This paper talks about the IAM model. The model proposed will integrate with the existing security system and add a set of decentralized identity authentication methods and access management methods. This method provides more reliable authentication for each sign-in and also reduces the number of accounts. A fraud detection system predicts the possibility of a successful attack against the authentication method. It monitors the activity and behaviour of the users. Whenever there is unusual behaviour, it raises the flags. FDS creates a user behaviour model and categorizes the unusual behaviour from the model. This behavioural model works very dynamically. The common example is when a user tries to buy new electronics like a computer or mobile. Companies or organizations should set a predefined set of rules by which the devices need to abide before getting access. These rules should be governed by high authority people to protect data security. To achieve such secure architecture the cloud platforms, need to set up SSO functions beyond companies' standard policies. The paper talks about different strategies that can be put to use. Employees and organizations go through very little downtime faced by employees since updates need to trigger manually.

III. PROBLEM STATEMENT

Now a day enterprise IT team face the inexorably intricate challenge of giving granular access to data information and resources, as per roles and responsibilities of users related to the organization internally and externally as per their request while at the same time restricting unauthenticated person to have unauthorized access to sensitive corporate data and resources. A growing distributed workforce is one of the valid challenges that an organization is facing. An organization hire the best talent from all over the world so the workflow doesn’t stop 24 by 7 which not only remove the constraints of geographic location but also boost the productivity of a company. However, with people working from all over the world results in IT team facing one of the most daunting challenges of maintaining a constant and similar experience for all the employees connecting to corporate data and resources from different places of the globe without compromising the security of an organization. Another challenge face by IT team is distributed applications. With the advancement of cloud based applications, employee and anyone related to the organization has ease to login to critical business applications from anywhere and at any point of time. Hence, with this ease comes the difficulties of managing user identities to access these applications. Unavailability for proper method to access these application and proper password management will increase the IT burden and finally increased cost of support for those applications and resources. One more challenge faced by IT team is productive provisioning that comes into picture if there is no centralized IAM system in place in that case IT team staff must manually provision access. The more time it takes for a user to access those critical business application the less productive the use will be and also failing to revoke the access from those application for those employee that resign from the organisation will also cause a serious security consequences. Hence, IT team have to manually provide access to new people joining the organization and also revoke the access when an employee leaves an organization, it is time consuming as well as labour intensive and sometime might also cause human error which is not acceptable. IT team managing all these aspects maybe be efficient for small to medium companies but not for large scale organization with large number of employees with multiple departments.

There are multiple people associated with an organization like employees working in that organization, contractors, partners, stakeholders who access the corporate network with their personal devices. The main challenge here is for the IT team to having to proactively react to protect the organization’s network for any kind of security threats and alerts and IT team also struggle to maintain and manage who has access permissions to corporate data, resources and which devices they’re using to access it. Password problem I must say remains one of the most valid challenges because with the growing number of application that an employee use on a day to day increases per the need of the market and the organization. These applications use different authentication methods and standards and protocols which may be really frustrating for an employees who spend more and more time managing the resulting list of passwords and needing to sign in each and every time daily. Also remembering passwords for each and every application is so frustrating and IT teams have to help the employee whose accounts gets locked because of multiple attempt of account login when they forget their password.

IV. PROPOSED SYSTEM

The proposed system that is designed is to overcome the above mentioned problem statements. A successful IAM solution can solve most of the mentioned problems by providing various solutions that increase the efficiency of the task force within an organization. A comprehensive and properly managed IAM solution provides the visibility and control needed for a distributed workforce to an enterprise IT team. The Identity solution will help the system administrator control, manage and simplify access rights for all the critical business applications hosted on- premise or off- premise or combination of both kind. The robust identity solution can reduce the IT burden by automating the provisioning and de- provisioning process by giving IT team the full access rights of people connected to the organization directly and indirectly. Automated provisioning and de- provisioning will help or speed up the process of enforcement of strong security policies and finally reducing human error while managing these identities. IAM provides a good strategy that will make it easy and fast and secure to grant and revoke access to critical business applications on employees and other devices that are accessing the data and resources of the company. IAM provides solutions like Single- Sign-on and federated user identity which will reduce the password issue that is mentioned above. SSO will give each and every employee an ease of accessing all the applications they use daily in one location by just signing in once and not needing to sign in each and every time reducing the time wastage and increasing the efficiency. SSO can integrate password management across multiple domains and various authentication and attribute-sharing standards and protocols.

V. IMPLEMENTATION

We are going to discuss about the architecture and deployment models for identity access management for cloud services. This is a vast topic we are going to cover three different cloud service models SaaS, PaaS, and IaaS. We will talk in detail with three different deployment scenarios public, private, and hybrid. There are different communication protocols to address authentication, authorization, and provisioning. The cloud security has many different kinds of security standards which make it hard to choose from. It is hard to choose because it is not one size fit different company has different types of requirements. It requires work to determine which standard is good to solve a specific problem. Few cloud service providers even provide security standards which often incompatible with the company requirements. IAM is the starting point for companies to think about cloud identity. Security standards are much better driven by cases and risks. Our main objective is to establish an architecture that fulfils all the company requirements.

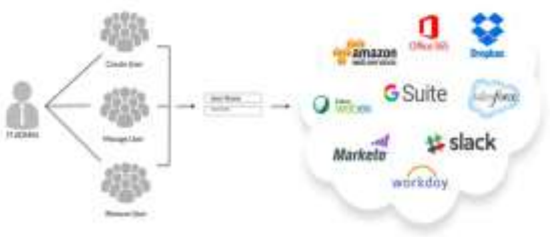

Figure 2: IAM Single sign on

To make it efficient we separate design from implementation standards. The design pattern is a skeleton structure for the underlying environmental complexities. It is a good implement design pattern for each use case to solve core problems. There are three core cloud IAM Methods SSO (Single Sign-On), Provisioning, and attribute exchange SSO is implemented using user identity and related attributes which are stored across different identity management platforms. The identity management repository within a larger group decides to validate a user at the requested time. Federated identity is custom-made for the cloud to efficiently separate roles between the enterprise and cloud provider. Each user can specialize in a field that they are best at handling with the help of identity protocol established to exchange between users. SSO architecture uses one or more identity services to act as an authoritative source for account data. Relying parties generally support cloud providers. Their main task is to accept and verify identity and provide proper access rights to cloud applications. The protocol defines how it’s initiated, which attribute are sent. The entity with the freshest and most correct user data to control and manage the account. The federation method is flexible for single sign-on for open interactive application architecture.

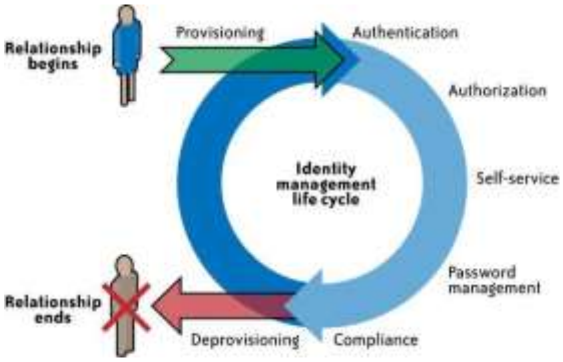

Figure 2: IAM provisioning and de-provisioning

VI. SCOPE

Identity and Access Management (IAM) allows every single people within an organization to securely and safely access data and also provides internal security team of a company with a dashboard giving information about current risks and enterprise-wide activity that should be flagged or monitored. Modern IAM solutions are mostly cloud-based, and mobile-friendly that gives an organization a flexible solution that's simple to execute for small to large companies. IAM solutions provides features like Multi-factor Authentication, Single Sign On, User Management, Login Management, Role Management, Services Management, Group Management, Policy Management, Adoption policy, Identity policy, Password Policy, Provisioning Policy within an organization to automate the task of the IT team.

SSO is easy to implement and manage many sets of credentials, overcome unprotected password management methods and improve the user experience. SSO improves security and productivity. SSO analyses client requirements and provides the best SSO services to fit the requirements. Design and implement the architecture of the SSO method. SSO method also provides an ongoing in-use security process to integrate for your SSO.

Passwords do not provide good protection in a modern organization from new threats. This is when multifactor authentication (MFA) and two-factor authentication comes in to picture. MFA prevents access for unauthorized users from access data that should not be accessible to the user. Implementation of MFA is a huge challenge. Implementing MFA needs a lot of experience handling various security products and applications. The company needs to design a proper MFA architecture for smooth implementation.

Privileged accounts have high-level access like super user access in the confidential system for administrative work and maintenance purposes. These root accounts are usually called keys to the kingdom. If you don't properly secure and monitor, the hackers can escalate privilege access to all your information. These issues can be solved by properly implementing Privileged Access Management. The technology uses advanced AI which predictive methods to automatically identify left out accounts. This method improves security.

VII. CONCLUSION

This study presents an outline of existing projects and structures for user Identity and Access Management systems. Identity and Access Management (IAM) allows every single people within an organization to securely and safely access data. For a business or an organization, an efficient and effective identity management strategy make sure that employees, stakeholders, and customers only access the data expected for them — while limiting access to sensitive information or data which is not meant for them. The way to successful identity management is guaranteeing that the correct individuals are getting access to the correct system. An Identity and Access Management solution is a software solution or framework that oversees and empowers identity management within a company or an organization.

VIII. REFERENCES

[1] G. Senthil Kumar, N. Kandavel, K. Madhavan "To Discovery the Cloud Services Authentication an Expert Based System Using Multi-Factor Authentication" 10.1109/ICACCS48705.2020.9074195©2020 IEEE

[2] Lokesh Saravanan Ramamoorthi, Dilip Sarkar "Single Sign-On: A Solution Approach to Address Inefficiencies during Sign-Out Process" 10.1109/ACCESS.2020.3033570 © 2020 IEEE

[3] Kunying Li, An Ren, Yu Ding, Ying Shi, Xiaobo Wang "Research on decentralized identity and access management model based on OIDC protocol." 10.1109/ECIT50008.2020.00065©2020 IEEE

[4] Libor Dostálek "Multi-Factor Authentication Modelling" 10.1109/ACITT.2019.8780068 ©2019 IEEE

[5]: Sagar Gupta "Single Sign-On beyond Corporate Boundaries" 10.1109/ISMS.2018.00017©2018 IEEE

[6] Michael Kuperberg. "Blockchain-Based Identity Management: A Survey

From the Enterprise and Ecosystem Perspective" 10.1109/TEM.2019.2926471©2020 IEEE

[7] Shantanu Pal "Limitations and Approaches in Access Control and Identity Management for Constrained IoT Resources." 10.1109/EEIC.2001.96563810.1109/PERCOMW.2019.8730651 ©2019 IEEE

[8] Mumina Uddin; Shareeful Islam; Ameer Al-Nemrat "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control" 10.1109/ACCESS.2019.2947377 ©2019 IEEE

[9] Tri Hoang Vo, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann "Privacy-preserving user identity in Identity-as-a-Service" 10.1109/ICIN.2018.8401613 ©2018 IEEE

[10] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy "Multi-Factor Authentication: A Survey" ©2018 Cryptography.

[11] https://medium.com/identity-beyond-borders/identity-provisioning-dd1a8814573e

[12] https://www.akku.work/blog/what-is-an-iam/