Niharika Anand

Role of IAM in an Organization

Bachelor's thesis

Bachelor of Engineering in Information Technology

2021

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree title	Time
Niharika Anand	Bachelor's of Engineering	2021

Thesis title

Role of IAM in an Organization

29 pages
1 page of Appendix

Commissioned by

Kaakkois-Suomen Ammattikorkeakoulu

Supervisor

Matti Jutilainen

Abstract

Many identities are possessed by the user in this digital world. The access rights and the digital identities requires to be managed and controlled at all levels. Managing the identities and controlling the access rights is Identity and Access Management. It is essential for all organizations with thousands of users and is the best practice to ensure control of user access. It identifies, authenticates, and authorizes users to access a resource in an organization. This in turn improves the efficiency of access management. The goal of this thesis was to study the role of identity and access management solutions in an organization. The main aim of the thesis was to find out how identity and access management works and implemented in an organization. Also, what are the risks and challenges when implementing these solutions were studied. Different security faucets which could be used in association with identity and access management were researched. Answer to some questions like how it could be implemented or what are the functions were researched. The use of the cloud to implement these solutions was also studied which protects the access to the resources on-premises and into the cloud. Various authentication methods were studied like multi-factor authentication, single sign-on, etc. The research was based on the work done during the internship in an organization with an identity and access management team. Based on the study and research the conclusion was made which included the benefits of identity and access management in the security and productivity of the organization. The practical part thesis was based on the survey questions answered by managers, the CEO, the IAM team and the IT administrators of an organization. Also, the employees who work in the organization answered the survey. It was done to observe how the accesses and privileges are given according to the job role at different levels.

Keywords

IAM, Authentication, Authorization, Identification

TABLE OF CONTENTS

Appendix 1: Some of the survey questions/answers and to whom they were directed to

1 INTRODUCTION

IAM ensures that the right users have access to resources using the framework of policies. Giving access using identity and authentication to various IT resources also manages access to hardware and applications. Identity and access management have become critical in recent years due to the increase in cybersecurity offenses. IAM products and applications manage the identification and data of individuals, software applications, and hardware related to computers. It covers how a person gains identity or permission is given to access the resources. It can also cover the technologies that protect the identity. User access to critical information can be controlled by managers working and using the IAM framework. Systems like SSO, two-factor authentication, MFA, or privilege access management are used in IAM. Technologies like these provide the ability to secure the identity safely, and the only data that is necessary and relevant is shared within organization is ensured by data governance functions.

Information about the employee, such as what all can be accessed and modified and by whom, is managed by identity access management. Defining rules and privileges of users to access cloud or on-premise applications is the role of IAM (Appendix 1.) Access to devices like smartphones, controllers, etc., is managed for the users like customers or employees. Digital identity individual or device is the core objective of identity management, and it must be maintained, updated, and monitored until the device or user's access life cycle ends. These rules of IAM are not just limited to users but also devices and applications too. Tools and technologies for tracking the activities, reporting them, changing users' roles, and enforcing policies are provided by IAM. Since covid making the physical boundaries irrelevant, identity and access management have become more of a necessity. Businesses moving towards remote users, have given employees not just within the organization but also outside of it access to the organization's internal information. Many companies have invested in IAM-related products since the pandemic began, which was found during survey (Appendix 1.) Defender and enabler of resources behind its walls are what IAM should be considered rather than just the provider of access credentials. Some examples of IAM solution providers could be Azure Directory, IBM security identity and access

assurance, and Oracle identity cloud service. The goal of this thesis is to study the role of IAM in an organization and what are the risks involved in the implementation. This was done by surveying the employees of an organization who have different job roles and privileges. These goals were researched extensively and mentioned in the later part of the thesis.

2 CAPABILITIES

Ancillary data is also controlled by identity management to use applications like contact information with creation deletion or updating user identity. To grant access to the users and the devices is the overall goal of identity management. Some important advantages of identity and access management are:

- It ensures all the employees are authenticated properly and authorized, to perform tasks. Management and storage of user identities and access policies are also an advantage of IAM.
- There is a decrease in internal and external data breaches if the company is properly handling the identities and has better control of the access granted to their employees.
- Overall productivity can be increased using automating IAM systems which allow operations to be more efficient. All the access privileges can be changed in one go once the security policy is updated. The number of tickets sent to the helpdesk for password reset could be reduced. Automation set are also used for repetitive IT tasks. Tools like Spiceworks, Gsuite, etc are deployed for this purpose. (Appendix 1)
- It also adds an extra security layer. Instances of data bridges or illegal access to confidential information could be eliminated by controlling the access of the user. IAM can protect against various cyber-attacks by preventing the spread of sensitive information like login credentials.
- A better user experience is provided. There is no need for the user to keep multiple credentials to access multiple systems. Even passwords and pins are no more required with biometrics being used.

Major concepts are incorporated in identity and access management. These key concepts are identification, authorization, and authentication.

2.1 Identification

Identifying an employee or the application running of the system uniquely is the ability called identification. Something which can uniquely identify the object like username or password could be used to accomplish this. To determine if the subject can access the resource, identifier is used by the security systems. Some

of the identification methods in the physical world could be fingerprints, surveillance systems, DNA samples, etc. Similarly in the digital world, it is possible to identify the user using the technique of device fingerprinting. The user could be identified by their writing style or even the way they play games on the computer. The starting point of security access is identity. Since a lot of sensitive information is usually stored in an organization's IT infrastructure it is very important to identify the users with the same accuracy as physical identities. Any user who wants to connect with the IT system must identify, as this is the primary goal of the identity management system deployed by the organization. (Chanika Ruchini, no date)

2.2 Authorization

What operations an entity can perform is the information authorization manages. Roles-group of processes is called roles. Related to a particular job function, the employees are granted access. These are authorizations that are given to authorize all the users that have been given the role. Delegation is allowing one user to perform actions on behalf of another or modifying systems without a global administrator (Chanika Ruchini, no date). The rest of the identity and access management processes of the organization are carried out by authorization after the user has been authenticated. Authorization in simple terms is what you can do. Definition of an access policy is what ‘to authorize’ means. Having access policies are something on which the access control relies, in systems and networks. Multi-user operating systems release authorization since they include role-based access control. Where a resource is accessed the access control process verifies if the user is authorized to access that resource or not. Access should be given based on the principle of least privilege. Guest users or customers are usually not required to go through authentication since they have limited authorization (Appendix 1.) In some operating systems, the user is granted access to all the resources by default while in others the administrator needs to authorize the user for each resource. An alternative to per-system authorization is an atomic authorization. In this, the authorization information is distributed by a trusted 3rd party (Martin Thoma, 2020).

2.2.1 Delegation

When a another user handles the authentication details by the permission of the owner, it is known as a delegation of authority in computer security.

Delegation can be divided into two classes that are delegation at authentication or Identity level, where an effective identity, different from the validated identity of the user is provided by an authentication mechanism, given that the owner of validated identity has been already authorized by the owner of effective identity and has received the delegated account password. ‘Sudo’ or ‘su’ commands are popular in this technique, while ‘sudo’ command can only be used when a person first starts the session using their original identity.

The second class is delegation at the authorization level, provided by different operating systems such as Linux, Windows, etc., used when the delegation is for only specific rights (Role-Based Access Control delegation). Risk of denial of services is always there in such kind of delegation.

2.3 Authentication

Using passwords, biometrics, or gestures on the touch screen to verify if the entity is whom it claims to be. For example, the user provides the ID to the system, which then authenticates the user using the password that is supplied by him (Martin Thoma, 2020). The authentication factor is something covering a range of elements that are used to verify a person’s identity before granting access. In simple terms, authentication is who you are. Main methods of authentication are:

- Something you know (Knowledge Factor) - This can include the password or the pin which the user knows of.
- Something you have (Ownership Factor) - This includes ownership factors like an identity card.
- Something you are (Inference Factor) - This include inherent factor like biometrics.

2.3.1 Protocols

There are set rules for interaction and verification for endpoints or systems to communicate, called authentication protocols. There are as many protocols, and standards as applications users need to access. It is essential to select the correct authentication protocol, which ensures security. There are some standard authentication protocols as mentioned in SailPoint, 2020.

2.3.1.1 Password Authentication Protocol (PAP)

Due to the lack of its encryptions, this is the least secure protocol to validate the users. To validate the provided credential, there is a routine login process that requires the user to enter the username and password to enter the system. When communicating between the server and the device, this is the last option used.

2.3.1.2 Challenge Handshake Authentication Protocol (CHAP)

To verify the user there is a high standard of encryption using three-way exchange off a secret. An MD hash function is sent to a remote host who has received a local router challenge. Only after the router has matched the expected response, it establishes a connection that is authenticated otherwise it denies the access. While the operation of pap is based on initial authentication approval, the chap is much more secure because it can send a challenge anytime during a session.

2.3.1.3 Extensible Authentication Protocol (EAP)

Many authentication types are supported by this protocol, like smart cards, one-time passwords, etc. EAP is of higher security because it allows remote devices and the access point a mutual authentication using built-in encryptions when it is used for wireless communication. Disconnects the users to such an access point which asks their credentials for the verification by authentication server then it again requests utilizing the server to verify the user and then completes the process.

2.3.2 Types

Authenticating that an entity is what it purports to be is the main task of IAM systems in an enterprise. Entering username and password to login screen is the most basic kind of authentication. The IAM system then checks into the database, if the record matches; it grants access to the resources for that user (Appendix 1.)

2.3.2.1 Single Sign-On

In this solution, the user is granted one set of login credentials which the individual uses to access multiple applications. This method is much easier for the employees since they don't have to keep track of various certificates. Secure SSO links between the resources are all created by identifying a central domain. This also ensures that they are automatically logged out of all the help and applications linked to their account when they end the session as mentioned by the IAM Manager of the organization in Appendix 1.

2.3.2.2 Two Factor Authentication

This kind of authentication provides a double layer of protection to authenticate if the user who is logging in is genuine or not. This kind of authentication is similar to multi-factor authentication. After the password is accepted, the system prompts the user to enter a temporary code sent to a mobile number or email, just as in the case of multi-factor authentication. Impossible for someone other than the original user to have both of these, so it minimizes the risk-off resource compromise.

2.3.2.3 Multi-Factor Authentication

Two or more identifying credentials must be presented by the user except username to gain access to the application in this kind of authentication. This adds another layer of protection to the resources. Like many applications, it asks for a temporary code sent to an email or phone number as soon as the user enters the password. To confirm user identity, factors like biometrics device-based confirmation additional passwords are used. This is like 2-factor

authentication, but the only difference between these is that the user could use more than 2 or 3 steps to verify the user in multi-factor authentication. In contrast, in 2-factor authentication, there are only two steps.

2.3.2.4 Biometric Authentication

This kind of authorization depends on unique biological features like fingerprint voice or face to check identity. These authentications are very strong, but they require external hardware like a fingerprint reader or processing software. Risk-based authentication: As higher risk is detected, the risk-based authentication prompts the user for multi-factor authentication. This usually happens when the user's location is different as it should be based on the IP address or malware is detected. For more precise authentication biometrics is used by modern IAM systems. Fingerprints, voices, even DNA could be collected as a range of biometrics. Biometrics and behavioral authentication are far more secure than passwords. The only drawback of using biometrics as digital authentication is that once there is a data breach it is impossible to recover the password like fingerprints or iris as it can't be swapped out. Also, biometrics is expensive and could be used by large scale organizations only.

2.3.2.5 Unique Passwords

This is the most common type of digital authentication. Numbers symbols, complex passwords are required by the organization to ensure security. It gets difficult to remember multiple unique passwords unless all the information can be gathered using a single sign-on automatically.

2.3.2.6 Pre-Shared Key (PSK)

Users in an organization who are allowed to access the same resources are given a key which is a type of authentication that is digital. As compared to individual passwords this type of authentication is not very much secure. (Gittlen & Rosencrance, no date)

2.3.2.7 Behavioural Authentication

Analyzing keystrokes over mouse use characteristics is used by organizations as behavioral authentication when dealing with information that is sensitive and confidential. If the behavior of the user or the machine falls outside the norm then it is detected by IAM system using artificial intelligence and could lead to system lockdown automatically.(Gittlen & Rosencrance, no date)

In these modern times, there are much better ways to protect resources. Some of them were mentioned above. (Sandra Gittlen, 2021)

3 ACCESS MANAGEMENT

There has to be a way to give rights and privileges for every identity. Its administrators are responsible for the same other than assigning digital identities and authorization methods. Giving the least freedom is the best way to practice access management. This means that access granted to the organization's resources for the shortest amount of time only to complete the task (Appendix 1.)

3.1 Privilege Access Management (PAM)

This type of access is only for the admins or the users who make changes to this system. If these credentials are compromised in any way, it could lead to a severe threat. The accounts are isolated, and their activity is monitored by privileged access management solutions to show that the credentials are not compromised, and also there is no misuse of the privileges. Compromising privileges and credentials are the consequences of data breaches. Privileged accounts need monitoring and protection to avoid such effects. Since the rights of a local administrator are the main target of cybercriminals, implementation of least privilege security who to be critical, both endpoints and privileged credentials need to be secured thoroughly to protect sensitive data.

3.2 Role-Based Access Management (RBAC)

To simplify access, IAM should assign management privileges based on the role of the employee in an enterprise. Access could be given as per the requirement

of the job by the administrator instead of giving one-by-one entry to the privileges. What a user in an organization can create, modify, or view can be controlled by role-based access management. Authorized users can be restricted to access the system using this approach. Performing user assignments are made simply because of the components of role-based access control such as role permissions, user role, etc. huge amount of permissions, and users within large organizations could be facilitated administrations of security using role-based access control. Even though MAC and DAC are different from role-based access control frameworks but the policies can still be imposed without any complication. It is the best practice to manage privileges within a single system. Hierarchical creation of rules and privileges is important to use RBAC within an organization that has an IT structure that is heterogeneous. (Juliana De Groot, 2019)

Across any organization, the process by which identity data is collected and analyzed is called identity governance. To secure the organization and meet the regulatory requirements, a robust identity governance program is required. Information about who you are is confirmed by identity management. It defines job title, reports and confirms that you are the same person whom you say from the database. Access management then based on the confirmed identity allows th user to access the resources of the organization. Like the person who is the manager would be having the access to the timesheets of the employees but he won't be allowed to have the access to his own timesheet.

4 WORKING OF IAM

Earlier, IAM included only essential elements in identity management systems, which were:

- The system uses the directory to define individual users. Tools to modify, add and delete the data.
- Regulating and enforcing user access by a system. Recording and auditing system.

Authentication methods to verify a user or device identity was done by regulating user access. It also verifies passwords, digital certificates, hardware, and

smartphone software tokens. However, in today's scenario, a strong username and password don't cut the height and security threats. So multi-factor authentication has been introduced. To reduce the security risk, the IAM systems use biometrics, artificial intelligence to add risk-based authentications. Access to critical information is controlled by IT, which the IAM framework enables within the organization. The system administrators can change access to resources or network, based on the roles of the users. IAM offers these kinds of role-based access control products within the organization. In an organization, to view, create or modify a resource by any individual is access. Job, authority, and responsibility define these roles. Within an organization, the IAM system does the following:

- The login information of the user is captured and recorded.
- Database of user identities is managed.
- Access to the privileges are given or removed as required.

It means centralized service should be provided by the IAM and make aspects of the company user base visible. Interestingly it just does not manage the digital identities for users but also the devices and applications. Mainly there are two tasks of identity management solutions.

- Confirming that the user is whom it claims to be in the database using their credentials. There are more secure and flexible tools rather than traditional username and password solutions which are IAM cloud identity tools.
- The only appropriate level of access is granted by identity access management systems. IAM allows narrow access in the content management system instead of having access to the entire software suite using username and password.

Many different systems need to be integrated with the IAM system. There are some standard technologies that all the IAM systems support. (Chanika Ruchini, no date)

4.1 Security Access Markup Language (SAML)

The authentication and authorization exchange information security access markup language which is an open standard is used between identity provider and service. To log into the application is the most common method which is provided to the employee by IAM.

4.2 OpenID Connect (OIDC)

To enable logging in into the application from an identity provider OpenID connect is used which is a newer open standard. It is similar to security access markup language in what uses Json through transmit data while the SAML uses XML.

4.3 System for Cross-Domain Identity Management (SCIM)

To exchange identity information automatically between two systems this standard support is used. It is very similar to the previous two but the only difference is that the system for security domain identity management keeps the information of the user updated. It updates or deletes the user when a new user joins or someone leaves respectively in the the enterprise. In the IAM space, this is the key component to provision users.

Earlier users could create user accounts for all the applications to which they want access because the identities and privileges were managed within organization’s premises. For example, if someone wants to access two different applications over services, he has to create two separate accounts and manage the user credentials. In such scenarios, similar passwords are used for both the accounts which result in data breaches. If we look at this from the point of view of the organization, managing multiple accounts can result in high costs and low productivity. Centralized access management systems maintained by IAM solve these issues. A central system is used to handle the authentication of the user and the management of the accounts. identity provider is a component that is used to manage the users. The user is not required to maintain multiple accounts and the developer doesn't have to worry about the management of the user which is the main advantage of centralized access management system in the organization.

Core components that make the IAM framework are:

- A database that has the identities of all the employees and access privileges.
- Tools to create monitor modify and delete privileges.
- A login auditing system that can access history.

Some simple examples of IAM could be:

- When the user enters the login credentials IAM systems verify those credentials using the database of the organization.
- It is also not necessary that someone who logs into the system can access all the resources of the company.
- Access is not granted to everyone for modifying the resources. But special privileges are provided according to the job roles. Without IAM being in effect anybody could view or modify the work.

4.4 Implementation

There must be a system to govern the identity and access for proper data security. The employers' productivity could be increased by using solutions that could allow them to access data on various applications and devices. Also, greater collaboration could be established with other organizations all vendors using IAM solutions. Auditing of existing and legacy systems is the best way to implement an IAM solution. Organizations could collaborate early and often if the gaps and opportunities are identified. All the user types and access scenarios need to be mapped out to show that the decor objectives of the IAM solution could be defined. In day-to-day operations using IAM solutions, the organization and the users can ensure security tracking battles of the highest standards. Also, transparent administration could be ensured. To implement IAM some tools are required like password management tools, security policy enforcement application, skills identity repositories, etc. Some IAM tools could include:

- Multi-factor authentication - It means to access service more than one type of proof is required to say who you are. some choices of multi-factor authentication are iris scan facial recognition etc (Section 2.3.2.3).
- Single sign-on - It means that once the user signs in into the IAM portal and can have access to all the other software without signing into them (Section 2.3.2.1).

4.4.1 Strategies included in IAM implementation

Zero trust principles like identity-based security policies and least privilege access should be used when implementing IAM solutions. The following strategies were mentioned by the IAM manager of the organization (Appendix 1.)

- Central identity management - Having centralized management can make managing access to the resources and identity level on the principle of zero trusts simpler. This means that users could be migrated from other

systems or other user directories could be synchronized with IAM within any environment.

- Secure access - IAM needs to make sure that identities are confirmed for those who are trying to log in. For securing add identity level this is a must. This could be done by implementing multi-factor authentication and adaptive authentication.
- Policy-based control - No more privileges should be given to the user except the authorization required to perform the tasks. Access to the resources based on job role or as required should be the design of an IAM. This then can ensure that the resources, wherever they are being accessed from are secure.
- Zero trust policy - User identity and access points are constantly monitored by the IAM solutions of the organization. Without zero-trust policy, the operations of the organization were like if you are in once, then you have the access but with this policy, all the members of the organization are monitored, and their accesses are managed.
- Secured privileged accounts - All the accounts created in the management system are not equal. The accounts which are granted special privileges to the resources containing sensitive information should be provided support and security.
- Training and Support - Training must be given to the employees and the administrators who are most engaged with the IAM products which ensure long term health of IAM installations.

5 DEPLOYING IAM IN ORGANIZATION

The First Step for the businesses is to decide who will play the lead role in the organization to develop, enact, add and enforce the IAM. The IAM department impacts all the other departments be it users or devices. The IAM design pattern lays out the architecture of various roles that interact with IAM components and the systems that rely on them. The IT professionals need to get familiar with this design pattern before implementing the IAM system. The steps to build an effective IAM structure are as follows:

- Usage list is made with the names of employees the applications/software being used, which validates the assumptions of the user if they are correct, which later helps in selecting the IAM product or service that is correct for the organization.
- Some systems might need a specific type of federation, such as cloud-based applications and on-premises applications linked together.

For the IAM to be successful best practices, need to be kept in mind, including the documentation of expectations and the responsibility. The most crucial part for the organization is to create a process with which they can evaluate the

efficacy of IAM control that is being used currently. In an organization, it is not just the IAM teams responsible for making decisions. Still, it is spread across different groups like development teams, IT infrastructure operation managers, legal teams, and so forth. Managing a secure network is just the beginning of IAM techniques. The IAM should use the same model as the DevOps cloud team for continuous value delivery to deliver the software as per the recommendations. The rule of IAM is not just protecting the users, but it goes beyond that.
IAM also protects agents and containers APIs secrets and application keys, entities like these, and it is recommended that these be managed appropriately with cross-functional teams. Mighty factor authentication polls and adaptive authentication should be tired closely with IAM. Prevention of account takeovers and subtle phishing attacks could be possible if IAM is used appropriately. An evolving authorization mode model for adaptive multi-factor authentication should be rolled out as a recommendation that can safely enable remote access. Takeover attack methods are being evolved and to prevent that, these protections are needed. There is department in every organizations that is responsible for managing the digital identities of the staff and objects. (Appendix 1)

5.1 Functions

There are four essential functions of identity management in the world of online engineering systems.

5.1.1 Pure Identity

Without any regard to access, this is creating management and deleting identities in an enterprise. IAM can construct a model of pure essence by setting rules, for example, unique identities in a namespace. There could be multiple attributes to a given identity and multiple identities to a given entity within a namespace. There are a finite set of properties to a shared identity object that records the information used externally to the model. The user could use properties like digital signatures or software tokens internally to verify identity. Some properties can be maintained, stored, or retrieved without treatment by the model. Identity management is a set of operations that are defined on a given model. How the

model content could be provisioned among multiple identity models is often expressed by identity management.

5.1.2 User Access

This is like a smart card that adds the data associated with it being used to log into services by the employee. User access allows the user to get a unique digital identity that IAM could evaluate and to which IAM could assign access controls. It gets easy for the administrators and employees to use a single identity to gain access across multiple systems. It further allows the organization to minimize the privileges granted, simplifying the monitoring and verification of the accesses. Also, IAM could keep track of the accesses of the user from initiation to termination. Deep learning identity management systems are not just for managing the set of identities but are granting timely access to those entities via their identity. Identity management and access management are the two sets of processes that are closely related.

5.1.3 Service Function

Service function is a system that delivers role-based and personalized services to users and the devices they are using. Services get continuously added for internal users and the customers too. Identity management is required to access these services properly. Further, due to the partitioning of identity management, it is now possible to serve many or all the activities of an organization using a single identity.

Evolution to control access to almost all the digital assets like network equipment portals content is being done for the internal use of identity management. Usually, services require much access to private information like address books or preferences or contact information. Henceforth, it is essential to control who is granted the permit. Identity federation means that without knowing the user's password, federated identity still can authenticate what this system relies on. Users can log in just by establishing against one of the federation systems, which is called the circle of trust. Identity provider and service provider are the two

systems in this setup. To get access to the service provider, the user needs to authenticate against the identity provider. A specific assertion to the service provider is sent by the identity provider when the authentication is successful. Some core functionality provided by IAM systems in a company are:

- Manage user identities - To create, modify, delete the user IAM system can be the sole directory. New identities could be created for the users who require a special type of access to the tools of the organization using identity and access management systems.
- Provisioning and deprovisioning users - Granting users specific tools to access levels is called provisioning. By consulting the managers, the IT department can provision users by their job role. Since it is not possible to provide the role of each user the IAM systems enable role-based access control. This could also work in reverse when the ex-employees need to be removed from accessing the organization's resources to avoid security risks.
- Authenticating users - To authenticate the user IAM systems are used by confirming if they are whom they say. Multi-factor authentication is the most secure authentication today and adaptive authentication is preferred.
- Authorizing users - To grant access to the resources according to the job role or group of the users is ensured by access management. To avoid granting users access individually they can be grouped by their job roles or departments show large cohorts can have the same privileges.
- Reporting - To ensure compliance and to assess the risks to the security the IAM tools generates reports after almost all the actions which are taken on the platform such as logging in, type of authentication, etc.
- Single sign-on - The users can authenticate their identity with just one portal instead of many resources using the identity and access management solutions with the single sign-on (Section 2.3.2.1).

6 RISKS AND CHALLENGES

Privacy concerns are raised when personal information is put onto a computer network. Organizations could implement a surveillance society if proper protection of the data is absent. Heavy use of identity management is done by services like social web and online social networking. The biggest issue is how the users can be helped to decide how they can manage access to their personal information. When the thieves gain access to information related to identity, that is called identity theft. The data could be like the details to get access into the account of a bank. IAM cannot cover everything despite being present in the organization's security stack. The user accesses are called the user's birthright access, which is given to them when they start working in the organization. How

these new users are granted access touches many departments, which causes an issue to delegate this to the right people and managers. The access rights changes should be detected by the IAM systems automatically, which they cannot. It is not feasible to manually adjust the axis privilege and control for many users. Automated on-boarding and offboarding of the users could be considered if this level of automation becomes necessary. For example, if we do not automate the offboarding process, it could guarantee that all the access rights have not been revoked.

Even though the IAM products have gotten better over time, the complexity of user onboarding is still the same. Onboarding cannot be done without excel spreadsheets or other manual methods. It is essential to keep a watch on the users after logging into the systems to monitor what they are doing. Also, the relation between single sign-on and IAM should be carefully orchestrated. The main aim is to integrate one SSO system in every constituency to mediate access to all the organization's applications. Identity management should be built with all the new applications from the start, as suggested by IT managers. The best way to do this would be by selecting a target app that could later be used as the template to pilot any IAM and identity governance. Enterprise could expand this letter to all the apps in the enterprise.

6.1 Identity Theft

Identity theft occurs when there is data is stolen. Personal information is misused to gain financial advantages or other benefits. Personal information can include pins, passwords, and even biometrics. The main difference between data breaches and identity theft is that in identity theft the victim does not have any knowledge of how the personal information was obtained by the hacker. Usually, the victims cannot detect identity theft. It is also possible that the hacker without committing identity theft misappropriate personal information which causes identity fraud. The chances are very low that if there is a data breach in the organization, it would lead to identity theft also. Identity theft could lead to as disastrous as a terrorist attack. there are categories of identity theft.

6.1.1 Criminal Identity Theft

This happens when the hacker has access to the personal information which is then misused to pose as that individual when the hacker is arrested. This could lead to the criminal being late free and all the charges are put under the name of the individual whose information was stolen. Usually, the victim gets to know about the theft only when there is some action taken against him. But even after there is some action taken the victim cannot clean their personal information from the hacker's database.

6.1.2 Financial Identity Theft

This kind of theft is very common. Claiming to be someone else and then obtaining loans or credit is included in financial identity theft. Even the information related to the tax return could be stolen from the organization’s databases and misused resulting in the direct deposit in the account which is controlled by the thief.

6.1.3 Identity Cloning

True identity can be concealed by impersonating someone else in this kind of identity theft. The most common example of this kind of theft is the people who pose as someone else on social media platforms. Another example of this kind of theft is the migrants who try to hide their illegal status. If false credentials are obtained to pass the authentication test, this could continue indefinitely unlike identity theft which is used to gain financial information. In the latter kind of theft, the victim gets to know when there is any kind of transaction.

6.1.4 Medical Identity Theft

In this kind of theft the hacker poses as the patient to get medical care. Insurance information could be obtained from the organization’s database by the hacker to pose as the patient. Due to this kind of theft medical history is added to the record of the victim. Something which is much more valuable to cybercriminals

than credit card information is the data collected by the hospitals or other organizations managing medical aid schemes.

6.1.5 Child Identity Theft

For the imposter's gain, a child's identity is misused. it could be anyone from the family or friends who wants to target children. Since there is no information associated with the account of the children, it is highly valued. Many illegal documents could be obtained using the child's identity. This kind of theft usually goes on for many years until the child realizes it. Children who are in foster are the biggest targets of these cybercriminals. This is because they are moved often and their information is shared with multiple agencies. These foster children who are victims even within their own family are left to deal with this alone.

This kind of personal information is stored in the organizations database due to various reasons. Majorly victims do not realize the identity theft until there has been a negative impact on their life. Usually if the sensitive data of the organization is not protected the hacker can easily gain access to the database which contains all the information related to the employee. The organization stores such kind of data for the purpose of insurance of the family or salary payments, etc. Many of them are made aware of it by the financial institutions or when they find suspicious activities happening in their bank accounts. It is important to watch out for the warning signs. Some indicators which could help in detecting identity theft are:

- An authorized withdrawal from the bank account or the charges for the services that the victim never availed.
- Calls from the bank regarding suspicious activity in accounts.
- Cards like debit or credit being received without applying.
- When a loan is applied credit score is investigated which can also be indicated if such kind of information is received.
- Lack of funds in the bank accounts which cause check bounces because there were unauthorized withdrawals.
- Personal information can be misused which the victim gets to know when the police come to arrest.
- Credit cards are used by someone else could be known when there is any sudden change in the credit score.

- Mails could be stolen or redirected which is known when the bills do not arrive on time.
- Credit score indicating that loan can't be granted.
- Post office sending a notification that the mails have been redirected.
- The hacker could also report their earnings to tax authorities which can be shown in the yearly tax return. It could indicate that the earning was more than what was earned.

Identity theft can be partially mitigated if the IT systems in the organization do not demand too much amount of personal information and access is granted based on the job role or as required to perform certain tasks. The risk is increased when personal identifiers like driving license or credit card information are used to identify and authenticate the user. Users can be exposed when unauthorized access is given to sensitive data by the organization. The organization needs to ensure adequate network security to reduce search risks.

7 IAM AND OTHER SECURITY FAUCETS

The growth of the cloud tools in an enterprise is due to the easy and fast deployment of these services. It will take a longer time if the computers must be installed with software manually. Is it on cloud or data centre is the main difference between on-premise and cloud services. Though the popularity of cloud services has increased there are still some online service providers which prefer on-premises solutions. The best example of this kind of service provider is banks who need to implement these services on-premises for the highest level of security to show that the personal information of the customer can be protected. On-premises, solutions are preferred when the data needs to be controlled highly but still as per the reports more than 80% of the providers will choose cloud as a deployment option by 2022 (Sami Lindgren, 2021).

7.1 IAM and AI

Artificial intelligence has changed identity and access management. Due to which organizations are doing authentication and access management in a much better and improved way. Artificial intelligence is also essential for user and entity behavior analysis so AI can detect those suspicious activities. Indicators such as

wrong login, more often login in less time, login from an unknown location or device or user not on company-provided VPN could signal malicious activity. To flag such indicators in real-time to prevent attempts of the hack AI is used for investigation.

7.2 IAM from the Cloud

IDaas, identity as a service, and managed identity services. Cloud is the new source of identity and access management services offered by vendors. A complementary solution to pre-existing IAM system on-premises could be identified as a service which is one approach. The security provider could manage the identity services. With managed security service solutions monitoring and management of IAM solution off an enterprise which could be running either on cloud or on-premise. (Appendix 1)

7.3 IAM for the Cloud

Traditional systems, private clouds, and public cloud environments are how an enterprise today could have applications and data on-premises. The major challenge is how the access to a resource by the user could be seamlessly possible wherever they are located. An identity and access management system across a hybrid multi-cloud environment that supports SSO and MFA would be an ideal type (Section 2.3.2).

7.4 IAM and BYOD

Bring your device is a program that organizations adapt to show that the employees have the freedom to work with their own devices from anywhere. The organizations could embrace mobility and adjust BYOD securely if the IAM is combined with the unified endpoint management platform.

7.5 IAM and IoT

It is a well-known story that the hacker gained access to the corporate network and stole data by compromising an intelligent aquarium thermometer. The same

thing happened with CCTV cameras which were network-connected. In this world of the Internet of Things, the hacker could hack virtually any device. The hacker has access to the whole network that is wide open without access management in the organization.

8 CONCLUSION

It is difficult for organizations to provide correct access to the levels at the correct time. Proper methods should be implemented to mitigate risks and resolve inefficiencies of the organization. IAM is the way to fulfill this. The domain of identity and access management has expanded mainly with the work becoming remote and maximum usage of mobile devices after the pandemic. The advent of new hardware connections combined with insecure networks, and unprecedented employee expectations increasing requests for remote access to sensitive data and the threat of phishing and other web-based attacks as users enter rogue websites. Artificial intelligence will play an essential role in the future of IAM as it can identify patterns and rapidly expand knowledge at the same rate as exposure. With persistent authentication, the user context is continuously evaluated in each interaction artificial intelligence can analyze microscopic interactions considering time location and even user movement by calculating the level of potential risk at each point. Next-generation AV software, host-based firewalls, and endpoint detection and response (EDR) continue to evolve and enhance security in the organization. It is the requirement of the hour for the companies to have IAM which can provide online security and can also increase the productivity of employees. Right people accessing the tools required to do their jobs is ensured by identity and access management for which tools like Gsuite or Spiceworks are deployed.(Appendix 1) Employee apps could be managed without logging in to each administrator using identity management and access systems. Not just people but other identities can also be managed using identity and access management systems by the organization like software and hardware. IAM should be considered a defender and enabler of the resources rather than just provisioning and revocation of the credentials. Registration and authorizing access in the configuration phase and then identifying, authenticating, and controlling people or groups of employees in the operation phase to access

resources based on previously authorized rights. Managing the information of users is the only task of identity management. It includes information authenticating the identity of users and actions they are allowed to perform.

8.1 Security

Usually, the only failure in the security is the password which when breached can become vulnerable to attack. the worst can be getting access to the email address used for password recoveries. This is when IAM services and tools are used to detect the mistakes and failures when they are made. Identity thefts are also avoided by updating the information of the employees regularly. The IAM plays a major role in the security of the organization by granting the access to only authorised users after proper identification. There is a possibility of data breach or identity theft if unauthorised access is given or correct IAM tools are not implemented. Covid has made IAM essential for the organizations to protect their information from data breach or identity thefts. Too much of the personal information of employees should not be kept in the database as suggested by the IAM Managers in Appendix 1.

8.2 Productivity

As soon as the employee logs in into the main IAM portal the administrator then does not have to worry about giving the right access to the user to perform the duties. The accesses are predefined according to the job roles or group. This reduces the workload from the IT professionals since all the employees get access to the resources as required for their job role. These accesses are managed either as a group or role instead of individually. Authentication methods like single sign on allows the users to access all the resources just by entering the credential once instead of remembering multiple identities (Section 2.3.2.1). This in turn improves the efficiency of the working of the IT administration and helps the organization to track all user activities too using IAM tools.

There has been an evolution of IAM and other access roles over the years. The modern versions can adapt to the organization's environment and is feature-rich.

(Gittlen & Rosencrance, no date) IAM encompasses the following on a fundamental level:

- In any given system, how are individuals identified
- How are roles identified and delivered to any individual
- Maintaining the system by adding, removing, and updating users
- Accesses are assigned as per the requirement to the user or group of users
- Securing the system by protecting the sensitive data within it.

The roles of the IAM are onboarding the users or offboarding the users promptly and managing the access rights. It is concluded that identity and access management play a major role in the working of an organization. It manages the access to the resources after the identification of the users on different levels. In this situation of covid and everything happening remotely the need of identity and access management in any organization has increased. To protect sensitive data from being accessed to unauthorised users the administrators need to implement appropriate identity and access management tools. This is most required today in an environment where it is necessary to provide right access to all the resources to avoid mishappenings. Depending on the level of protection these solutions could be implemented either on-premises or on cloud. Identification of the user when access must be granted to certain resource should be done using proper authentication methods to mitigate the risk of identity theft. Organizations should make sure to centralize all the security and critical systems around identity. The IAM's role in an organization is to decide who can access the resources and under what conditions they can access them. IAM could become irrelevant if it is not connected to all the parts of the business like intelligence or customer and partner portals or the marketing. Accounts for the users are added, deleted, or modified by the IT administrators without delays to avoid unauthorised access to the resources of the organization. Access for users to the resources should only be provided to complete the given task to protect the sensitive data. As the number of cyber-crimes are evolving, so does the security of the organization. Identity solves the access control problem and reduces the cost of building secure systems. It improves productivity and makes it the best choice for organizational security and management (Isha Upadhayay, 2020).

9 REFERENCES

Authentication (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Authentication (Accessed: June 16, 2021).

"Authentication Methods Used for Network Security" (2020) *SailPoint*. Available at: https://www.sailpoint.com/ (Accessed: July 23, 2021).

Authorization (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Authorization (Accessed: June 13, 2021).

De Groot, J. (2019) "What is Identity and Access Management (IAM)?," *Data Insider*. Available at: https://digitalguardian.com/ (Accessed: June 15, 2021).

Delegation (computer security) (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Delegation_(computer_security) (Accessed: June 15, 2021).

Gittlen, S. and Rosencrance, L. (no date) "What is identity and access management? Guide to IAM," *SearchSecurity*. Available at: https://searchsecurity.techtarget.com/ (Accessed: July 22, 2021).

IBM security verify for workforce IAM - adaptive access (no date) *Ibm.com*. Available at: https://www.ibm.com/products/verify-for-workforce-IAM/adaptive-access (Accessed: August 18, 2021).

"Identify, Authenticate, Authorize: The Three Key Steps in Access Security" (no date) *Wallix*. Available at: https://www.wallix.com/blog/ (Accessed: August 9, 2021).

Identity and Access Management (IAM) (no date). SECURITY ENCYCLOPEDIA. Available at: https://www.hypr.com/ (Accessed: June 27, 2021).

Identity Management (no date a) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Identity_management (Accessed: June 25, 2021).

Identity Management (no date b) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Identity_management (Accessed: August 10, 2021).

Identity Theft (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Identity_theft (Accessed: August 15, 2021).

Lindgren, S. (2021) "How to deploy your IAM system: Cloud vs. On-premises," *UbiSecure*. Available at: https://www.ubisecure.com/identity-platform/ (Accessed: August 16, 2021).

OneLogin (2019) *What is Identity & Access Management (IAM)?*, *Onelogin.com*. OneLogin. Available at: https://www.onelogin.com/learn/iam (Accessed: August 18, 2021).

Privileged Access Management Solutions (no date) *Ibm.com*. Available at: https://www.ibm.com/security/identity-access-management/privileged-access-management (Accessed: August 18, 2021).

Role-based access control (no date) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Role-based_access_control (Accessed: August 10, 2021).

Ruchini, C. (no date) "Introduction to Identity and Access Management," *Identity Beyond Borders*. Available at: https://medium.com/identity-beyond-borders/ (Accessed: August 12, 2021).

Thoma, M. (2020) "Identification vs Authentication vs Authorization," *Plain and Simple*. Available at: https://medium.com/plain-and-simple/ (Accessed: August 2, 2021).

Upadhyay, I. (2020) "Identity Access Management: Why Is It Important?," *Jigsawacademy*. Available at: jigsawacademy.com (Accessed: July 6, 2021).

What is identity and access management? IAM, SSO, MFA and IDaaS definitions (no date) *Ibm.com*. Available at: https://www.ibm.com/topics/identity-access-management (Accessed: August 18, 2021).

Appendix 1

Some of the survey questions/answers and from whom that were asked.

Questions	Answers
Why does the organization have IAM team separately if IT managers are already there? (CEO)	IAM manages identity and accesses
Free or paid IAM solutions to protect the organizations sensitive data? (CEO, IAM Manager)	As required to protect data
How expensive it is to deploy IAM tools? (CEO, IAM Engineer)	Not too much
On-premise or cloud solutions? (IAM Engineer, IAM Manager)	Cloud since work is remote
Considering that the organization has single sign-on authentication method, wouldn't it be better if multi factor authentication is used? (IAM Team)	User has to remember too many credentials
What tools are currently deployed? (IAM Team)	Spiceworks
How the team mitigates the risk of identity theft or data breach? (IAM Associates)	Managing access and identities
What all employee information is stored in the database? (Employees, IAM Team)	Only the information required for work purpose
How did you know which solutions will suit the organization’s needs? (CEO, IAM Manager)	Depends on the information in database
Was the investment in IAM solutions made before or after the pandemic started? (CEO)	Earlier solutions were on-premise but now everything is on cloud
Except from the employees are guest users also required to go through different levels of authentication? (IAM Associates)	No, they have least privileges

What are the main roles of the IAM team? (IAM Team)	Manage identity and access of user
How the IAM team grants access to a user? (IAM Engineer)	After the user proves identity
What kind of practices are used during access management? (IAM Engineer)	Principle of least privilege is followed
What kind of strategies are used when IAM solutions are implemented? (IAM Manager)	Secure access, zero trust, training, etc
Except IAM team is anyone else responsible for making the decisions? (CEO)	All the departments are responsible