International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-13 Issue-6, January 2024

A Model Apporach for Identity and Access Management (IAM) System in the Cloud

Anil Kumar, Abhay Bhatia, Anju Mishra, Tanu Gupta

Abstract: ***Through use of cloud computing, information may be accessible from a range of different types of devices. It is now possible to communicate with a company at any time or location, regardless of location or time zone. Using the cloud has a number of advantages, some of which include lower expenditures on information technology and infrastructure expenses, more agility, and improved continuity planning. These benefits can only be attained via the implementation of a reliable identity and access control system for cloud applications and services. Managing these identities and limiting the access that cloud clients and applications have continues to be a significant challenge in the modern day. In order to strengthen the protection offered by a venture, it is necessary to set up a trust worthy identity and access management (IAM) system in the cloud. The findings of this study provide an intelligent and reliable IAM system that is based on cloud computing.***

Keywords: IAM, Cloud Computing, Access Control System, Reliable Identity, SAML, SPML, XACML

I. INTRODUCTION

Intelligent solutions from the future generation of IT operations boost the efficiency and accuracy of digital identification access permissions in near real-time. IAM's patent-pending innovation lessens the difficulty of managing and collecting information from many systems and sources to keep track of who has access to what. With the aid of artificial intelligence and machine learning, by doing so, it facilitates more precise and rapid adjustments to user rights that occur in almost real-time contextualized identification decisions and remain up to date with changing user access rights (Mohammed, 2021, [6]).This allows businesses to proactively identify risky areas that may benefit from more management without resorting to the time-consuming and error-prone manual provisioning of existing IAM solutions. It's crucial to know everything there is to know about the person and the situation at hand while managing their access permissions.

Manuscript received on 02 January 2024 | Revised Manuscript received on 10 January 2024 | Manuscript Accepted on 15 January 2024 | Manuscript published on 30 January 2024.
*****Correspondence Author(s)
Dr. Anil Kumar*, Department of Computer Science & Engineering, RIT, Roorkee (Uttarakhand), India. E-mail ID: chauhananil01@gmail.com, ORCID ID: 0000-0002-8918-3004
Dr. Abhay Bhatia, Department of Computer Science & Engineering, RIT, Roorkee (Uttarakhand), India. E-mail ID: dhawan.abhay009@gmail.com
Dr. Anju Mishra, Department of Information Technology, AKGEC, Ghaziabad (U.P.), India. E-mail ID: anju.iitd@gmail.com
Tanu Gupta, Department of Information Technology, AKGEC, Ghaziabad (U.P.), India. E-mail ID: tanuparmar2810@gmail.com

The issue is that rather of being based on complete knowledge present access control techniques are instead dependent on assumptions. We have created a proactive identity management strategy using our IAM capabilities that reduces human error and costs, raises risk awareness, and makes it easier to spot outliers. Swinging doors and towers can now have better functionalities and safety thanks to integrated solutions leveraging cutting-edge analytics and artificial intelligence (AI).(Programme , 2022, [8]|)

IAM is continually growing in critical areas, including administration of consumer contact preferences, data security, authentication, internal data synchronization, and compliance with privacy regulations. It is imperative that the relevance of an intelligent and experienced IAM strategy not be understated in any way. There is a great deal of difficulty, for many businesses, in defining who will have access to what information, which leaves their systems vulnerable. Based on their research, Forrester concluded that 83% of companies do not have a developed IAM strategy. The risk that these businesses will face challenges related to data violation is twice as high as it is for enterprises that take an IAM approach. In addition to this, the research establishes a direct connection between improved IAM practices and lowered potential dangers to employees and customers, increased productivity, enhanced management of privileged activities, and significantly reduced monetary losses. The major objective of this endeavor is to investigate the ways in which AI and IAM may work together to enhance cyber security and other aspects of operations(Ahmad , 2022, [1]).

II. LITERATURE REVIEW

Almulla et al. 2010 [12][15][16], businesses are looking to the cloud horizon to grow their on-site infrastructure. In the market, it offers a number of services, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Confidentiality, integrity, and availability are the three information security issues that will be covered in this study. The ownership of their data is a major problem for the majority of enterprises. In addition to discussing Identity and Access Management (IAM) security issues, this paper will outline the current status of user access to the cloud, including authentication, authorization, and auditing, as well as new IAM protocols and standards

Mukundrao et al. 2011 [13][17][18][19], this work addresses the cloud computing data storage security issue by proposing a more flexible and effective distributed verification scheme.

The methods for securing user data include encryption before storage, user authentication processes before storage or retrieval, and creating secure channels for data transmission. These methods rely on the cryptographic algorithms [RSA] and digital signature techniques. This technique finds misbehaving servers while achieving the availability, dependability, and integrity of erasure-coded data; hence, anytime data corruptions happen during the storage correctness verification, this technique should finds the problematic servers, A thorough performance study reveals that the plan needs to protect user data in cloud computing from malfunctions, illegal data modification attempts, and even server.

M. Mackay et al. 2012, one of the biggest developments in computing over the past ten years is the emergence of virtualization and cloud computing. But even with its growing popularity, a number of technological obstacles keep it from reaching its full potential as a genuinely ubiquitous service. The concerns of data security and customers' mistrust of using cloud services as the basis for their IT infrastructure are crucial to this. This is an extremely complex issue with numerous interrelated components that still need to be properly resolved, such as robust service guarantees, platform integrity, data and network security, and many more. This paper presents a revolutionary integrated platform idea to improve the security and integrity of cloud services. Next, it is utilized in the context of crucial infrastructures to ascertain the fundamental parameters, constituents, and attributes of this infrastructure.

Abdulla et al. 2014, the provision of strong identity and access management (IAM) to users is one of the main goals of the majority of organizational information security solutions. This includes systems that are distributed throughout the world and that provide the organization with constant access to sensitive and private data. Given the rapidly increasing number of mobile devices on the market, coupled with their limited resources, cloud computing has become the natural choice for executing resource-intensive operations over the cloud. Cloud service providers (CSPs) are developing new services, such Security as a Service (SecaaS), to address the security challenges. Based on our examination of security risks and countermeasures, we believe that mobile cloud users need more controls for Identity and Access Management. For customers and service providers to take into consideration, we have provided some security guidelines and best practices for ensuring strong information security, including IAM for expanding mobile users in the cloud.

Zahoor et al. 2017 [14], Network access to a shared resource pool for computation, storage, and several other purposes is made possible via cloud computing. We address cloud authorization, one of the major security challenges associated with cloud computing adoption, in this study. We have introduced a formal model that can design and validate Identity and Access Management (IAM) rules on Amazon Web Services (AWS) called Attribute built Access Control (ABAC). The foundation of the model is Event-Calculus. The proposed approach is expressive and scalable. We have provided general Event-Calculus modes in addition to tool support to automatically convert JSON-based IAM policies in Event-Calculus. We also provide performance evaluation results on actual IAM policies to validate the scalability and practicality of the solution.

Tariq et al. 2018, Cloud computing's Identity and Access Management (IAM) is a broad field that provides safe access to cloud resources. An effective identity and access management system (IAM) is essential to preserving the cloud-stored data's Confidentiality, Integrity, and Availability (CIA-triad). IAM must receive attention from the research community since it is a crucial security element of cloud computing. Because directory services map user access to various apps and devices, they are at the core of an organization's Identity and Access Management (IAM). This paper describes the importance of directory services and how to properly comprehend them. Additionally covered in the article is directory-as-a-service, a solution that minimizes the difficulties businesses have while using directories. The directory supplied as a cloud service, or directory service supplied via the cloud as opposed to on-premise directory solutions, is the main focus of the directory-as-a-service paradigm.

Schulze et al. 2018, the Payment Card Industry Data Security Standard (PCI DSS) mandates that any entity of the cardholder data environment (CDE) involved in the credit card payment process has to be compliant to the requirements of the standard. Hence, cloud services which are used in the CDE have to adhere to the PCI DSS requirements too. Identity and access management (IAM) are essential functions for controlling the access to the resources of cloud services. The aim of this research is to investigate the aspects of IAM required by the PCI DSS and to describe current concepts of IAM for cloud services and how they relate to the requirements of the PCI DSS.

Utkarsh et al. 2020, this study demonstrates that the primary concern with cloud computing is security and privacy. Businesses must consider before outsourcing their services to the cloud. We must keep important information like credit card details and license plates hidden from the public since digital photos include them. We describe a novel way to secure picture partitioning for cloud computing, where critical data is stored on private cloud while the remaining non-sensitive portion is stored on public cloud. Only authorized users will be able to access the private cloud with the use of tokens, while anyone can access the public portion. Essentially, this method considers two approaches, storage of data and safety.

- **Gaps in the Overall Identity and Access Management**

For enterprises of all sizes, modernizing an IAM program in the cloud is challenging. Individuals that own on-premises identity and access management systems typically owe money on their systems' upkeep and adaptations. It will take some laborious work to go through this tangle and transition to a contemporary, cloud-based IAM system. For example, the company needs to make sure that users have easy access to the appropriate resources at the appropriate times and for the appropriate purposes.

III. RESEARCH METHODOLOGY

Methods of qualitative research are utilized here in the carrying out of this study. The research is based on the analysis of data acquired from previous studies as well as interviews with subject matter experts. For the purpose of researching the theory behind cloud computing and IAM, the scientific literature is consulted. The purpose of these interviews is to evaluate how well the concepts of IAM and cloud computing translate into actual practice. This research takes a methodical, step-by-step methodology. First, the IAM processes that are required for a conventional IT setting have been identified. Second, the various IAM designs that exist in a cloud computing context are identified and accounted for. Third, research is conducted on the changes in IAM procedures that occur within a cloud computing context. The variations in IAM processes in a cloud computing context are identified through a combination of interviews and research into the relevant literature. These variations are analyzed in search of loopholes and vulnerabilities, which are referred to as risks. Studies of existing literature and analytics are utilized in order to locate any and all dangers. In order to frame the risk research, KPMG's model for cloud computing risks has been modified, and this model is being employed. The following types of business risks are accounted for by this model: financial, vendor, regulatory and compliance, data, operational, and technological. The legal, data, technological, and operational risks associated with IAM in the cloud are all thoroughly examined. Risk related to rules and regulations encompass all those that apply to the organization and how well they are complied with. Data risks comprise all of the security guidelines and standards put in place to protect the organization's data. Risks associated with technological modifications for IAM in a cloud computing environment are referred to as technology risks. All risks connected to the operational management of the organization are included in operational risks. Controls can be put in place or already exist to eliminate, reduce, or mitigate risks. The COBIT framework is used to establish controls for the recognized risks. A frequently used framework for IT governance and control is COBIT. Alternatives like ISO27001 and SAS70 have a less ideal domain structure and are too extensive for our investigation. The lack of an IT focus in the COSO framework also makes it less appropriate for this study.

IV. THE IDENTITY ACCESS MANAGEMENT (IAM) SOLUTIONS

The two categories of Identity and Access Management (IAM) systems are “Identity Management” (IdM) and “Access Management” (AM). The Identity Management system is used to control user profiles and rights. For managing the provisioning and de-provisioning of capabilities, workflows are employed. Access management refers to the practice of using user profiles for the purpose of restricting access. It takes care of things like user authentication, Single Sign-On (SSO), and permissions.(Liu , 2021, [5])

Controlling who has access to what systems is an essential component of keeping data safe online. Keeping track of who may access what, when, and where is becoming more challenging as traditional perimeter barriers crumble and employee turnover rates grow. The importance of SSO, Meta Directories, LDAP, Virtual Directories, automated provisioning/de-provisioning of user accounts and privileges, and role management is growing as threats and regulatory requirements do the same. When properly implemented, identity and access management guarantees that only authorized users can access data when and where it's needed. IAM satisfies the need to guarantee correct resource access in a variety of evolving technological contexts while also satisfying more stringent regulatory constraints. Each and every company should priorities IAM as a top priority. As the focus of IT shifts more toward the business world, it will become increasingly important to have achieved great success in addition to technical know-how. The author conducts research into the area of rules and the relevant conceptual framework for structuring the IAM, and their findings point to the existence of the following central process.

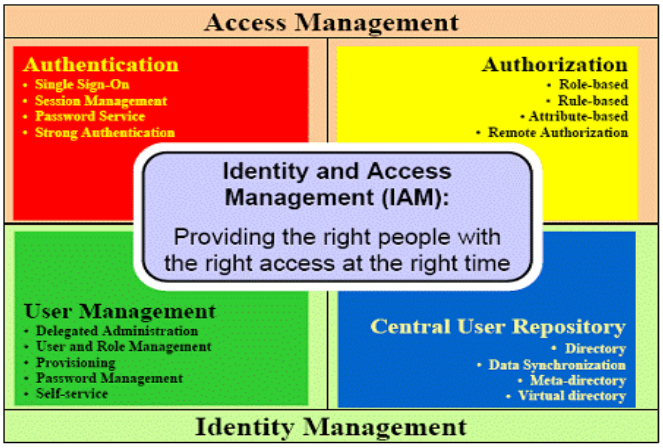

Figure 1: IAM Security

Provisioning of Identities: The process of providing identities within an organization, which includes both the creation and deletion of user accounts referred to as "identity provisioning."

Management of users: Managing the identities of all those who access an organization's resources

Authentication: The term "authentication" refers to the act of checking a person's claimed identification with many sources of information. These methods include things like a password, a certification, biometrics, and so on.

Authorization: The authorization module provides a client-side interface to enable the enforcing of authorization rules whenever a client attempts to perform an operation within the system. These guidelines determine who can see and do what with the information stored in the system.

Policy Management: This module is in charge of enforcing the policies that determine which users have access to which resources. It works out which policies are relevant to a user and figures out which resources that user is allowed to access in order to make those determinations.(Canedo, 2022, [3])

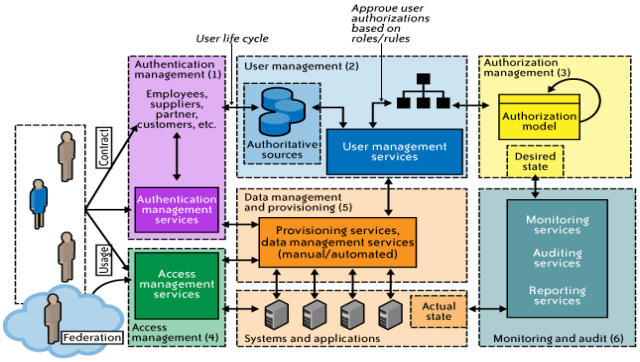

Figure 2: Functions of IAM

In the Cloud, many potential solutions to this problem have been proposed, but at this time, no single standard has gained widespread acceptance. At this time, the most successful companies in the world have come up with various identity management systems. Microsoft Identity & Access, IdM4Cloud, Novell Identity Manager, and McAfee Cloud Identity Manager are just a few examples. The majority of the existing architecture is geared on user identity information management and authentication, authentication, and access control in a unified platform. Furthermore, users are rarely involved in the uploading of resources, whereas the existing framework is primarily meant for the access management of cloud resources.

V. IDENTITY ACCESS MANAGEMENT- THE FRAMEWORK

Examining the most important projects to standardize the industry and identifying the needs, benefits, and drawbacks of implementation are all important steps toward ensuring the widespread adoption of standard IAM principles. From this examination of the original sources, we are able to extract some key principles for IAM, such as:

A. Security Assertion Markup Language (SAML): It is written in XML, and its full name is the Security Assertion Markup Language. It makes it possible to share information on identity and security across the entirety of the security domain. SAML is required in order for a system to be able to exchange its security information with several other systems. On the other hand, in addition to this standard SSO, it may also be used for a range of other functions. The following examples demonstrate how the SAML standard can be applied in a variety of contexts, including single sign-on (SSO), federated identity, and online services, among others. Two parties are required for the SAML exchange to take place at a bare minimum: the party that is sending the message and the party that is receiving the message. In some implementations of this standard, users of a browser window or program that executes SAML are considered entities, and in some situations, they may even take on the role of the sending party. It is usual practice to refer to the party that makes a SAML statement as a SAML authority. A SAML statement is made by a system entity, which is referred to as the sending party. The recipient, on the other hand, is an entity that makes use of assertions that have been made. In order to provide support for the SSO system, SAML defines entities that are capable of functioning as Identity Providers (IdP) and entities that are capable of functioning as Service Providers. The declaration that is included in IdP includes data about users, such as their e-mail addresses and other information. After the user's identity has been verified by entering a password to access the system, the Service Provider is able to ascertain the user's access privileges by examining the user's email address(Andi, 2021, [2]).

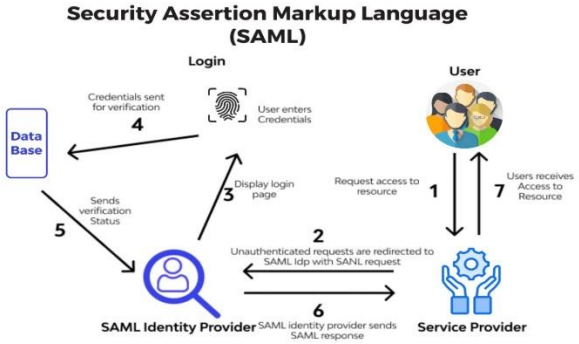

Figure 3: SAML Working

B. Service Provisioning Markup Language: A conceptual framework that was established as an XML application by the "Organization for the Advancement of Structured information Standards" (OASIS). Because of the existence of this conceptual framework, businesses now have the power to reveal unrestricted information regarding their clients, services, and available resources. SPML is a brand new standard that is currently being developed to aid businesses in easing the process of establishing user IDs that can be utilized in cloud computing environments. This is being done in order to facilitate the creation of the standard. The development of a brand-new standard is facilitating the completion of this simplification project. To provide an illustration, a cloud-based application might send a request to an organization's enterprise resource planning system (ERP) in order to update the information on user accounts. In addition to this, the functioning of ERP systems typically makes use of cloud computing. All the software as a service (SaaS) providers will be able to provide immediate account creation for newly registered users, provided that they are able to guarantee support for software that is delivered as a service (software as a service, or SaaS) (Slamet, 2021, [10]). This new user-based management system will provide users with enhanced efficiency in comparison to the traditional user-based management system, which requires users to register in advance. Adoption of SPML could lead to standardization and automation of the access and rights management for cloud services, without tying customers down to a proprietary format. This would be advantageous for both customers and service providers. This would be beneficial in many ways. A cloud-based service provider retrieves information about a new user's attributes from a SAML sequence, generates a real-time SPML message, and then sends it to an authentication service so that the new identity can be added to the cloud-based user's database. This is the most recent iteration of this process. Adoption of SPML may also lead to a reduction in the number of errors that occur during the authentication process. This would be a positive outcome.

Retrieval Number: 100.1/ijsce.D364514040924
DOI: 10.35940/ijsce.D3645.13060124
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

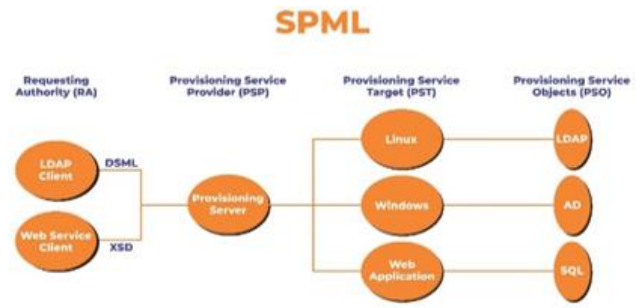

Figure 4: SPML Architecture

C. eXensible Access Control Markup Language: XACML is not only a declarative access control policy language that is implemented in XML, but it is also a processing model that specifies how the rules should be processed. This model is in addition to the fact that XACML is implemented in XML. Access control provided by XACML is more adaptable, general, and expandable than that provided by an access control list (ACL). The OASIS standard known as XACML provides a description of both a policy language that is implemented in XML as well as an access control decision request/response language that is also implemented in XML. Both of these languages are used to communicate with one another regarding access control decisions. The markup language XML is used to implement both of these languages. The policy language outlines the overall access control needs, and it comes equipped with standard extension points that may be used to define new functions, data types, combine logic, and so on. You are able to build a question in the request/response language to inquire as to whether or not a particular activity should be permitted, and then analyze the response. Permit, Deny, Indeterminate, which means that a decision cannot be made because an error occurred or some required value was missing, so a decision cannot be made, and Not Applicable, which means that the request can't be answered by this service, are the four values that are always included in the response regarding whether or not the request should be allowed. Indeterminate means that a decision cannot be made because an error occurred or some required value was missing, so a decision cannot be made(Andi, 2021, [2]).

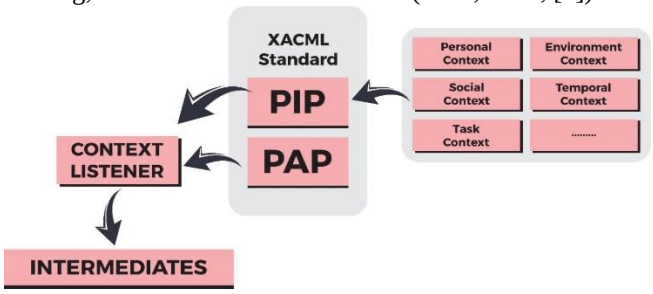

Figure 5: How XACML Works

D. Open Authentication (OAuth): OAuth 2.0 is an authorization mechanism that enables users to gain access to a variety of services without being required to expose their credentials in any of the interactions that they have to take part in. This frees users from the burden of having to remember multiple sets of login information for each service. When a user authenticates himself to an authorization server, the user is rewarded with one of two possible outcomes: either an authorization code or an access token. This scenario truly takes place in the real world. This code or token can then be used to gain access to resources, and the user does not need to re-authenticate themselves to the authorization server or provide their username and password each time. Tokens of access are checked for validity with every request that is made for a particular service. Because of this procedure, there is a risk that the performance of a distributed architecture would suffer, which could have a significant influence on the whole system. This is as a result of the fact that if there is a large number of authentication requests, the performance of the server may be negatively affected(Shankar., 2021,[9]). OAuth 2.0 has quickly become one of the most widely adopted protocols for usage in access delegation inside micro service architectures. It is possible to implement it in online applications as well as backend services, and it concurrently satisfies the authentication and authorization concept. Moreover, it is backwards compatible. It is essential to highlight the widespread implementation of OAuth 2.0 as an authorization protocol, which is used to safeguard services that make use of the Representational State Transfer (REST) model. In addition to the utilization of the HTTPS protocol for the purpose of data transfer, it is important to highlight the widespread implementation of OAuth 2.0 as an authorization protocol.

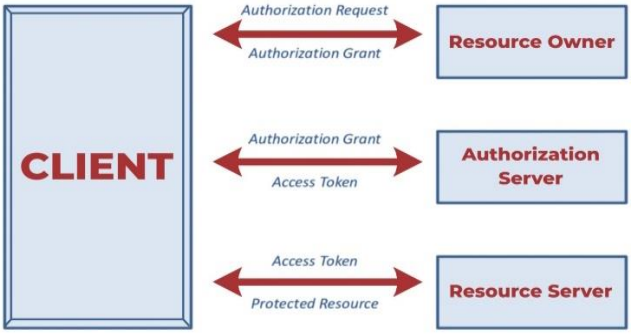

Figure 6: OAUTH 2.0 Working

E. OpenID: User-Centricity was a primary consideration throughout the development of OpenID Connect, a protocol that enables the deployment of federated identity at scale. The protocol is built in such a way that the Identity Provider will only reveal the claims about the End-User to the Relying Party once they have obtained agreement from the End-User directly. Because of this, Identity Providers are given the ability to enforce consent as the legitimate basis for the presentation based on the privacy notice provided by the Relying Party. Additionally, the protocol makes it possible for two distinct types of identity providers to function: those managed by the End-Users, and those offered by third parties(Editors., 2022, [4]).

F. Information Card: Information cards offer a graphical representation of one or more claims (stated identity attributes), which can be put to use for a variety of purposes including registration, authentication, and others. The promotion of information cards was led primarily by Microsoft, but it also received support from a number of other vendors.

Microsoft was providing support for claims-based identity and information cards via a set of related product components, the Eclipse Foundation was providing support via their Higgins initiative, and access management vendors were supporting claims-based identity and information cards to varying degrees. The OASIS Identity Meta-system Interoperability standard contains a codification of the concepts surrounding claims-based identities as well as the supporting standards(Ahmad, 2022, [1]).

G. Open Authentication (OATH): Open Authentication (OATH) and Hash-based Message Authentication Code (HMAC-SHA-1) are two examples of open-sourced algorithms that are used extensively in the process of developing single-use passwords. Both of these methods are hash-based and employ SHA-1 as their hashing algorithm. The OATH protocol utilizes an event that was developed on the basis of the OTP algorithm. This procedure, in the majority of instances, makes use of sequences of secret character request numbers, and on rare occasions, it also makes use of other data, such as a customer's unique seed. OATH events are solely attended by parties; hence there are no other participants. In order to generate the OTP, the procedure is used on each and every piece of data that is available. RSA was the first business to offer an enterprise OTP solution that made use of a number of software platforms in addition to other types of factors such as a token. RSA's solution was also the first enterprise OTP solution to use multifactor authentication. The one-time password (OTP) and the validity period that was synchronized between the client and the server-side are both calculated by RSA using a time-based technique. These values are then synchronized between the client and the server. It is necessary to offer the user with a sign that indicates the length of time the secret code will be valid in order for the user to be able to utilize the code before the allotted amount of time has passed.(Wu, 2021, [11])

H. Open Authentication API (OpenAuth): Certain websites and programs are able to authenticate to America Online (AOL) and the AOL messenger because they make use of an application programming interface (API) that was developed by America Online (AOL). With the assistance of the AOL Open Authentication API (OpenAuth), third-party websites and applications are now able to authenticate AOL and AIM users directly through their very own websites and applications. This capability was previously only available to AOL and AIM itself. Users of AOL or AIM can now access AOL services or new services built on top of AOL services in a seamless manner by logging into a third-party website or application and accessing those services using their AIM or AOL credentials. This allows users to access AOL services or new services built on top of AOL services in a way that was not previously possible. Users are able to access AOL services as well as new services developed on top of AOL services in a smooth manner thanks to this. The following is a list of some of the Benefits:

- It grants access to the user's data, but only to a limited extent, and it grants access even after authorization tokens have expired.
- It makes it possible for users' data to be shared without the need for the release of personally identifiable information.
- It is simpler to install and offers more robust authentication.

I. JWT in Cloud Computing: Popular for use in SaaS (Software as a Service) and cloud computing applications, JSON Web Token, or JWT, is an authentication and authorization mechanism. It is a clear and safe method for two parties to convey their arguments. Here are a few instances of how cloud computing and SaaS could use JWT:

- ***Statelessness:*** Because JWTs are stateless, the server is spared from maintaining track of each user's session information. All pertinent information is contained in the token itself. Consequently, SaaS applications can be dispersed among numerous servers or micro services with more ease.
- ***Security:*** JWTs are digitally signed using a secret key or a public/private key combination. This prevents manipulation and safeguards the integrity of the token. To protect the secret content of the token, JWTs can also be encrypted. Because of these security features, JWT is a reliable technique for authorization and authentication in cloud computing environments.
- ***Single Sign-On (SSO):*** JWT can be used in SaaS applications to enable Single Sign-On for multiple services. After signing in and getting a JWT from an identity provider (IdP), a user can use the same token to access several SaaS services that trust the IdP. This eliminates the need for users to log in separately to each SaaS service, improving user experience and reducing costs related to credential management.

VI. IDENTITY ACCESS MANAGEMENT AND THE CLOUD

"Identity and access management", also known as "IAM", refers to the security-related mechanisms that enable resource security and maintain the identity of cloud services. It is possible for it to carry out a wide variety of tasks, including identity management and maintenance, the enforcement of policies, authentication, and authorization. IAM ensures that only the appropriate identities are used when accessing particular services. It is responsible for managing them and ensuring the safety of each individual identity. The process of verifying the user's or service's identity is referred to as authentication, and the mechanism that does so is called an authenticator. In a cloud computing environment, authentication guarantees that only users who are authorized to do so can gain access to the various resources that are made accessible by the cloud service provider. Authentication is the mechanism that enables one entity to approve another entity and is considered to be the mechanism. The goal of this feature is to verify that only authorized users or applications are able to access particular resources. Authentication is a process that is carried out through the software or as a component of the software itself. If the resources that are kept in the cloud are accessed, then cloud computing authentication is ensured; in this situation, the identity of the user is offered to the cloud service provider.

Retrieval Number: 100.1/ijsce.D364514040924
DOI: 10.35940/ijsce.D3645.13060124
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A cloud provider is able to select and provide a variety of authentication mechanisms, each of which offers a different level of safety and protection. The efficacy of these mechanisms is directly proportional to their reliability and integrity.(Partida , 2021, [7])

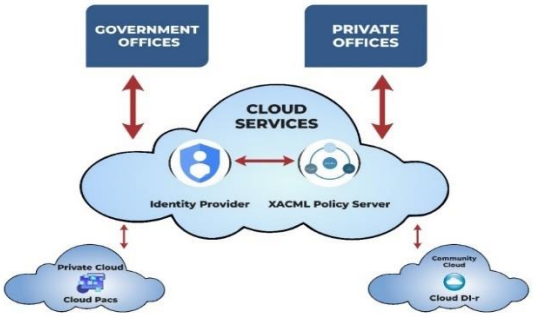

Figure 6: Common Services used in Cloud

A. Functions of IAM are:

i. *The Cloud Identity Management:* "Identity Management" (or "IM" for short) refers to the company's internal information management system. This represents the methodical administration of a single identity within the confines of the organization, including authentication, rights, authorization, and roles. The primary objective is to improve safety and output by decreasing overhead, redundancy, and downtime. Because of the diverse nature of cloud computing, identity management must account for every type of user, each of whom may engage with a different set of devices in a different setting. Many IM services show that directory integration is possible for both wired and wireless users. This is so because the directories used by both sorts of users are shared. With this service, consumers can make better use of their existing setups. Additional security options include access control, single sign-on, digital identity management, and a password manager. Cloud services have a number of benefits that cannot be matched by any other traditional product. Proceed through the steps below to acquire an understanding of the few advantages that come with identity management in cloud computing.

- **Network Capability Enhancements:** With IM, or identity management, it's easy for all users on a network to access the same set of resources.
- **Provides a secure collaboration:** SaaS protocol provides safe and reliable communication between all of your virtual networks of vendors, wholesalers, and business associates.
- **Support On-demand improvement:** A cloud-based solution shields businesses from the issue of customer turnover. Whenever necessary, all professionals may offer 24-7 help and monitoring.
- **Boost Overall Productivity:** It is well known that service providers configure and host cloud-based services. Additionally, this can cause users or any other clients a minor or nonexistent trouble. As a result, numerous businesses can boost their general production.
- **System of Centralized Management:** Users of cloud-based services can centrally administer their company's various services and software. Identity management can be accomplished with a single click on a centralized dashboard.

ii. *Assurance of the implementation possibility of federated identity and single sign-on (SSO):* Due to its advantageous usability and security guarantee to reduce password fatigue and the security risk of accessing third-party websites, Single Sign-On (SSO) has been widely used during the past 10 years. Among the social networking and email providers that provide free Web SSO solutions are Google, Microsoft, and Facebook. Initially, federated identities were to be used for cross-domain authentication through SSO. With significant work concentrated on the security enhancement of the federated identity and related administration systems (IdPs), the majority of today's online Service Providers (SPs) totally outsource the account authentication process to reliable and trustworthy Identity Providers. After the IdP side authentication is successful, the associated online account is usually accessible by an end-user without the need for additional security checks(Liu, 2021, [5]). The Authorization Code Flow, which involves the token access and URL redirection across three key parties—the end-user, service provider, and identity supplier—is frequently used for SSO authentication. Individuals that attempt to enter into internet services or accounts are known as end users. Websites that offer services to end users are known as SPs. The identity management systems called IdPs are in charge of giving SPs authentication services. In a cloud environment, various application services may be hosted and may make use of the same physical resources. Each application service is conceptually isolated from the others, nevertheless. Because different types of system entities use these services, the application service provider must oversee a suitable process for choosing access control options. This means that, following successful authentication; various users should look for and utilize the resources and services for which they are authorized in a particular enterprise security domain.

iii. *Authorization Management:* Role-based access control (RBAC) cloud environments are suggested to use the central security system. The system provides authorization services for cloud-based application services. The entire security architecture includes the Policy Decision Point (PDP) server. It establishes a role-based access control system and provides authorization services to application service providers within a security domain. The Policy Administration Point (PAP) component provides policy administration services to security administrators. It acts as the main policy repository, and security managers' creation and storage of security policies provide the basis for authorization choices made by the authorization service provider. The PAP part of the suggested security solution is implemented on the PDP server. The security administrator must assign various access roles to end users who might have access to resources at an application service site. PAP provides role definition and assignment services for authorized security administrators. Before an end-user may be allocated a role, they must have a valid IDMS registration entry.

PAP and IDMS work together to manage how end-user attributes, like as roles, are stored and retrieved from a single repository. The security administrator simultaneously defines the role-based policy. It explains the result of authorization depending on a mix of role, action, and resource. Consequently, the decision service is housed within a single security system(Canedo, 2022, [3]).

iv. *Compliance Management:* Access and identity management (IAM) in the cloud is a set of techniques and an architecture that are closely related to how well business operations are supported by IT. IAM techniques and processes, when properly implemented, can greatly enhance the effectiveness of a conceptual framework's compliance controls. For instance, by fully automating the procedure of providing and cancelling access credentials, organizations can reduce the possibility of unauthorized access(Mohammed, 2021, [6]). The IAM's internal processes and practices not only give you a bird's eye perspective of the business, but they also provide an automated processing aspect that can fend off outside threats. Due to the cloud service providers' present low and superficial adoption of the SAML, SPML, and XACML standards, each provider's compliance should be individually verified using parametric methodologies, depending on the particular scenario under analysis.

VII. CONCLUSION AND FUTURE SCOPE

According to what the author has claimed, widespread adoption of cloud computing has not yet occurred due to difficulties with access and identity management. When it comes to identity and access management, it is important for a company to protect any proprietary or confidential information that it stores. If this information were compromised, it could have an impact on the relationships that the company has with other businesses as well as the productivity of its employees. Even while the necessary technological infrastructure is already in place, just relocating these systems to an environment that is supported by cloud-based services may not immediately result in the benefits in efficiency, responsiveness, and adaptability that are required. The massive volumes of dynamic processing resources accessible in the cloud, along with the high numbers of users that will be consuming those resources, will test the scalability and automation of access and identity management. The fact that the organization already has IAM solutions in place is going to make things even more complicated. Due to the complexity and standardization requirements of the architecture, moving the IAM architecture of an organization to the cloud would be a process that would take a long time and be expensive. Cloud-based identity information sources can't be relied upon, and the implementation of Identity and Access Management (IAM) standards by cloud service providers is haphazard and frequently doesn't match an organization's own quality benchmarks. Both of these factors contribute to the emergence of problems. The same cannot be said for the PaaS or IaaS tiers, despite the fact that an increasing number of SaaS providers are integrating SAML support.

According to the findings, just a small fraction of cloud service providers are starting to account for organizational needs in IAM. In order to implement federated identity management solutions, SAML and SSO support is required. The Cloud EAM capabilities are still at a rudimentary level, despite the fact that almost all of these providers are incredibly large organizations (such as Microsoft, Google, or Sales force). The author believes that the adoption of fundamental standards such as SPML, SAML and XACML, along with an API-type interface that streamlines automated access and identity management processes, will accelerate due to demand from cloud service providers. There are also technological and psychological barriers that hinder businesses from readily consenting to store identity management data sources in a location outside of their boundaries. The need for unshakeable control over one's own data as well as total trust in the cloud services provider are obstacles to cloud computing's mainstream adoption. The problem is made worse by the fact that many use cases require duplicating data sets or keeping a copy of the client organization's data sets in the cloud. This makes solving the issue even more difficult. Even the largest businesses still struggle with keeping all of their identity and access management services in sync, although this may become less of a challenge as more universal standards are adopted. The author argues that before a business ever contemplates migrating to the cloud, it must incorporate an IAM strategy into its overall plan to adapt to the new paradigm in order to minimize unpleasant and expensive shocks. It is common practice to recommend the usage of Identity-as-a-Service (IaaS) solutions to businesses that have inadequate IAMs and have a need to interface with a large number of partners or a desire to participate in a number of different federated identity schemes. Long-term cost savings for businesses can be achieved by developing an IAM strategy and contemporary architecture prior to attempting cloud extension via common protocols like SPML, SAML and XACML. The company may save money as a result of this.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics (Switzerland)*, *11*(1), 1–34. https://doi.org/10.3390/electronics11010016
2. Andi, H. K. (2021). Analysis of Serverless Computing Techniques in Cloud Software Framework. *Journal of ISMAC*, *3*(3), 221–234.

https://doi.org/10.36548/jismac.2021.3.004
3. de Almeida, M. G., & Canedo, E. D. (2022). Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. *Applied Sciences (Switzerland)*, *12*(6). https://doi.org/10.3390/app12063023
4. Editors, L., Yasuda, K., Lodderstedt, T., Nakamura, K., & Vercammen, J. (2022). *OpenID for Verifiable Credentials*. https://doi.org/10.1145/3442381.3450085
5. Liu, G., Gao, X., & Wang, H. (2021). An investigation of identity-account inconsistency in single sign-on. *The Web Conference 2021 - Proceedings of the World Wide Web Conference, WWW 2021*, *April 2021*, 105–117. https://doi.org/10.1145/3442381.3450085
6. Mohammed, I. A. (2021). *Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled*. *August*. www.ijcrt.org
7. Partida, A., Criado, R., & Romance, M. (2021). Identity and access management resilience against intentional risk for blockchain-based IOT platforms. *Electronics (Switzerland)*, *10*(4), 1–26. https://doi.org/10.3390/electronics10040378
8. Programme, D., Electrical, I. N., & Engineering, A. (2022). *Regulations in Identity and Access Management*.
9. Shankar, T. N., Rakesh, P., Bhargawa Rao, T., Hari Bharadwaj, L., Rakesh, C., & Lakshmi Madhuri, M. (2021). Providing security to land record with the computation of iris, blockchain, and one time password. *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021*, 226–231. https://doi.org/10.1109/ICCCIS51004.2021.9397176
10. Slamet, C., Syaripudin, U., Kaffah, F. M., & Tiasto, B. E. (2021). Implementation of Rivest Cypher 4 algorithm in Security Assertion Mark-up Language protocols on Single Sign-On services. *IOP Conference Series: Materials Science and Engineering*, *1098*(3), 032109. https://doi.org/10.1088/1757-899X/1098/3/032109
11. Wu, L., Cai, H. J., & Li, H. (2021). SGX-UAM: A secure unified access management scheme with one time passwords via intel SGX. *IEEE Access*, *9*(March 2012), 38029–38042. https://doi.org/10.1109/ACCESS.2021.3063770
12. Almulla, S. A., & Yeun, C. Y. (2010). Cloud computing security management. In *2010 Second International Conference on Engineering System Management and Applications* (pp. 1-7). IEEE.
13. Mukundrao, J.A. and Vikram, G.P., 2011. Enhancing security in cloud computing. In *Information and Knowledge Management* (Vol. 1, No. 1, pp. 40-44).
14. Zahoor, E., Asma, Z. and Perrin, O., 2017. A formal approach for the verification of AWS IAM access control policies. In *Service-Oriented and Cloud Computing: 6th IFIP WG 2.14 European Conference, ESOCC 2017, Oslo, Norway, September 27-29, 2017, Proceedings 6* (pp. 59-74). Springer International Publishing. https://doi.org/10.1007/978-3-319-67262-5_5
15. Goyal, Ms. P., & Deora, Dr. S. S. (2022). Reliability of Trust Management Systems in Cloud Computing. In Indian Journal of Cryptography and Network Security (Vol. 2, Issue 1, pp. 1–5). https://doi.org/10.54105/ijcns.C1417.051322
16. Karthiga, S., & Velmurugan, Dr. T. (2020). Enhancing Security in Cloud Computing using Playfair and Ceasar Cipher in Substitution Techniques. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 4, pp. 912–920). https://doi.org/10.35940/ijitee.D1363.029420
17. Mishra, J. P., Panda, S. R., Mishra, S. K., & Pati, B. (2019). A Novel Observation on Cloud Computing in Education. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 3, pp. 5262–5274). https://doi.org/10.35940/ijitee.D1363.029420
18. Radhamani, V., & Dalin, G. (2019). Significance of Artificial Intelligence and Machine Learning Techniques in Smart Cloud Computing: A Review. In International Journal of Soft Computing and Engineering (Vol. 9, Issue 3, pp. 1–7). https://doi.org/10.35940/ijsce.c3265.099319
19. Kumar, Y. K., & Shafi, Dr. R. M. (2019). Key Enforced Access Control and Performance Analysis of DES and RSA Cryptography in Cloud Computing. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 1, pp. 7220–7225). https://doi.org/10.35940/ijeat.A9995.109119

AUTHOR'S PROFILE

Dr. Anil Kumar is working as an Assistant Professor in Department of Computer Science and Engineering at RIT, Roorkee Uttarakhand, India. He is having more than 18 years of academic experience and worked with various reputed engineering institutions. He has completed his B.Tech in IT from AKTU (formely UPTU), M.Tech in Computer Science and Engineering and Ph.D. in Computer Science and Engineering. He had reviewed several journals articles too. He is having distinguished record of research papers with more than 15+ International, Scopus and SCI papers. He is also in his bucket as a researcher with research area of Artificial Intelligence, Machine Learning, Image Processing and Computer Network.

Dr Abhay Bhatia is working as Assistant Professor in Department of Computer Science and Engineering at Roorkee Institute of Technology, Roorkee, Haridwar Uttarakhand. He is having 12+ years of academic experience and worked with various reputed engineering institutions. He has completed his B. Tech in Computer Science and Engineering from AKTU (formely UPTU), M.Tech in Computer Science and Engineering from Rajasthan and Ph.D. in Wireless Sensor Networks. He is currently an active member of IEEE as well as a reviewer for several journals too. He is having distinguished record of research papers with 17+ Indexed, Scopus, IEEE and SCI papers. He also visited many institutes for guest lecture on various upcoming researches. Moreover 4 patents with 5 book chapters are also in his bucket, he is also author to a book on IoT, as a researcher with research area of Artificial Intelligence, Machine Learning, Image Processing and Wireless Sensor Network his work is up heading to great research.

Dr. Anju Mishra has received her Ph.D. in Computer Science & Engineering from Amity University Uttar Pradesh Noida. Her research interests lie in the areas of Computer Vision and Image Processing, Machine Learning and deep learning, Healthcare systems, and Biomedical signal processing. She has worked with institutions of repute and has the research and academic experience of about 16 years. She is currently working as an Associate Professor in the Department of Information Technology, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh. She has published more than 30+ research papers in reputed international journals and conferences. She has been a reviewer for many international journals and conferences of repute and guided the B. Tech and M. Tech students.

Ms. Tanu Gupta is an Assistant Professor in the Department of Information Technology, Ajay Kumar Garg Engineering College Ghaziabad, Abdul Kalam Technical University in Lucknow, India and M.Tech. in Computer Science and Engineering. She is having many research papers with more than 10+International, Scopus and SCI papers. She is also in her bucket as a researcher with research area of Artificial Intelligence, Machine Learning, Cyber Security Data Mining and Computer Network.