JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Novel Approach to find IAM Functionality in Cloud Computing

[1]Dr.Mahesh V, [2] Mr. Amarnath J L, [3] Mr. Jayaprakash B

[1,2,3] Assistant Professor,
School of Computer Science and IT, Bengaluru, Karnataka, India
E-mail: {v.mahesh, jl.amarnath, b.jayaprakash}@ jainuniversity.ac.in

Abstract : In cloud frameworks, user identity authentication is a major issue. There is a direct risk of delicate information loss and serious data exposure if design flaws in a cloud user identity authentication system are not addressed. Today's cloud user identity management solution has a basic flaw is that it is excessively reliant on third-party services. The goal of this research is to design, deployment, and integration of an identity management framework into Cloud Computing.

IndexTerms - **Identity as a service (IDaaS), Lightweight Directory Access Protocol (LDAP), Platform-as-a-Service(PaaS), Identity and Access Management(IAM), Amazon Quantum Ledger Database (QLDB), Virtual Private Cloud (VPC)**

I. INTRODUCTION

Through the advancement of the web technology, there are an increasing number of applications available to make our lives easier. People nowadays utilize a wide range of mobile phone apps, and utilizing an app necessitates creating an account and creating a password. As a result of these phenomena, users are required to remember a large number of passwords and accounts. Despite the fact that there are numerous internet-based mechanisms for remembering passwords, such as cookies, their security has been measured. Numerous prominent Internet firms have introduced apps in recent years that allow users to register for the application by an account provided through additional facility supplier. This phenomenon is accompanied with an identity management system.

Identity management is a concept that combines policy, engineering and programming to allow approved resources to precisely determine users' identities and govern the flow of information between them. [1]. To determine whether to approve the user to use the service, the identity management system uses an personality identifier to denote the individuality, which recognizes a facility supplier. In order to accomplish a customer's individual info, identity management typically employs one of three methods: The first is data of both the users and the service providers are aware as a passwords, the second one is that the info that both the user and identity management are aware of, and the third is that the both of the user and identity managements are aware of. The third category is for user identity qualities that may be validated, such as fingerprints, iris, and so on [2].

The sensitivity of data and the privacy of information has been a growing source of concern for businesses. The usage, maintenance, and security of Personally Identifiable Information (PII) gathered from all users which are part of the identity validation and authentication parts of identity management. An important task is to stopping unwelcomed logins to cloud-based data possessions or resources. One tireless issue is that an association's distinguishing proof and validation frameworks probably won't collaborate to the public cloud, making it challenging to expand or adjust the current cloud to help cloud offices. In the cloud biological system, confirmation and access control have difficulties with personality and access the executives.

Cloud computing advancements and the development of various cloud provisioning prototypes, like Software as a Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), had a significant impact on Information Technology in recent years. Cloud computing enables multiple tenants to share a pool of resources, resulting in faster development times, lower capital outlay, and usage-based maintenance. Existing cloud computing models, on the other hand, do not support virtualized network resource provisioning, which causes network dependability and reliability issues for both the cloud user and the cloud provider [3].

Because the cloud provider is responsible for managing user IDs, cloud ecosystems do not allow for cloud provider regulated access. If a user's credentials are shared among numerous cloud providers, a hostile cloud provider can misappropriate information using the user's identity credentials. As a result, employing a well-defined cloud-provider independent identity management system to safeguard and manage user identity information is critical. The fundamental support of this study is to design, deployment, and integration of an identity management framework into Cloud Computing.

II. LITERATURE SURVEY

The key objective of any associated identity management device is to guarantee that subscribing users are verified according to the regulations of various cloud servers and that sensitive data is safeguarded from unauthorized access. To recommend and develop related identity management models, a wide range of techniques, procedures, and organizational proficiencies are employed, and every device will have its specific attributes, approaches, and functions. Due to the nature of cloud-based services that function in shared open settings, the requirement for these identity management methods is especially clear for cloud suppliers and clients. As a result, various studies and researches have been undertaken in order to increase cloud identity management's dependability and effectiveness.[4].

Verification of qualified customer credentials with security, data breaks and shared technological vulnerabilities are just a few of the issues that cloud web services face. As businesses hand over security control to third-party suppliers, the number of roles and number of stakeholders change significantly [6].

Identity as a Service refers to the administration of user distinctiveness in the cloud by third-party providers (IDaaS). Challenges such as identity data localization, secrecy, trust establishment, and availability develop as a result of non-organizational IDaaS providers' engagement in identity management. The identity provider is in charge of enabling the security system for cloud apps. The identity management method is used to manage users, protect customer right of entry, authenticate login username and pasword, and guarantee that only the appropriate persons have admittance to the possessions of the services in cloud. To authenticate users, passwords, biometrics, tokens, and certificates are utilized [7].

In most businesses, the risk, cost, and effort associated with controlling identity increases in lockstep with the company's growth. Each company requires a distinct stong identity management system for accurate identity management. This reduces the risk of identity management, along with the cost and time it takes to encounter the identification and admittance needs of the company's personnel. An organization's well-established identity management system includes a wide range of functions and benefits [5].

The access control cloud is made to see if the correct individual is getting access to the right resources in accordance by means of preset policies. The major objective of this strategy is to making resource safety and confidentiality more convenient. The net is protected in contrast to unlawful admittance once the admittance control device is employed effectively. For access management, a wide range of models and technologies are available. The same cloud is utilized by multiple organizations with various policies in a cloud environment, which increases the danger of unauthorized people accessing resources. Compulsory admittance regulator, discretionary access control (DAC) model, role based access control mode, and risk based access control model are some of the access control approaches employed in cloud for IAM. The access management system collaborates with the identity management system to control customer admittance to applications. The advantages and benefits of a deep-rooted access management system for a business are numerous [8].

For the full life of those assets in the business, Identity and Access Management (IAM) is a continuous process that necessitates frequent updates for all critical applications, user attributes, cloud applications, and more. To prevent unauthorized access, it can also entail managing privileged accounts, defining role-based access control, and access review. Traditionally, identity governance has been a combination of technology and business processes used to generate and manage access levels in order to reduce security risks and boost user productivity with company resources. Identity Governance and Administration of all lifecycles can be accomplished with a single software solution with modern IAM systems..

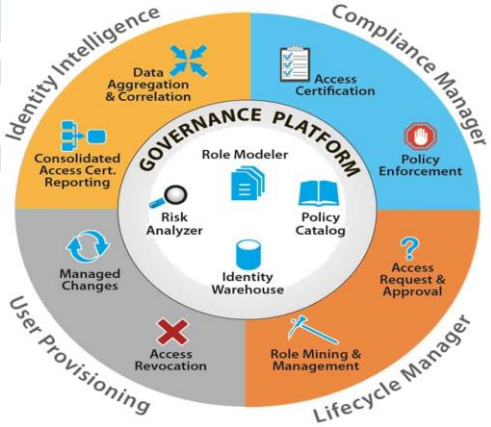

Figure 1: IAM User Lifecycle Management
(Source: https://sath.com on 15th Feb 2022)

The principle of least privilege, or the minimum access should govern onboarding new employees and machine identities to carry out their job functions. Humans and machines are the two main players in every network. Login credentials are used by humans to identify themselves. Machines are able to identify and authenticate themselves by utilizing certificates and keys.

By automating regular procedures and providing end-users with a seamless experience, IAM solutions should save the time spent onboarding and offboarding users, managing job role changes, and ensuring every digital identity is accounted for. An ideal solution should provision, make mid-lifecycle changes to, and deprovision accounts for users, or listen for these activities from existing HR systems.

- The following list depicts the entire Identity Lifecycle process:
- New user enters the organization
- Digital identity created
- Single Sign On multifactor Authentication process is setup.
- User is assigned a Role in the organization
- Accounts are created for the systems and Applications the user will need access to

- Access is Certified to applications periodically
- User Requests Access to resources when needed
- User's Role changes in the organization
- New application accounts are created and Provisioned
- Discontinued applications are deprovisioned, through Reconciliation
- User leaves organization
- User access is removed to all accounts

III. GLITCHES WITH EXISTING IAM FUNCTIONALITY

Identity Management and Access Management are the two components of IAM. Identity provisioning and de-provisioning are the most important aspects of identity management. Access management encompasses verification, approval, and policy administration. IAM is in control of deciding who takes admittance to whatever resources and at what time they have access. IAM also manages the consumer identity phase, It consists of design, preservation, bringing up to date, and removal of customer authorizations. Identity and access management delivers the below explained facilities [6]:

a. Authentication facilities: The important question is involved in authentication. What's your name? The procedure of confirming a customer's credentials in order to obtain entry to constrained possessions is known as authentication. User names and passwords are being used for authentication from many years to till now, but current IAM now demands multi-factor authentication. To authenticate a user, resilient authentication practices more than one factor, such as a fingerprint or an OTP. At the time of each transaction completing, risk based authentication examines the risk of trusting the requesting agent by taking into account geographic location, history, behavioral, and other characteristics. Depending on the risk level, transactions may be approved or rejected (low or high).

b. Authorization Administration facilities: It provides an answer to the question of what a user can do. Merely the facilities and resources a user is entitled are accessible to him, thanks to authorization regulations. Consumers will be given a predefined set of rights established on the role that they have been assigned by the organization. Appropriate policies should be put in place, and admittance would be granted or refused based on those guidelines.

c. Identity Supervision: Identity is the procedure of generating a user digital ID or account that allows consumers admittance to cloud resources. Whenever the new employee starts working for a firm, he is granted a digital identity which permits the admission of the enterprise's source and fulfil the responsibilities assigned. The user account is de-provisioned whenever the employee leaves the enterprise or moves to some other department. For this purpose services called Active Directory and LDAP are used.

d. Federated Identity: Associated Identity Management creates trust among several apps or administrations using a third-party source. The federation server of the identity supplier saves consumer data and credentials, permitting one shot sign-on without passwords. When the consumer attempts to log in for particular service, an identity supplier offers a token using common identity conventions like SAML, OAuth, and others, rather than providing credentials. The service provider accepts this token since it beliefs the identity supplier and the certified consumer. SSO removes the essential to remember multiple IDs and passwords aimed at numerous apps.

e. Compliance management: Menace supervision for audits needs adequate observing and recording. It is a method of analyzing and inspecting approval and verification records to verify if they fulfill with established safety ethics and procedures. Real admittance procedure execution necessitates obedience observing, inspecting, and recording.

IV. EXPERIMENTAL RESULTS

This section goes through the advantages of Amazon VPC endpoints and links to a self-paced session where you may learn more. You can launch Amazon Web Services (AWS) resources inside using the Amazon Virtual Private Cloud to create a defined virtual. This virtual network has the appearance and behavior of a regular network in your data centre. Another benefit is the ability to take advantage of AWS's scalable architecture.

A VPC endpoint permits user to securely link his/her VPC to AWS services. Installation of internet gateway, Network address translation (NAT) device, VPN connection, or AWS Straight Join association is not required. Virtual gadgets that are horizontally scaled, redundant and extremely existing VPC components are called endpoints. VPC endpoints allow instances and services in VPC to communicate without placing user network traffic at risk of outages or capacity limits.

By reducing traffic to internet gateways and saving money on NAT gateways, NAT instances, and firewall maintenance, we can reduce the network path. You also have a lot more control over how users and apps interact with AWS services with VPC endpoints. VPC endpoints are divided into three categories: Gateway load balancer endpoints and Interface endpoints. Let's have a look at the various types of endpoints and their applications.

For example, the gateway load balancer endpoint is capable of allowing the interception of traffic and routing into a network or security service that you have setup using the GLB. The virtual applications such as firewalls, intrusion recognition systems, and most deep packet assessment systems can all be deployed, scaled, and operated using gateway load balancers. Justin Davies, one of our employees, has created a fantastic blog article describing the architectural patterns that AWS Gateway Load Balancers support.

A Gateway endpoint, on the other hand, lets user to grant access to Amazon S3 and Amazon DynamoDB to others. Mentioning both the gateway endpoint and the Amazon Web Services resource to which the endpoint allows access can have resource policies specified. An AWS Identity and Access Management resource policy that can connect to a Virtual Private Cloud endpoint is called a Virtual Private Cloud endpoint policy. It's a distinct policy to bound endpoint accessing certain service. Within a VPC, this allows for granular access control and private network connectivity. Generate a strategy that is used to limit access into a specific Amazon DynamoDB table, for example. This strategy would use a Virtual Private Cloud endpoint to restrict table accessing into only certain users or groups.

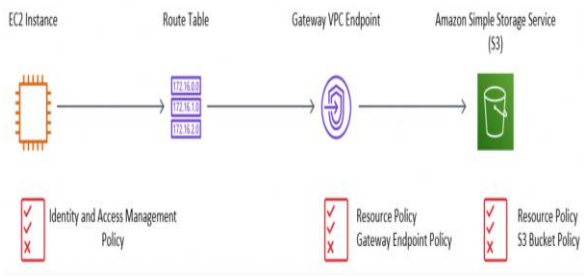

Figure 2: Using a Gateway VPC endpoint to access Amazon S3.

The Interface endpoint is a third specific variety of endpoint, and it allows user to connect to AWS PrivateLink-based services. A huge number of AWS services are included in this. Other AWS customers and AWS Partner Network (APN) partners can also include services housed in their own VPCs. User no longer need to rely on a public internet connection when utilizing Amazon Web Services PrivateLink is given to access Amazon Web Services partner services. The cost of sending data from Amazon EC2 to the internet varies depending on the amount of traffic. Transfers at AWS US-East 1 Virginia are taxed at $ 0.09/GB beyond the first 1 GB per month ($0.00 per GB). Interface endpoints, like gateway endpoints, can be secured by imposing resource constraints on both the endpoint and the resource it accesses. Security groups can be used with interface endpoints to limit access to the endpoint.

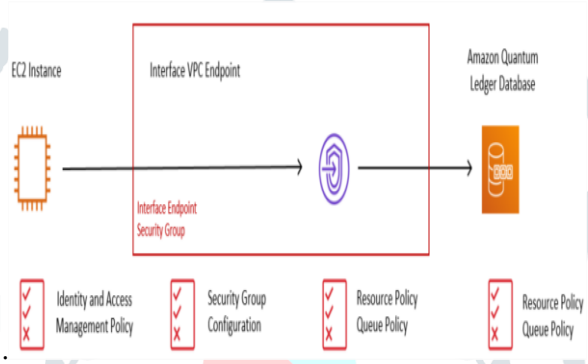

Figure 3: An Interface VPC endpoint to access QLDB

V. CONCLUSION

The paper aims a novel approach to find IAM functionality in cloud computing. The Literature survey names the different types of references used for reaching the novelty of the approach. The glitches in the IAM functionality give the description of the IAM and its functionality. The experimental and results section gives the experimental results of the two different types of scenarios in AWS. The experimental results page gives the demonstration of various results for the AWS and IAM used in AWS. This paper gives all the readers a conclusion to find the novel approach to find IAM functionality in cloud computing.

REFERENCE

[1]. S. Wang, R. Pei and Y. Zhang, "EIDM: A Ethereum-Based Cloud User Identity Management Protocol," in IEEE Access, vol. 7, pp. 115281-115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[2]. P. Angin,B. Bhargava and R. Ranchal el at., “An entity-centric approach for privacy and identity management in cloud computing” IEEE symposium on reliable distributed systems. IEEE, 2010, pp. 177–183.

[3]. R. D. Dhungana, A. Mohammad, A. Sharma and I. Schoen, "Identity management framework for cloud networking infrastructure," 2013 9th International Conference on Innovations in Information Technology (IIT), 2013, pp. 13-17, doi: 10.1109/Innovations.2013.6544386.

[4]. F. F. Moghaddam, P. Wieder and R. Yahyapour, "A policy-based identity management schema for managing accesses in clouds," 2017 8th International Conference on the Network of the Future (NOF), 2017, pp. 91-98, doi: 10.1109/NOF.2017.8251226.

[5]. I. Indu and P. M. Rubesh Anand, "Identity and access management for cloud web services," 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), 2015, pp. 406-410, doi: 10.1109/RAICS.2015.7488450.

[6]. A. Sharma, S. Sharma and M. Dave, "Identity and access management- a comprehensive study," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1481-1485, doi: 10.1109/ICGCIoT.2015.7380701.

[7]. A. Singh and K. Chatterjee, "Identity Management in Cloud Computing through Claim-Based Solution," 2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2015, pp. 524-529, doi: 10.1109/ACCT.2015.89.

[8]. N. Naik and P. Jenkins, "A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards," 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2016, pp. 89-90, doi: 10.1109/MobileCloud.2016.22.

[9]. Y. Yang, X. Chen, G. Wang and L. Cao, "An Identity and Access Management Architecture in Cloud," 2014 Seventh International Symposium on Computational Intelligence and Design, 2014, pp. 200-203, doi: 10.1109/ISCID.2014.221.

[10]. S. Neela, Y. Neyyala, V. Pendem, K. Peryala and V. V. Kumar, "Cloud Computing Based Learning Web Application Through Amazon Web Services," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 472-475, doi: 10.1109/ICACCS51430.2021.9441974.