CHALLENGES OF IMPLEMENTING CLOUD SECURITY SYSTEM THROUGH IDENTITY, ACCESS & RISK MANAGEMENT [IARM] IN A HYBRID IT ENVIRONMENT

Sai Siddhartha Chary Aylapuram
IV B.Tech., 7th Semester, CSE (Cloud Technology & Information Technology), Sir Padampat Singhania University, Bhatewar, Rajasthan-313601, India,
siddharthaylapuram@gmail.com

Abstract: The majority of promises of cloud security -- improved IT efficiency, flexibility and scalability -- come with one major challenge: security. As enterprise IT adopts more cloud systems while keeping on-premium solutions, controlling who is granted access to which applications becomes increasingly important. This presents CIOs and their teams with a whole new set of identity management challenges. In addition, users must keep track of multiple URLs, user names, and passwords to get access to their applications from the ground to the cloud. Its role is also fundamentally changing. The spread of IT resources in the public sector has been associated with a sharp increase in the level of intra-organizational and inter-organizational communications. Strengthening security can create friction for your employees and consumers. To implement identity management, an enterprise must be able to plan and collaborate across business units. Identity management works best when IT, security, HR, and other departments are involved. Identity management systems must enable companies to automatically manage multiple users in different situations and computing environments in real time. There are challenges in security as a part of Identity, Access & Risk to Verify Trust helps to protect against malicious actors while balancing Multi-Factor Authentication (MFA) requirements.

Keywords: Cloud Security, Risk, Identity, Access, Hybrid Environment, Access and Risk.

1. Introducing Risk In Information Security And Management

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This exercise involves certain amount of risk. Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. If confidential information about a business' customers or finances or new product line fall into the hands of a competitor, then a breach of security could happen and may lead to loss of business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For individuals, information security has a significant effect on privacy, which is viewed very differently in different cultures [1]. For a government, information security means maintaining the law and order among the public, safeguarding the lives of its people, thwarting enemy attack on its installations, and so on and so forth.

1.1 **The Importance of Digital Identity Risks: Few of the important identity risks are mentioned below**

1. User Password Fatigue
2. Failure-Prone Manual Provisioning and Deprovisioning Process
3. Compliance Visibility: Who Has Access to What?
4. User Directories for Each Application
5. Managing Access for Remote Work
6. Keeping Application Integrations Up to Date
7. Different Administration Models for Different Applications
8. Sub-Optimal Utilization, and Lac of Insight into Best Practices
9. Provide Consistent Access to On-Premium and Cloud Applications

1.2 Components of Identity Access Management Service

An IAM service can be split into four main components. An IAM system can also be used to deploy single sign-on (SSO) technologies. This can significantly decrease the number of passwords users need. SSO incorporates a federated-identity approach by using a single login and password to create an authentication token, which can then be accepted by various enterprise systems and applications [2].

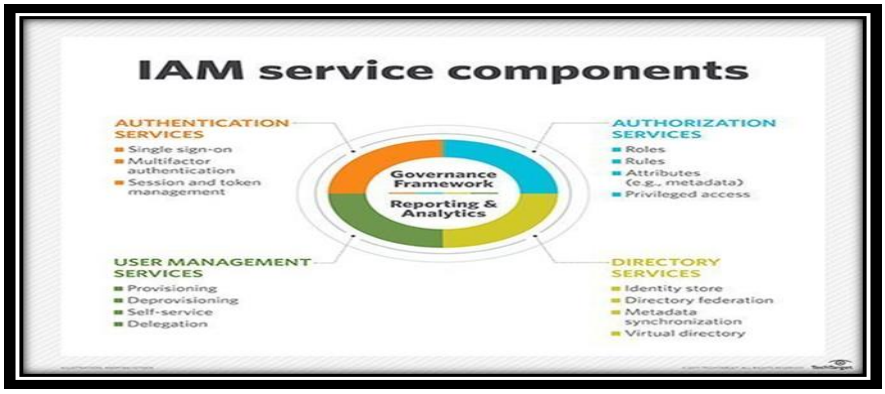

Fig. 1.1 IAM Service Components

Combined with multifactor authentication and enforceable security policies, enterprises can lower the risk of security breaches. An example of such policies includes the principle of least privilege, which gives users only the access they require to fulfill their roles [3].

1.3 Federated Identify Management

Federated identity management (FIM) is an arrangement between multiple enterprises or domains that enables their users to use the same identification data (digital identity) to access all their networks. These partners are also known as trust domains. A trust domain can be an organization, a business unit, a smaller subsidiary of a larger organization, etc [4, 5]. FIM is a system of a single login, and multiple access. For FIM to work effectively, all involved partners must have a sense of mutual trust. Each trust domain maintains its own identity management. However, all domains are interlinked through a third-party service that stores users' access credentials and provides the trust mechanism needed for FIM to work. This third service is known as the identity provider or identity broker [6].

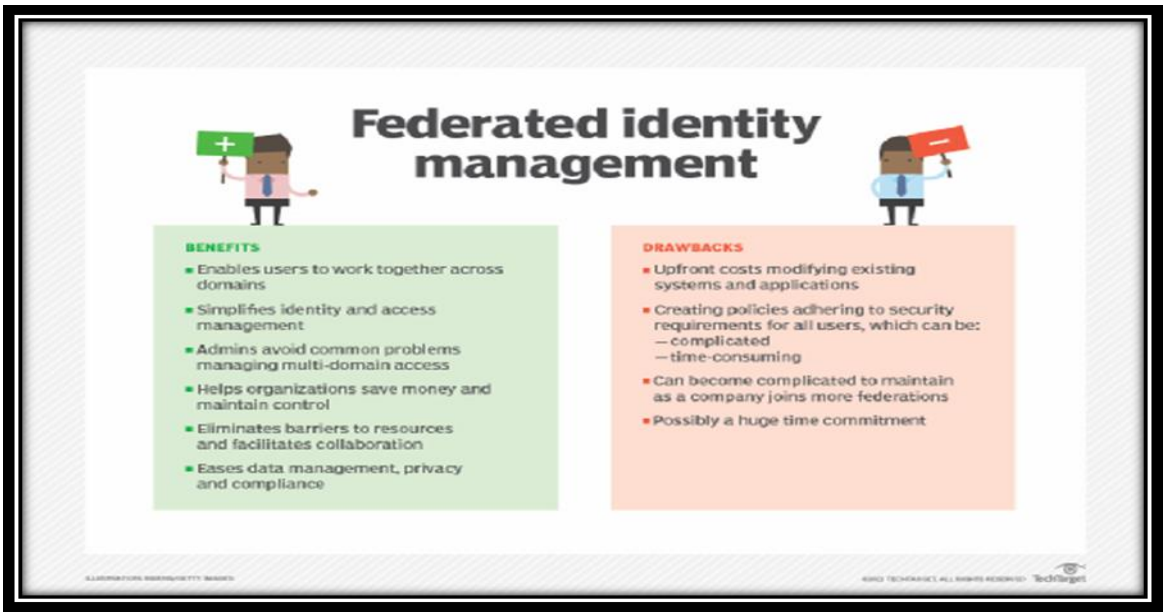

Fig. 1.2 Federated identity management

1.4. Challenges of implementing identity management

To implement identity management, an enterprise must be able to plan and collaborate across business units. Successful organizations will be those that establish identity management strategies with clear objectives, defined business processes and buy-in from stakeholders at the outset. Identity management works best when IT, security, HR and other departments are involved [8]. Identity management systems must enable companies to automatically manage multiple users in different situations and computing environments in real time. It's time-consuming to manually adjust access privileges and access controls for hundreds or thousands of users. Authentication must also be simple for users to perform and easy for IT to deploy and secure [9].

One of the top challenges in implementing identity management is password management. IT professionals should invest in techniques that can reduce the impact of password issues in their companies. Identity management tools should run as applications on a dedicated network appliance or server. At the core of an identity management system are policies defining which devices and users are allowed on the network and what a user can accomplish, depending on device type, location and other factors [10]. Management console functionality is key. It should include policy definition, reporting, alerts, alarms and other common management and operations requirements. An alert might be triggered, for example, when a specific user tries to access a resource to which they do not have permission. Reporting produces an audit log documenting what specific activities were initiated [11]. Many identity management systems offer directory integration, support for wired and wireless users and the flexibility to meet almost any security and operational policy requirement.

2 Literature Review

The specification of security requirements in a discrete and unambiguous form is the main concern of the software security requirements. There are various security specification languages such as UMLsec [Jürjens, 2014], secure UML [Lodderstedt et al., 2020], Secure Tropos [Firesmith, 2018], Misuse Case [Sindre et al., 2019] Abuse Case [McDermott et al., 2018], UMl

intr [Hussein et al., 2018] and Asml Sec [Raihan et al., 2017]. A number of open source tools are also available to recover the deleted emails [Rachid et al., 2017]. Most of the tools are meant for casual users and therefore, cannot be used by authorities for any legal purpose. Such tools are not considered as weapon in the arsenal of Computer Forensic [12].

There are several forensic tools that are commercially available for performing various forensic procedures. A number of open source tools are also available to recover the deleted data [Open Source Forensic, 2021]. Security is the furthermost prioritized aspect for any form of computing, creating it a clear prospect that security concerns are important for a cloud environment as well. As the cloud computing method might be related through possession of users‘ sensitive information stowed both at clients‘ end in addition to in cloud servers, identity management and verification are essential in cloud computing (Kim et al.(2016), Emam et al. (2016), Yassin et al. (2017), han et al. (2018)) Authentication of qualified users‘ credentials and guarding such credentials are part of primary security concerns in the cloud - violation in these parts might lead to undetected security breach as a minimum to a certain range for a particular period. A probable authentication scenario for cloud infrastructure is exemplified [13].

Strong user authentication mechanisms limiting illegitimate access are the first demand for securing cloud. Few authentication mechanisms are biometrics, OTP & passwords. Passwords can be unsafe if either too simple or too complex in their own ways (Ignacio et al. 2017). The other authentication means Biometrics comes with three big problems: Unlike passwords, biometric data cannot be stored as a hash. In case biometric data is ever compromised, there is no resetting like a password. Biometric systems are extremely susceptible to spoofing. A one-time-password (OTP) is based on a cryptographic algorithm, code that changes after every use, can only be used. Combining the two (two-factor authentication) provides greater security than any one [14].

3. Methodology of Application Provider & Application Architecture

The major contributions of the paper are summarized as follows: - Comparative analysis of different aspects in identity and access management mechanisms in cloud environment. - Overview of access governance policies which are least explored area in identity and access governance. - Overview of market leading identity and access control suite of products and solutions. - Overview of common security threats in Cloud IAM systems and prevention techniques. - Recommendations on governance policies and industry best practices [15].

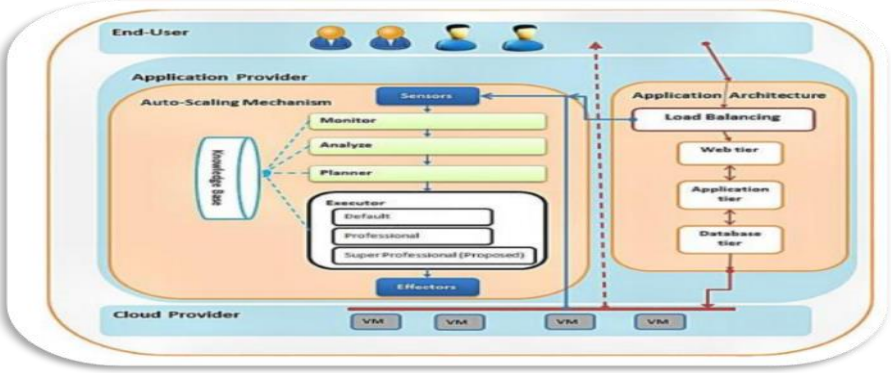

Fig. 3.1. Application Provider & Application Architecture

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, policies control who can create users, create and manage a VCN (Virtual Cloud Network), launch instances, and create buckets. For specific details about writing policies for this service. The individual resource types for Security Zones are included in the aggregate type cloud-guard family. For specific details about writing policies for other services [17].

3.1 Security for Core Services

Learn about key security features in the core Oracle Cloud Infrastructure services. Oracle Cloud Infrastructure Compute lets you provision and manages to compute hosts, known as **instances**. You can launch instances as needed to meet your computing and application requirements. After you launch an instance, you can access it securely from your computer, restart it, attach and detach **volumes**, and terminate it when you're done with it. Any changes made to the instance's local drives are lost when you terminate it. Any saved changes to volumes attached to the instance are retained [18].

Oracle Linux images hardened with the latest security updates are available for you to run on Oracle Cloud Infrastructure instances. Oracle Linux images run the Unbreakable Enterprise Kernel (UEK) and support advanced security features such as splice to apply security patches without rebooting. In addition to Oracle Linux, Oracle Cloud Infrastructure makes available a list of other OS platform images, including CentOS, Ubuntu, and Windows Server. All platform images come with secure defaults including OS-level firewalls turned on by default.

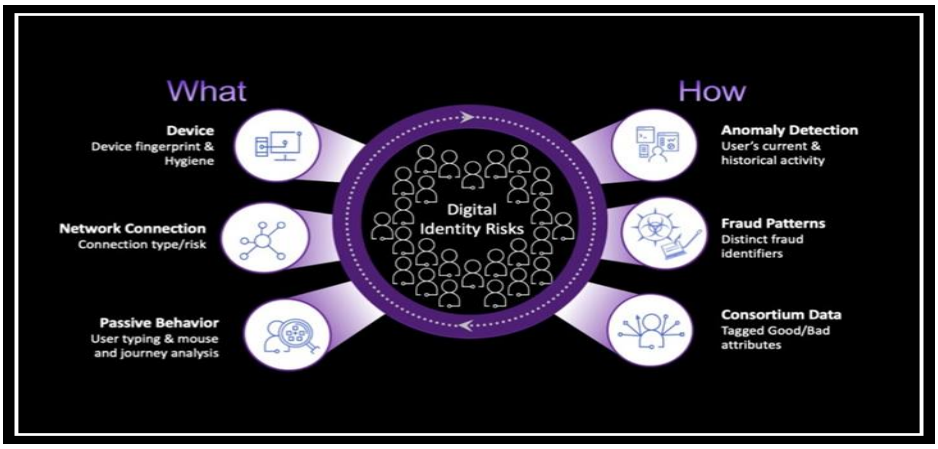

Fig. 3.2 What & How to provide security with authenticity

3.2 Oracle Cloud Infrastructure offers both bare metal and virtual machine instances:

Bare Metal A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation. After a customer terminates their bare metal instance, the server undergoes an automated disk and firmware-level wipe process to ensure isolation between customers.

Virtual Machine A virtual machine (VM) is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are ideal for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine. An Oracle Cloud Infrastructure VM compute instance runs on the same hardware as a bare metal instance, using the same cloud-optimized hardware, firmware, software stack, and networking infrastructure. All Oracle Cloud Infrastructure instances use key-based Secure Shell (SSH) by default. Customers provide the SSH public keys to Oracle Cloud Infrastructure and use the SSH private keys for accessing the instances. Oracle recommends using key-based SSH to access Oracle Cloud Infrastructure instances. Password-based SSH could be susceptible to brute-forcing attacks, and is not recommended.

4. Results & Agreeable Cases:

Risk management in information security means understanding and responding to factors or possible events that will harm confidentiality, integrity and availability of an information system. The very first step that should be included in any risk management approach is to identify all assets that in any way are related to information. These assets can be different applications or can be servers, networks routers, switches, back-up disks and systems, laptops, computer desktops, mobile phones, or different devices which are used to process, transmit and maintain information. Asset can be a document, a research results, and basically anything that has a value for the company. Sometimes, information security itself is considered asset. The second step includes identification of threats toward identified assets. Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization. Threats can be a theft, virus, disclosure of important data, floods, infrastructure or software failure, hackers, etc. As a third step is to identify vulnerabilities. These vulnerabilities can include a wide range of cases: no data backup, no encryption, weak passwords, no remote wipe, no surge protection, no training, no access management, no firewalls, no business continuity plans, etc.

Security/Availability	Answer	Score
Continuity planning: Our continuity and performance planning makes clear distinctions on critical systems and data with availability (uptime) and Restore Time Objectives (RTOs) for different services. (An RTO is the target time you set for the recovery of your IT and business activities after a disaster has struck.)	Agree	Green
Security management: We have mature and auditable security-management practices that identify data value and criticality, and that ensure appropriate controls are in place according to best-governance frameworks and industry compliance requirements.	Disagree	Red
Internal SLAs: Availability and Restore Time targets for specific applications and services are spelled out for internal IT users in service-level agreements.	Disagree	Yellow
Identify management: Mature identity management processes and integrated application access management (single sign-on).	Agree	Green
Data protection: Data location, protection (encryption), and access are managed to meet compliance requirements.	Agree	Green

Fig.4.1. Security Availabiltiy Agree /Disagree Results

5. Conclusion:

As a conclusion, nowadays the value of information has reached a critical point becoming one of the most important assets that a company can possess, while collecting, processing, transmitting and storing has become too complex. It is up to organizations to decide for a specific approach for information security risk management system and all this depends in its scope, context of risk management, or industry sector. However, it is very important to consider the existing methodologies that have already shown good results. Identity management systems must enable companies to automatically manage multiple users in different situations and computing environments in real time. There were challenges in security as a part of Identity, Access & Risk to Verify Trust helps to protect against malicious actors while balancing Multi-Factor Authentication (MFA) requirements are agreed or disagreed.

References:

[1] Wayne Jansen and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication, pp. 800-144, 2011. [Online] http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
[2] S. Singh, Y.S. Jeong, J.H. Park, A survey on cloud computing security: issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222, https://doi. org/10.1016/j.jnca.2016.09.002.
[3] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, X. Huang, Hierarchical and shared access control, IEEE Trans. Inf. Forensics Secur. 11 (2016) 850–865, https://doi.org/10.1109/TIFS.2015.2512533.
[4] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, and Authentication in mobile cloud computing: a survey, J. Netw. Comput. Appl. 61 (2016) 59–80, https://doi.org/10.1016/j.jnca.2015.10.005.
[5] Z. Liu, J. Luo, L. Xu, A fine-grained attribute-based authentication for sensitive data stored in cloud computing, Int. J. Grid Util. Comput. 7 (2016) 237–244, https://doi.org/10.1504/IJGUC.2016.10001940.
[6] D.H. Sharma, C.A. Dhote, M.M. Potey, Identity and access management as security-as-a-service from clouds, Procedia Comput. Sci. 79 (2016) 170–174, https://doi.org/10.1016/j.procs.2016.03.117.
[7] A. Singh, K. Chatterjee, Identity Management in Cloud Computing through Claim-Based Solution, in: 2015 Fifth Int. Conf. Adv. Comput. Commun. Technol., IEEE, 2015. doi:10.1109/acct.2015.89.
[8] I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks, IEEE Commun. Mag. 54 (2016) 47–53, https://doi.org/10.1109/ mcom.2016.7452265.
[9] H. Saevanee, N. Clarke, S. Furnell, V. Biscione, Continuous user authentication using multi-modal biometrics, Comput. Secur. 53 (2015) 234–246, https://doi. org/10.1016/j.cose.2015.06.001.
[10] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. 13 (2014) 113–170, https://doi.org/10.1007/s10207-013-0208-7.
[11] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2011) 50–57, https://doi.org/10.1109/ MSP.2010.115.

[12] A. Khalil, M. Khreishah Azeem, Consolidated Identity Management System for secure mobile cloud computing, Computer Networks. 65 (2014) 99–110, https://doi.org/10.1016/j.comnet.2014.03.015.
[13] A.P. Méndez, R.M. López, G.L. Millán, Providing efficient SSO to cloud service access in AAA-based identity federations, Futur. Gener. Comput. Syst. 58 (2016) 13–28, https://doi.org/10.1016/j.future.2015.12.002.
[14] J.F. González, M.C. Rodriguez, M.L. Nistal, L.A. Rifón, Reverse OAuth: a solution to achieve delegated authorizations in single sign-on e-learning systems, Comput. Secur. 28 (2009) 843–856
[15] S. Iqbal, M.L. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M.K. Khan, K.K. Raymond Choo, On cloud security attacks: a taxonomy and intrusion detection and prevention as a service, J. Netw. Comput. Appl. 74 (2016) 98–120, https:// doi.org/10.1016/j.jnca.2016.08.016.
[16] B. Dong, Q. Zheng, F. Tian, K.M. Chao, R. Ma, R. Anane, An optimized approach for storing and accessing small files on cloud storage, J. Netw. Comput. Appl. 35 (2012) 1847–1862, https://doi.org/10.1016/j.jnca.2012.07.009.
[17] H. Liu, H. Ning, Q. Xiong, L.T. Yang, Shared authority based privacy-preserving authentication protocol in cloud computing, IEEE Trans. Parallel Distrib. Syst. 26 (2015) 241–251, https://doi.org/10.1109/TPDS.2014.2308218.
[18] C.A. Atwood, R.C. Goebbert, J.A. Calahan, T.V. Hromadka, T.M. Proue, W. Monceaux, J. Hirata, Secure web-based access for productive supercomputing, Comput. Sci. Eng. 18 (2016) 63–72, https://doi.org/10.1109/MCSE.2015.134.
[19] J. Liu, M. Au, X. Huang, R. Lu, J. Li, Fine-grained two-factor access control for web-based cloud computing services, IEEE Trans. Inf. Forensics Secur. 6013 (2015) 1, https://doi.org/10.1109/TIFS.2015.2493983.
[20] V. Chang, M. Ramachandran, towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput. 9 (2016) 138–151.
[21] C.A. Lee, Cloud federation management and beyond: requirements, relevant standards, and gaps, IEEE Cloud Comput. 3 (2016) 42–49, https://doi.org/ 10.1109/MCC.2016.15.
[22] Yuanchao Shu, Y.J. Gu, Jiming Chen, Y. Shu, J. Chen, Dynamic authentication with sensory information for the access control systems, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 427–436, https://doi.org/10.1109/TPDS.2013.153.
[23] C. Lyu, S.F. Sun, Y. Zhang, A. Pande, H. Lu, D. Gu, Privacy-preserving data sharing scheme over cloud for social applications, J. Netw. Comput. Appl. 74 (2016) 44–55, https://doi.org/10.1016/j.jnca.2016.08.006.