International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206124

Defence Mechanism for Access Management in Cloud Computing

Dr. AbidHussain[1], Dr. Praveen Kumar Sharma[2]
[1]Assistant Professor, School of Computer Applications, Career Point University, Kota, Rajasthan, India
[2]Vardhman Mahaveer Open University, Kota, Rajasthan, India

ABSTRACT

Cloud computing is a modern approach of distributed computing which provides different kinds of on-demand services for the business organization as well as individual users. It provides a platform to adopt information Technology and its features without huge expenditure on infrastructure and applications. However, cloud computing provides various types of services as per the requirement of the user and business is popular for But due to the increasing utility of cloud computing now, it also has many possibilities of various types of network attacks and privacy violations. However, the identity and access management are used to manage all the services including multi-tenancy and third party infrastructure based services provided by the cloud computing technology. In this paper, the issues related to authentication, access management in cloud computing environment are explained along with the proposed framework to reduce the problem in access management in the cloud computing.

Keywords : Cloud Computing, Security, Privacy, IAM, Compliance, Audit, Multi-Factor Authentication.

I. INTRODUCTION

The proposed research of the title "Defence Mechanism for Access Management in Cloud Computing" is an approach to provide accessibility for working on the cloud environment. Access Management technique in cloud computing is used to manage personal identity information of the user as well as business organization [1]. So that access to computer resources applications data and services is controlled properly.

Identity management helps prevent security breaches and plays a significant role in helping your company meet IT security compliance regulations. The benefits of keeping your customer or company financial data safe from unauthorized access can be huge.

Identity and access management solutions handle on boarding bringing an employee into the enterprise's network for the first time the management of their access lifecycle as they work in the enterprise, and off boarding the opposite of on boarding. In other words, this component of cyber security grants the right permissions to the right users at the right time and makes sure that users are who they say they are via authentication.

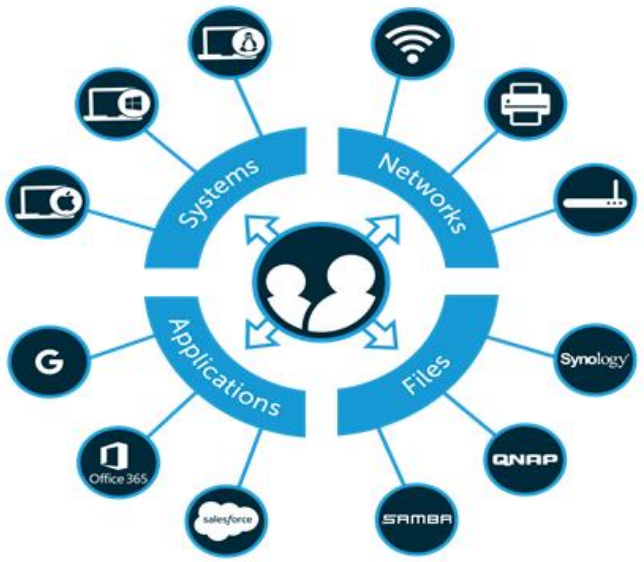

Figure 1 : Cloud Identity and Access Management System (IAM)

IAM is a framework provided to business processes that will help with management of electric and digital identity. This framework is an equipped with required policies to manage all the digital identity. This also has all the technologies those needed to handle and support identities.

On the other hand, cloud identity management differs from the traditional model in that it is optimized for integration across devices, operating systems, applications, and resources. This is essential, as cloud migration will open access to endpoints outside of enterprise control and across locations [2,3].

IAM systems provide administrators with the tools and technologies to change a user's role, track user activities, create reports on those activities, and enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and government regulations.

II. FUNCTIONS ACCESS MANAGEMENT IN CLOUD COMPUTING

The identity management system stores information on all aspects of the identity management infrastructure. Using this information, it provides authorization, authentication, user registration and enrolment, password management, auditing, user self-service, central administration, and delegated administration [4].

- **Stores information**

The identity management system stores information about the following resources: applications (e.g. business applications, Web applications, desktop applications), databases (e.g. Oracle, DB2, MS SQL Server), devices (e.g. mobile phones, pagers, card keys), facilities (e.g. warehouses, office buildings, conference rooms), groups (e.g. departments, workgroups), operating systems (e.g. Windows, Unix, MVS), people (e.g. employees, contractors, customers), policy (e.g. security policy, access control policy), and roles (e.g. titles, responsibilities, job functions).

- **Authentication and authorization**

The identity management system authenticates and authorizes both internal and external users. When a user initiates a request for access to a resource, the identity management first authenticates the user by asking for credentials, which may be in the form of a username and password, digital certificate, smart card, or biometric data[5]. After the user successfully authenticates, the identity management system authorizes the appropriate amount of access based on the user's identity and attributes. The access control component will manage subsequent authentication and authorization requests for the user, which will reduce the number of passwords the user will have to remember and reduce the number of times a user will have to perform a logon function. This is referred to as

"single sign-on" or "reduced sign-on." A realistic goal for an identity management system is to enable single sign-on for all Web applications, but it is currently unrealistic to provide single sign-on functionality for all applications across the enterprise.

- **External user registration and enrolment**

The identity management system allows external users to register accounts with the identity management system and also to enrol for access privileges to a particular resource. If the user cannot authenticate with the identity management system the user will be provided the opportunity to register an account. Once an account is created and the user successfully authenticates, the user must enrol for access privileges to requested resources[6]. The enrolment process may be automated based on set policies or the owner of the resource may manually approve the enrolment. Only after the user has successfully registered with the identity management system and enrolled for access will access to that resource be granted.

- **Internal user enrolment**

The identity management system allows internal users to enroll for access privileges. Unlike external users, internal users will not be given the option to register because internal users already have an identity within the identity management system. The enrolment process for internal users is identical to that of external users.

- **Auditing**

The identity management system facilitates auditing of user and privilege information. The identity management system can be queried to verify the level of user privilege. The identity management system provides data from authoritative sources, providing auditors with accurate information about users and their privileges.

• **Central administration**

The identity management system allows administrators to centrally manage multiple identities. Administrators can centrally manage both the content within the identity management system and the structural architecture of the identity management system.

III. BENEFITS OF ACCESS MANAGEMENT IN CLOUD COMPUTING

Cloud-based services offer multiple advantages over the traditional products and this is one reason why more attention is given towards it. Benefits of SaaS are not at all limited up to financial aspect but, also to many other aspects [7]. In addition, you reap many benefits from identity management that occurs every day, not just during a major threat.

- **Enhanced Networking Abilities:**Identity management makes it easy in sharing network capabilities with complete grid of end users who are connected with it. For example, if a new program is appended to a network then, this will easily be available for network users who are connected without any single delay.
- **Offers a Smooth Collaboration:** SaaS is increasingly being designed and utilized as the hub for connecting with virtual networks of several suppliers, distributors, and trading partners. After knowing that SaaS is cloud-based, it has become easy to establish a new connection between identification and access.
- **Improved On-Demand Support:** The problems that result from churn protects organization with cloud-based solutions. Experts will be able to provide 24*7 support and monitoring, whenever required.
- **Increase in Overall Productivity:** It is completely well-known fact that cloud-based services are hosted and configured by service providers. These pose a little or zero hassle either for end-users or

clients. The hassle-free identity facilitates users with ease in focusing on the business development. As a result, there will be the improvement in overall productivity of the organization.

- **Centralized Management System:** Businesses will be able to manage entire services and programs all at one place with help of cloud-based services. All the identity management will be done with a single click on the single dashboard.
- **Reduced IT costs:** Identity management enables automatic provisioning, providing or revoking users' access rights to systems and applications. Provisioning happens whether you automate it or not.

IV. CHALLENGES OF THE ACCESS MANAGEMENT

Many companies are moving toward the clouds and many are already into cloud computing. The problem started when these companies started facing identity problem in their cloud[8,9]. These were some serious problems those were not experienced before by them. It is as hard as managing data in your own data centre. However, as clouds came in IT have to do more than that and for un-experienced clouds, they do not know of the accessibility.

These changes in the system and security area very long, busy and devastating practice that shatters the security. Business got some problems here. Due this heavy process, they get more focused on managing data resolving identity problem. Their focus just gets moved from securing these clouds first and that makes it vulnerable. This creates a blind spot and increases security risk.

1. **Identity Provisioning / De-provisioning:**This concerns with providing a secure and timely management of on-boarding (provisioning) and off-boarding (de-provisioning) of users in the cloud.
2. **Maintaining a Single ID:**It is tough for the organizations to keep track of the various logins and ID that the employees maintain throughout their tenure.
3. **Compliance Visibility:** Who has access to what :When it comes to cloud services, it's important to know who has access to applications and data, where they are accessing it, and what they are doing with it.
4. **Security for 3rd party or Vendor Network:** A lot of services and applications used in the cloud are from 3rd party or vendor networks. You may have secured your network, but can't guarantee that their security is adequate.
5. **Password Re-use:** Due to the prevalence of outside threats, passwords have become essential to holding and managing any account online.

V. KEY COMPONENTS OF ACCESS MANAGEMENT SYSTEM

For making secure working environment of the access management in the cloud computing [10,11]. We can consider following key components :

- **User identity, Authentication, and Authorization Service :** Enables applications deployed to the cloud to externalize the authentication of users to a range of different identity providers.
- **Multifactor Authentication :** Combats identity theft by adding an additional level of authentication for application users.
- **Directory Services :** Hosts the user profiles and associated credentials that are used to access applications.
- **Reporting :** Provides a user-centric view of access to resources or a resource-centric view of access by users.

- **Audit and Compliance :** Validates implemented controls against an organization's security policy, industry compliance, and risk policies and to report deviations.
- **User Access Management :** Enables cloud providers to manage user identities in cloud-based platforms, applications, and services.

VI. PROPOSED DEFENSE MECHANISM

For maximizing security in enterprises, it is necessary to ensure a strong Access Management systems and authentication process. Access Management system implementation in Cloud should have consistency with existing Access Management and authentication implementation. This mechanism helps to mitigate risk of the business as well as individual in the cloud computing.

The architectural design of Access management System for cloud computing is shown Figure. 2.The basic functional components are user management, authentication and authorization management, information repository management. The major stakeholder are system administrator, cloud service users, cloud service providers [12].

The way that we choose to implement identity and access management in your cloud environment depends on your specific business requirements. We need to choose a cloud provider that supports the strategy we want to implement[13].This enables better collaboration, enhanced productivity, increased efficiency and reduced operating costs.

Our proposed Access Management System is an one stop solution for making defence mechanism for the cloud based system or software application. We can easy to use this mechanism to secure any web based application where we can easy to protect the system with specific roles and right of the users as well as administrator. We have also used multi-factor authentication controls that are used combat increasing levels of identity theft. It does control the level of required authentication based on a user's location, past activity, operation being performed, preferences, or other factors.

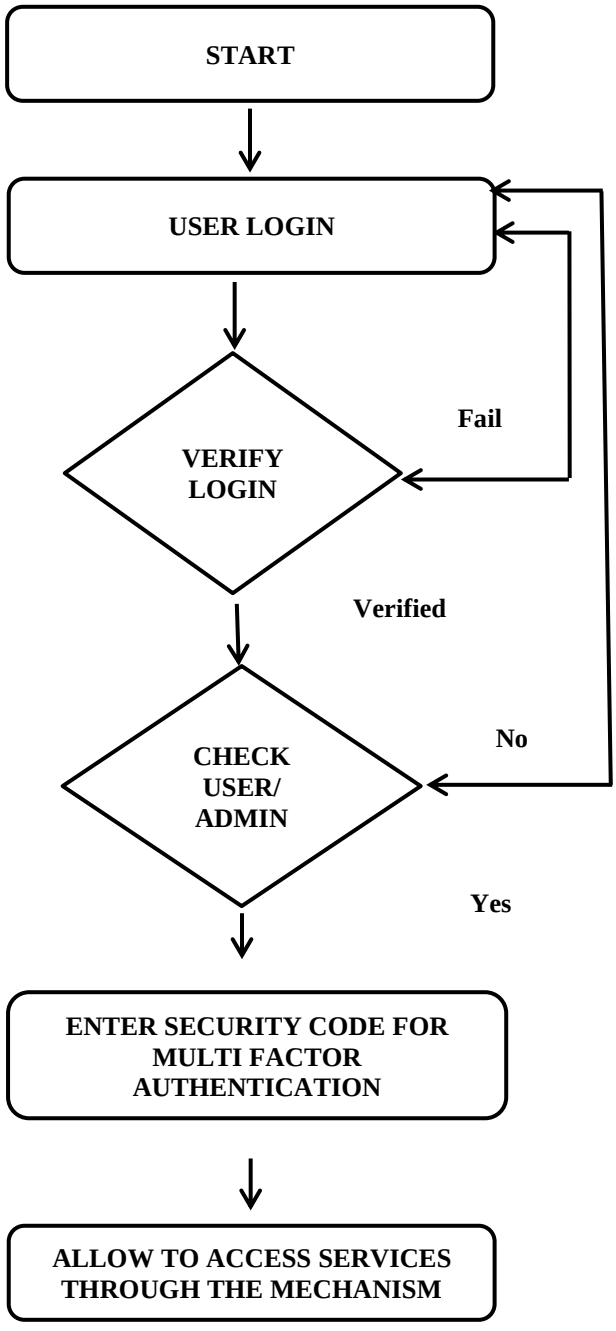

Figure 2 : Defence Mechanism for Access Management in Cloud Computing

In this proposed framework, we used Multi-Factor and Privileged Access techniques for validating user in the

cloud-computing environment. In this mechanism, user need to login with valid credentials. If login fail then system will be closed.

After successful login, this mechanism requires a security token as a form of multi-factor authentication. If the authentication fails then system requires login again. If the validation is success then check the privileged orroles of the logged user inside the user database. Whether it is user then allow to access only those resources which are assigned to the user. If the user's type is admin then allow to access administration module.

VII. CONCLUSION

The defence mechanism provided to business processes that will help with management of electric and digital identity. This mechanism is an equipped with required policies to manage all the digital identity. This also has all the technologies those needed to handle and support identities. Access Management is like a wall between critical information and employees/ users within the organization. With this, you can control privileges and circumstance of those privileges granted to the user[14]. The Access Management mechanism is developed for providing end level security with privileged and multi factor authentication techniques. Therefore, that one user has only one identity. This research represents proposed defence mechanism with its commonly use dmulti-factor authentication and privileged based accessibility, benefits, challenges associated with defence mechanism, recommendations and best practices from academia and industry perspectives. Finally, technology alone will not be enough to make organization secure it is the people, process and the IT that need to work coherently to make a secure information system. Future research is to fill the gap between the organization information flow security requirements and aligning it with the IAM solution.

VIII. REFERENCES

[1]. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011

[2]. F. Gens, "New IDC IT cloud services survey: top benefits and challenges," 2009.

[3]. A. Murphy, "Storing data in the cloud raises compliance challenges," 2012.

[4]. S. Lee, I. Ong, H. T. Lim, H. J. Lee, Two factor authentication for cloud computing, International Journal of KIMICS, vol 8, Pp. 427-432-33

[5]. SecaaS Implementation Guidance Category 1 Identity and Access Management. Cloud Security Alliance, pp. 43, 2012.

[6]. Abdul Ghafoor, MisbahIrum, Muhammad Qaisar, "User Centric Access Control Policy Management Framework for Cloud Applications", 2013

[7]. RizwanaShaikh, M. Sasikumar , " Identity Management in CloudComputing ", International Journal of Computer Applications (0975- 8887) Volume 63-No.11, February 2013

[8]. A. Josang and S. Pope. User Centric Identity Management, In Proc. AusCERT, Gold Coast, May 2005.

[9]. S.Subashini, V. Kavitha;"A survey on security issues in service delivery models of cloud computing";Journal of Network and Com

[10]. Yan Yang; Xingyuan Chen; Guangxia Wang; Lifeng Cao, "An Identity and Access Management Architecture in Cloud," in Computational Intelligence and Design (ISCID), 2014

[11]. H. Saevanee, N. Clarke, S. Furnell, V. Biscione, Continuous user authentication using multi-modal biometrics, Comput. Secur. 53 (2015) 234–246

[12]. D. Shlomi, “Privileged identity management: Securing the enterprise Network,” Security, vol. 2010, issue 12, pp. 4-6, December 2010.
[13]. S. Travis, “Identity in the cloud, computer,” Fraud & Security, issue 7, pp. 19-20, July 2012.
[14]. U. Habiba, R. Masood, M.A. Shibli, M.A. Niazi, Cloud identity managementsecurity issues & solutions: a taxonomy, Complex Adapt. Syst. Model. 2 (2014)

Cite this article as :

Dr. Abid Hussain, Dr. Praveen Kumar Sharma, "Defence Mechanism for Access Management in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 1, pp. 137-143, January-February 2020. Available at doi : https://doi.org/10.32628/CSEIT206124
Journal URL : http://ijsrcseit.com/CSEIT206124