ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

Studying Concepts of Identity Management Technologies and Secure Cloud Computing Technologies

Dr.Ashwani Sethi[1],Dr. Mahendra Kumar[2]
[1,2]Guru Kashi University, Talwandi Sabo

Abstracts

Cloud computing is a complicated system that enables desired services by combining a variety of networked devices. Cloud computing is made up of several types of configurable distributed systems with various levels of connectivity and utilization. Organizations are rapidly adopting cloud networks due to advantages such as cost-effectiveness, scalability, reliability, and flexibility. Cloud networks are subject to different types of network attacks and privacy difficulties, despite the primary benefits of cloud computing being enticing realities. In a cloud context, elements such as multi-tenancy and third-party managed infrastructure required the use of an identity and access management method.Many academics and industry professionals have addressed the issues of secure access to cloud resources. The concerns of authentication, access control, security, and services in a cloud environment are examined in this study, as well as the strategies recommended to address them. Identity and access management, security problems, and cloud services are addressed in a detailed comparative assessment of existing solutions from the perspectives of cloud service providers and cloud customers.

Keywords: *Access management,Cloud Computing,Technologies and Secure,Technologies.*

1. Introduction

Cloud computing is a collection of configurable computing resources such as networks, servers, storage, services, and applications that work together to provide cloud users with convenient and on-demand access. People frequently mention cloud computing, and it is now used in a variety of

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

business industries. Identity and other types of management in the cloud are the responsibility of cloud service providers (CSPs). However, identity management system vulnerabilities are responsible for a substantial number of data leakage instances. Identity and access management (IAM) in the cloud is a critical topic for cloud-based service acceptability. Currently, identity management is primarily based on CSPs, which falls short of meeting users' needs for flexible and fine-grained access control policies. Private Cloud, Public Cloud, and Hybrid/Federated Clouds are the three types of cloud environments. A private cloud is one that is specifically built and dedicated to the needs of a single company. Infrastructure support for numerous businesses is handled and maintained by a third-party supplier in a public cloud environment. The public cloud concept, also known as a multi-tenant environment, allows enterprises to pool resources in order to reduce total service costs. Hybrid cloud infrastructure, also known as federated cloud infrastructure, combines on-premises, private and public cloud services. Multi-provider clouds are another idea in cloud infrastructure, which is a system that relies on many cloud providers and distributes work load throughout the cloud environment.

The capacity and handling of information in a cloud framework is finished by organizations or with the assistance of outsider project workers. Information and applications put away in the cloud should be protected, and the framework should be in a solid climate, as indicated by the specialist co-op. Besides, clients should guarantee that their validation certifications are protected. There are various security weaknesses that risk information during the information access and capacity process in the cloud climate, especially when information is put away with the help of outsider suppliers who might be pernicious aggressors themselves.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

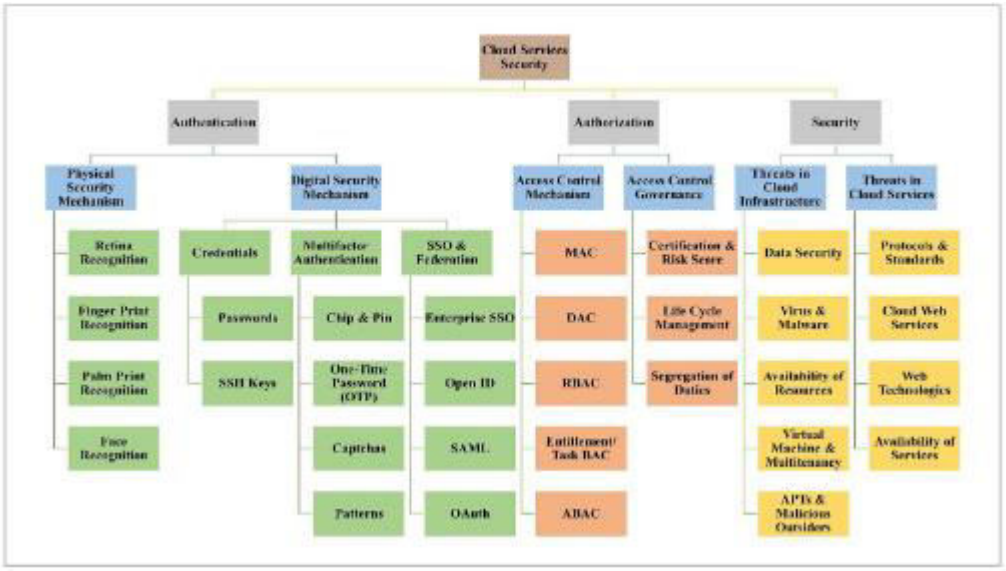

Figure: 1 Taxonomy of Cloud Services Security

2. Authentication mechanisms

The act of endorsing one element through one more element is known as confirmation. It's utilized to check whether an individual or an application is able to access or guarantee benefits. Commonly, the validation cycle is completed by programming or a part of programming. Sign on accreditations, multifaceted confirmation, outsider validation, basic text passwords, 3D secret phrase objects, graphical passwords, biometric verification, and computerized gadget verification are on the whole regular confirmation strategies in an organization setting. Any one or a mix of the previously mentioned verification strategies is utilized by a cloud framework. Consent to get to the cloud is as of now acquired utilizing a character the executives framework.

2.1 Physical security mechanisms

Endeavor Single Sign-on (ESSO) permits you to use less passwords and client IDs while getting to numerous applications. As recently expressed, "united character," or "personality organization," alludes to the advances, conventions, and use-cases that permit the exchange of personality data between in any case independent security areas. One of the most common use cases is cross-space, online single sign-on.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

2.2. Digital security mechanisms

2.2.1. Credentials and secure Shell keys

Qualifications show authority, status, access honors, and privileges. It demonstrates that the client is qualified for or meriting assets and administrations. A conventional methodology of getting the framework against undesirable action is to utilize certifications like a one-time secret phrase, design, or manual human test. In cloud settings, the most frequently involved frameworks for dealing with access qualifications are the Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (AD).

3. Identity & access management systems

Single sign-on and (ii) brought together character the chiefs are two standards that are at the center of Digital Identity Management. Single sign-on (SSO), as characterized in [2], is an element that permits a client to sign in once and get sufficiently close to all frameworks in an alliance. The client just necessities to sign in once and afterward gains admittance to every one of the assets in the alliance, alliance, or association without checking in again at every one. Kerberos-based and shrewd card-based SSO instruments are the two sorts of SSO components. Kerberos ticket allowing ticket TGT is utilized to concede qualifications with the Kerberos strategy. The client signs in with a shrewd card in savvy card put together sign-with respect to. While getting to various applications, Enterprise Single Sign-on (ESSO) assists with diminishing the quantity of passwords and client IDs utilized. "Unified personality," or "character organization," portrays the advances, conventions, and use-cases that empower the exchange of personality data across in any case independent security spaces, as shown previously. The utilization cases incorporate normal situations, for example, cross-space, online single sign-on.

3.1 Party that is reliant:

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

The website that wishes to verify the identity of the end-user. (This is the one who performs the service.) The server that verifies end-user identification (also known as the server-agent). User-agent: The user agent is the interface via which users interact with the identity provider or relying party (e.g., the browser). Here's how to put it to use.

3.2 Open ID:

A user visits a dependent party's website to obtain a service (e.g., a service provider). The user uses an Open ID form to log in to this reliant party. The user would supply his identify before to the logic process, which would be provided by an Identity. The relying party will use this information to find the identity provider's website.

4. Review of literature

Yassin et al. (2012)proposed another setting where clients don't enlist their passwords to the specialist co-ops. The passwords were provided with fundamental data from the information proprietor to the specialist organizations. The proposed strategy is more appropriate for the cloud climate and endures different known assaults.

Xie et al. (2016)principally centered on the information handling, putting away and getting to. The model was intended to guarantee that the clients with legitimate specialists got relating characterized information and the illicit clients were limited. Unapproved legitimate clients gaining admittance to the information made their model incredibly appropriate for the distributed computing standards.

Sood (2012)proposed a strategy for giving information by really taking a look at the trustworthiness and confirmation. They separated the information into various segments as, 128-bit SSL encryption, list developer, confirmation of advanced mark of the proprietor, message validate code and verification of client by proprietor and cloud. The creator's strategy gave accessibility of information by surpassing many issues like unapproved access, information

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

spillage, altering of information even from the cloud specialist co-op. The strategy accomplished the accessibility, unwavering quality and respectability of information crossing through proprietor to cloud, cloud to client and recovery of records from cloud via looking over scrambled information.

Nicanfar et al. (2014)introduced an original common verification and key administration component customized for shrewd matrix (SG) interchanges. The proposed instrument announced the requirements for getting the framework and dealing with the course of that framework. The creators clarified with regards to the advantages of public key foundation and the powerful asset usage because of key size and enormous key dispersion upward.

Hashizume et al. (2014)inspected concerning the security issues in cloud and current solutions for soothe the risks. The makers communicated that customary security frameworks were not working commendably in cloud environment as it was a confounded designing made from a blend of different headways. Modified security methodologies were upgraded for standard courses of action that could work with cloud plans.

Fernandes et al. (2014)outlined the works on cloud security issues and made a total overview of the composing in regards to the matter. They kept an eye on a couple of key subjects specifically shortcomings, risks, and attacks and proposed a logical order for their course of action. It furthermore contained a cautious review of the guideline thoughts concerning the security state of cloud conditions.

Armando et al. (2013)proposed a solitary sign-on convention for beating the validation defect in programs. Their work examined regarding the effect and remediation of SSO utilization. The current SSO conventions, for example, SAML SSO and Open ID experience the ill effects of confirmation defect. Assist and Bettencourt (2016) reviewed the different cloud league models accessible in the writing and assessed those structures in light of their useful and non-utilitarian properties.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

Fett et al. (2017)investigated the security parts of OpenID Connect. They made a complete conventional model of the web to foster a definite proper model of OpenID Connect. The creators formalized and demonstrated the focal security properties for OpenID Connect including verification, approval and meeting respectability properties in light of their model. Likewise, they proposed the security rules for the implementers of Open ID Connect.

Ferry et al. (2015)researched the potential security issues of O Auth, an approvals system for giving outsider applications with revocable admittance to client information. The creators likewise incorporated the examination of the security elements of a few well known O Auth coordinated sites. They contrasted that data with the danger model and proposed an answer that made out of three sections to be specific, client application, approval server and asset server.

George et al. (2017)zeroed in on the security in the correspondence between a client and specialist co-op and the manners in which a client data could be verified. The creators used the advantages of Security Assertion Markup Language (SAML) put together Single Sign-With respect to for security improvements. Security was given by utilizing hash-based encryption calculation (HBE). They proposed that higher security could be given to client login by utilizing an extra cryptographic procedure like Hash based Encryption calculation with the assistance of key trade convention.

5. Security threats in cloud environment

Distributed computing is another innovation that is rapidly turning into the most solid method for putting away and secure information. Indeed, even while a cloud-based framework enjoys many benefits, it has specific security worries about the information it stores. Distinguishing the greatest risks in a cloud climate is the initial move towards decreasing them. The ruling standards for the recently observed security issues in the cloud are shared and on-request access. The quick extension of distributed computing has expanded security worries in an assortment of ways. Information breaks, certification assurance, account commandeering, compromised points of interaction and APIs, vindictive insiders, DoS assaults, and shared innovation issues are among the security issues referenced. The many kinds of dangers that exist in the cloud climate, as well as their present commonness.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

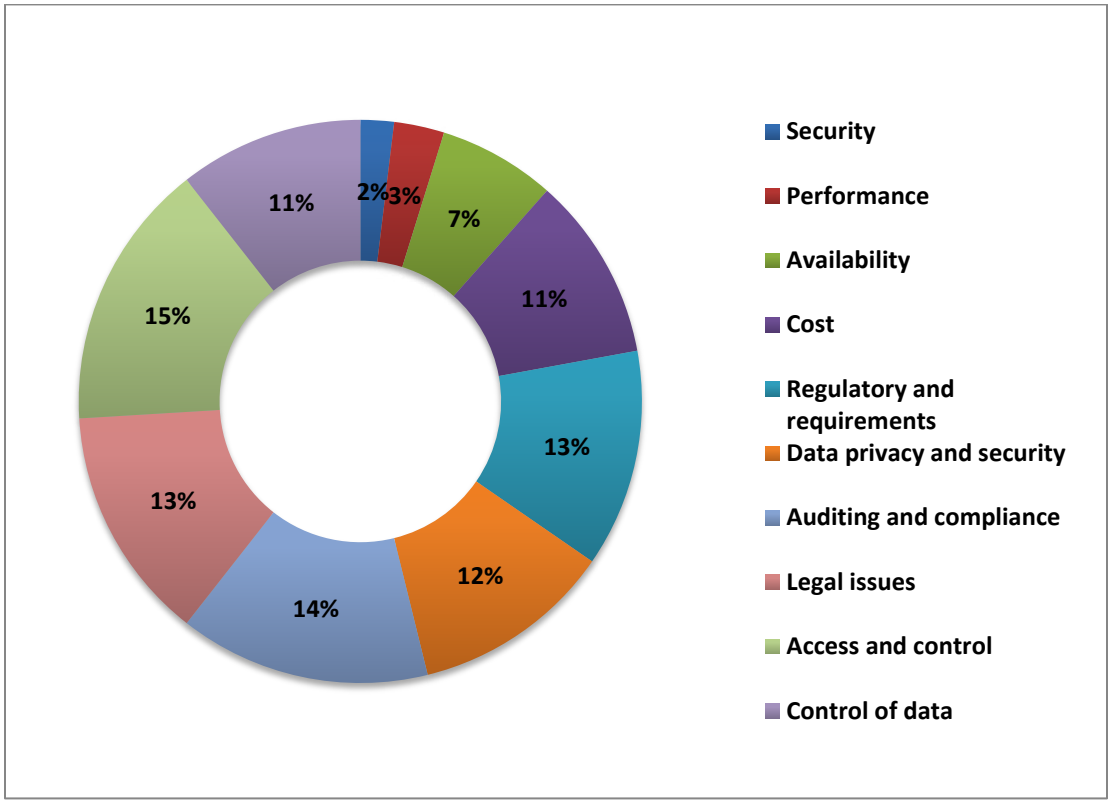

Figure: 5 Security Threats in Cloud Environment

5.1 Data security

In a cloud setting, information security is basic as far as accessibility, honesty, and classification. Cryptography is one of the accessible information security techniques. Cryptographic components promptly apply security shields to information. A few numerical methodologies for creating mathematical information for cryptography incorporate indivisible number factorization, obstinacy of the discrete logarithm, and irregular number producing. Changing advancements and secret word breaking techniques are two striking supporters. Because of the colossal development in the handling ability of present day PC hardware, enormous combinatory key spaces and search time intricacy are currently promptly and quickly cultivated.

5.2 Virus or malware

Malicious software, commonly known as malware, is software that is meant to interfere with normal computer operations. It's used to get access to computer systems that aren't connected to

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

the internet or to gather sensitive information. Malware has the heinous goal of working against users' wishes and wreaking havoc on the performance of cloud-based systems. Cyber criminals commonly distribute malware and entice victims to install it on their computers or mobile devices by making false promises. The criminals' ultimate goal is to obtain control of the computer or mobile device in question. Once malware has been installed, the attackers may be able to take complete control of the computer or mobile device.

5.3 Availability of resources

The expression "accessibility of assets" alludes to the frameworks and administrations that a validated element can access with legitimate approval. The accessibility of the cloud alludes to the assortment of assets that approved associations can access whenever. One of the main security prerequisites in distributed computing is accessibility, which guarantees that cloud clients might get to assets whenever and from any area. In certain conditions, materials are accessible in an assortment of arrangements that should be made accessible to cloud clients without interference during cloud administration access. The ability to keep carrying on with work as expected on account of a security break or fiasco is the major objective of accessibility.

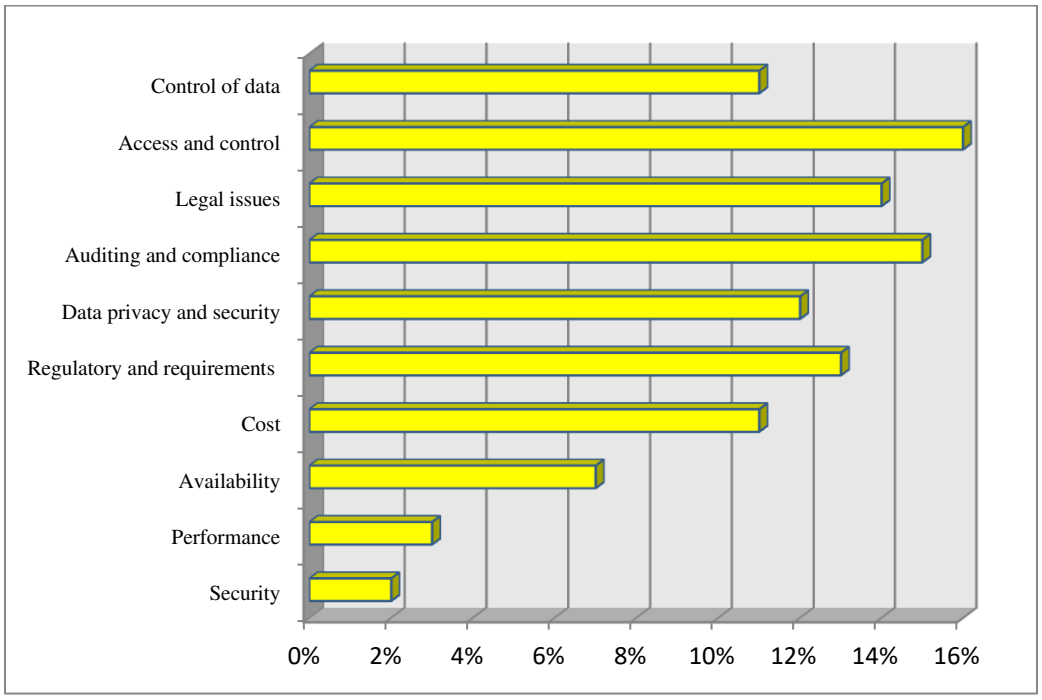

Figure: 5.3 Availability of resources

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

6. Materials And Methods

Web applications and cloud administrations are quickly arising as the inescapable innovation for correspondences between associations. Cloud based arrangements are at present sent to give enhancements in the current business cycles and administrations. The significant test associated with cloud is the security of information that is put away and moved. Cloud framework requires a broad validation instrument to safeguard information as well as to guarantee that the ideal individual is getting to the right data. However there are different answers for confirmation related issues, the validation components for cloud based networks actually experience in their security perspectives.

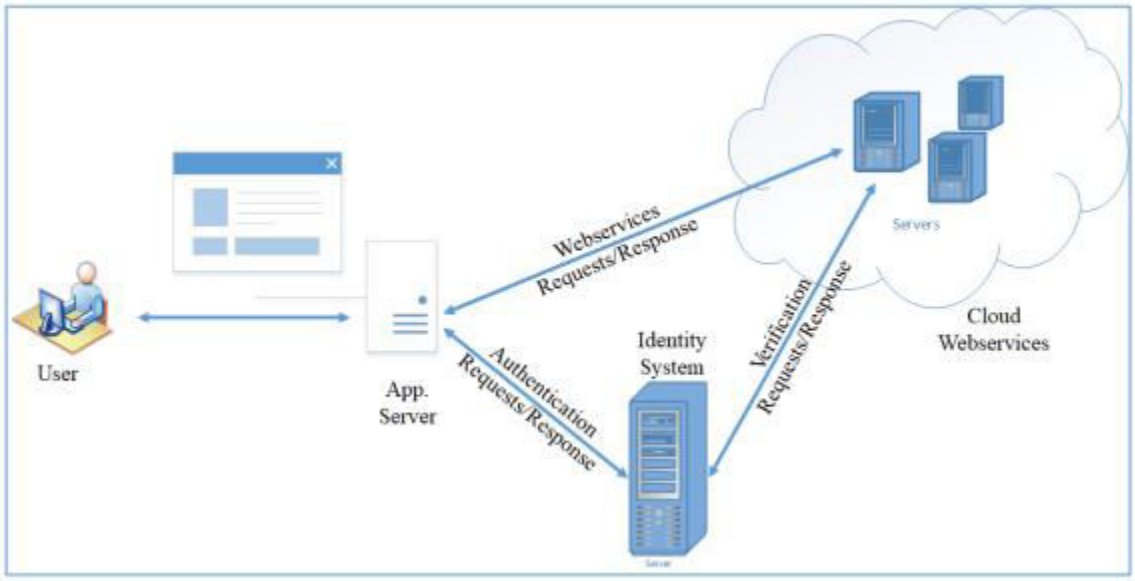

Figure 6.1: Identity management model for authentication

6.1 Identity Management System Model

The initial segment of this work is about the validation to cloud web administrations by approved clients. In personality the executive's model, the client is verified through a character framework. When the client is effectively confirmed against his certifications, the character framework gives a token to every personality. The tokens are revived in occasional stretch to such an extent that any unauthenticated people are restricted from utilizing the generally created badge of other

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

verified clients. While attempting to get to a cloud web administration from any started application, the application passes the token alongside the necessary boundaries.

6.1.1 Conceptual Framework of Identity Management Model

A coordinated personality the executive's framework for cloud web administrations joins SAML and token-based confirmation to give further developed security. In this framework, character provider(s), administration provider(s) and web administrations provider(s) are coordinated in a solitary engineering. The prospects of getting information in cloud climate are investigated through a half breed model of scrambled SAML statements for verification and access tokens for web administrations. SAML based correspondence is laid out with the end goal of verification with the assistance of metadata documents. A metadata record characterizes the objectives, restricting technique and qualities which are required to have been passed in a SAML demand.

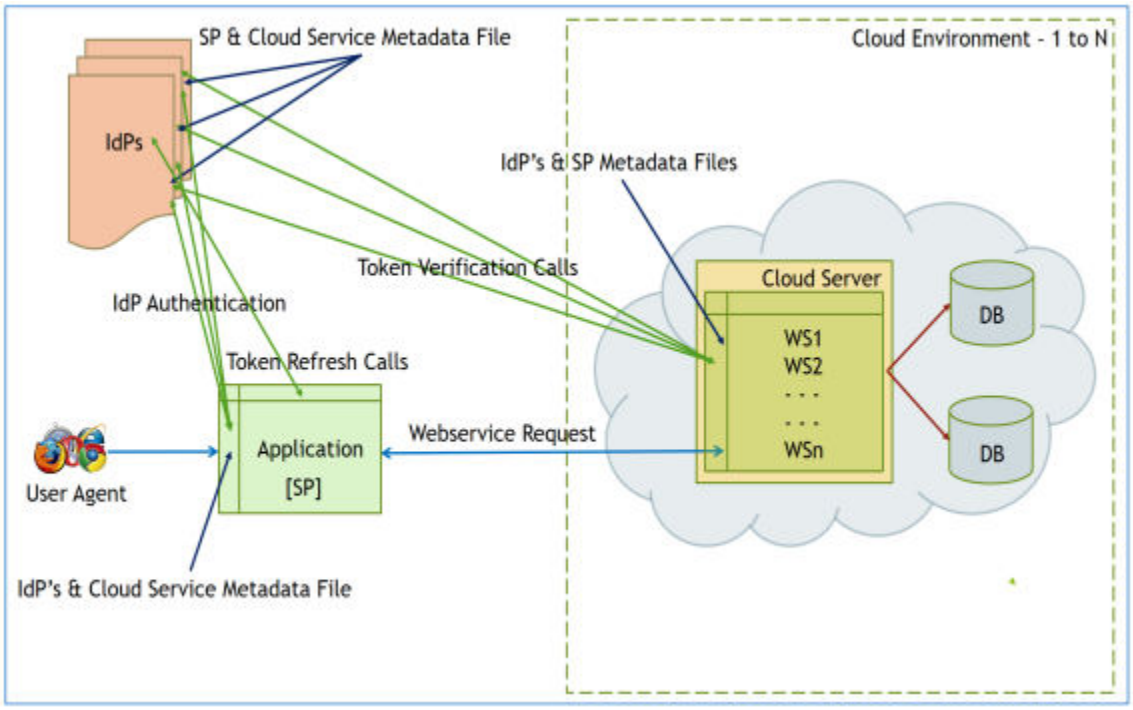

Figure 6.1.1: Architectural diagram of the authentication system model

7. Results

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

7.1Implementation Details

The model structure is executed and tried with the assistance of Microsoft Azure cloud stage. The personality supplier and the web administration servers are designed in independent Azure Windows 2008 Server virtual machines (Figure 7.1).

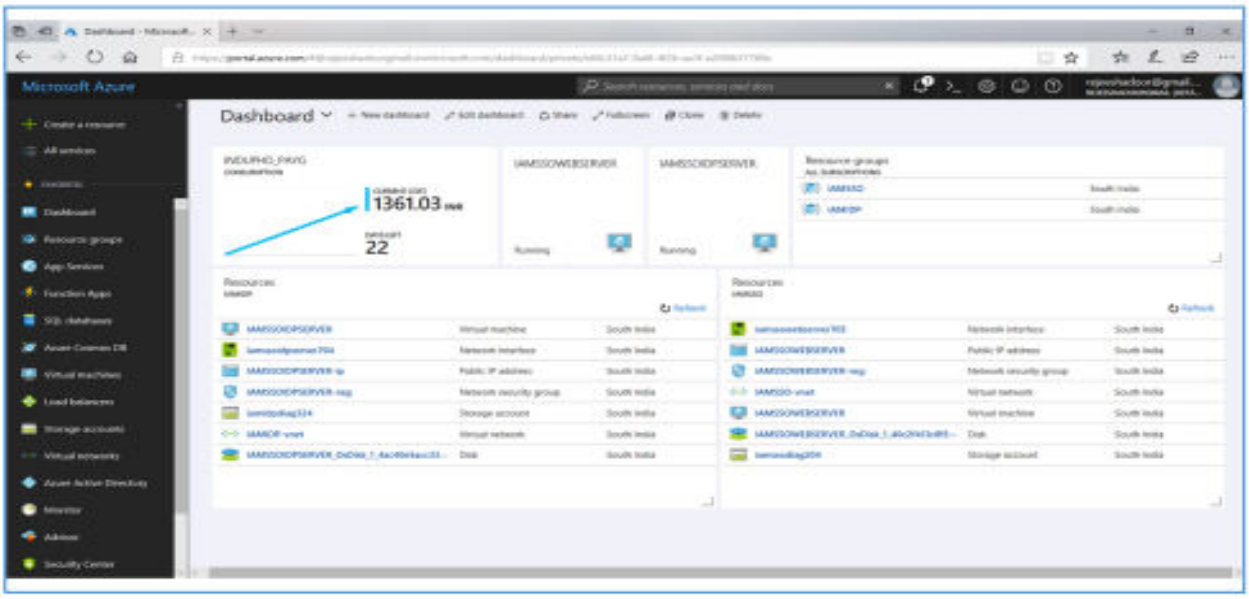

Figure: 7.1 Implementation Details

8. Discussion

A cloud design permits you to create, store, and access an assortment of assets from anyplace on the planet. Be that as it may, the insurance of these assets from different security dangers in the cloud climate stays a basic concern for cloud clients. The vital worry in the cloud climate is to screen, shield, and confirm the security of information very still, moving, and being used. Logon qualifications, for example, administration account and its accreditations are utilized in existing confirmation frameworks for cloud web administrations.They're usually hardcoded or specified in web service-using apps. The disadvantages of these systems include difficulty determining who or when a service is accessed, unlawful access if the credentials are known, and a lack of flexibility.

9. Conclusion

Distributed computing is a significant worldview for computerized arrangements since it lessens an association's capital and working expenses. Because of the idea of multi-tenure and outsider

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

designation for cloud climate support, security dangers and weaknesses are a major concern for this innovation. With an accentuation on personality the executives, access the board, security, and administrations, this study analyzed and portrayed the current security issues, possible dangers, and moderation in cloud administrations. This study investigations a few subjects, as well as the most generally utilized instruments and principle concerns related with every Mechanisms, proposals, and best practices according to the points of view of scholastics and industry The examination of different personality and access the board strategies, as well as the different cloud-based administrations, uncovers the need to work on existing character and access the executives structures, showing the bearing for future review and improvement of pertinent approaches.

10.References

1) Al-Janabi, S., Al-Shourbaji, I., Shojafar, M. and Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal.
2) Alexander, P., Pike, L., Loscocco, P. and Coker, G. (2015). Model Checking Distributed Mandatory Access Control Policies. ACM Transactions on Information and System Security, 18(2).
3) Alguliev, R. M. and Abdullayeva, F. C. (2013). Identity management based security architecture of cloud computing on multi-agent systems. Third International Conference on Innovative Computing Technology (INTECH 2013) (pp. 123–126). London.
4) Fan, K., Tian, Q., Huang, N., Wang, Y., Li, H. and Yang, Y. (2016). Privacy protection based access control scheme in cloud based services, 14(1): 7839758.
5) Fang, L., Susilo, W., Ge, C. and Wang, J. (2012). Hierarchical conditional proxy re-encryption. Computer Standards and Interfaces, 34(4): 380–389.
6) Faraji, M., Kang, J.-M., Bannazadeh, H. and Leon-Garcia, A. (2014). Identity access management for Multi-tier cloud infrastructures. 2014 IEEE Network Operations and Management Symposium (NOMS), pp. 1–9).

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

7) Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M. and Inácio, P. R. M. (2014). Security issues in cloud environments: a survey. International Journal of Information Security, 13(2): 113–170.

8) Wayne Jansen and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication, pp. 800-144, 2011.

9) 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), pp. 850-865,.

10) 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.

11) A.P. Méndez, R.M. López, G.L. MillánProviding efficient SSO to cloud service access in AAA-based identity federations Futur. Gener. Comput. Syst., 58 (2016), pp. 13-28, 10.1016/j.future.2015.12.002.

12) Gourkhede, M. H. and Theng, D. P. (2014). Analysing Security and Privacy Management for Cloud Computing Environment. 2014 Fourth International Conference on Communication Systems and Network Technologies, pp. 677–680. Bhopal, India.

13) Grobauer, B., Walloschek, T. and Stöcker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security and Privacy, 9(2): 50–57.

14) Gupta, R. (2016). Oracle GoldenGate for the Cloud. Mastering Oracle GoldenGate, pp. 507–535.

15) Habiba, U., Masood, R., Shibli, M. and Niazi, M. (2014). Cloud identity management security issues and solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1): 1–37.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021