International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.2.38

A Review Article on Authentication Protocols in Cloud Computing

Umaima Fatima[1] and Dr. Sheeba Parveen[2]
[1]Student, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
[2]Assosiate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: umaima0112@gmil.com

Received: 30-03-2023 **Revised:** 16-04-2023 **Accepted:** 29-04-2023

ABSTRACT

Cloud computing technology provides on demand computing resources like software, hardware and storage in pay-per-use model. Cloud computing is very beneficial for today's organizations, as there is no need to maintain physical infrastructure. These services and resources can be accessed from anywhere anytime over the internet. It is cost effective as users only need to pay for resources they use. Many individuals and organizations have shifted themselves over cloud environment as it is cheaper and convenient. As huge amount of sensitive data is being stored and processing in cloud computing environment so there is major concern of security. Lack of security may cause several issues. It may result in loss of organisation's data and may even leak confidential data of user and organisation to unwanted access. To implement security in cloud computing various authentication and encryption protocol exists. This aim of this paper is to review various authentication protocols given by various researchers all over the world.

Keywords-- Cloud Computing, Security Issues, Authentication, Authorization

I. INTRODUCTION

Cloud computing is providing on-demand services such as data storage , computing power , databases, software and servers over the internet. Cloud computing uses pay-per-use model. It allows to lower operational cost and scale business easily in times of need and lowers operational cost.

Cloud computing provides various advantages .It is being used in modern world in banking [1] and various other sectors[2][3][4] .It allows to easily scale resources and storage without investing in physical infrastructure .The user has to pay only for the resources that he actually use. Cloud computing allows to access data from anywhere anytime over the internet .Despite offering number of benefits, cloud computing suffers security challenges that must be addressed and taken care of .

A. Security Challenges of Cloud Computing

There are a lot of security challenges in cloud computing[5][6][7][8] . Researchers all over the world have analysed security issues and provided measure to improve it[9][10].Cloud services faces various security issues[11].Cloud service are vulnerable to denial of service attack that may result in downtime of entire system and halt the ongoing operation[12]. There are several insider threats in cloud computing such as Any malicious user gets into system access private and sensitive data. Many other attacks are also there in Cloud computing like Man-in-the-middle attack[13] ,SQL injection attack[14] and various other attacks .There may be data breaching issue too if a cloud service provider does not provide adequate security measures which in turn may result in unauthorized access to data. Cloud services are exposed to various user interfaces and application programming interfaces (APIs). If security measures are not adequately enabled in APIs then a user who is not authorized user may access data and may re-use the APIs or passwords.

B. Types of Cloud

1. Public Cloud: Public clouds are the cloud computing services available publicly over the internet that can be accessed by any authorize user in pay-per use-model. They are highly elastic and scalable. Public clouds are mostly managed and provided by some third party service providers. Public clouds provide a range of services such as computing power, storage, networking, and applications that are accessible over the internet, and can be quickly provisioned, scaled up or down, and accessed remotely from anywhere with an internet connection. Public clouds are known for their scalability, flexibility, and cost-effectiveness.

2. Private Cloud: The private clouds are dedicated for use of a particular organization. In private cloud organisations have complete control over resources, security and data. Private clouds are used by organisations that have more control over data and have specific security requirements or they have some sensitive data or work .Here computing resources and services are delivered via secure private network. It has less security issues as compared to public cloud

3. Hybrid Cloud: Hybrid cloud services combines both public and private cloud solution .Here applications and data shares resources between public and private cloud service based on requirement. Hybrid cloud allows flexibility and helps to meet demands in times of changing requirements of an organization or individuals in modern world [15][16][17].

4. Community Cloud: Community cloud service is a cloud service managed and used by a group of members or community for a special purpose. Community cloud is designed to serve the need of specific community with similar interests and requirements. It provides a way between public and private cloud offering a level of customization, security and privacy that may be required by organizations with shared interests. Community clouds are commonly used by organizations such as healthcare, government, finance, and education, where there are shared interests and requirements, or collaborative initiatives.

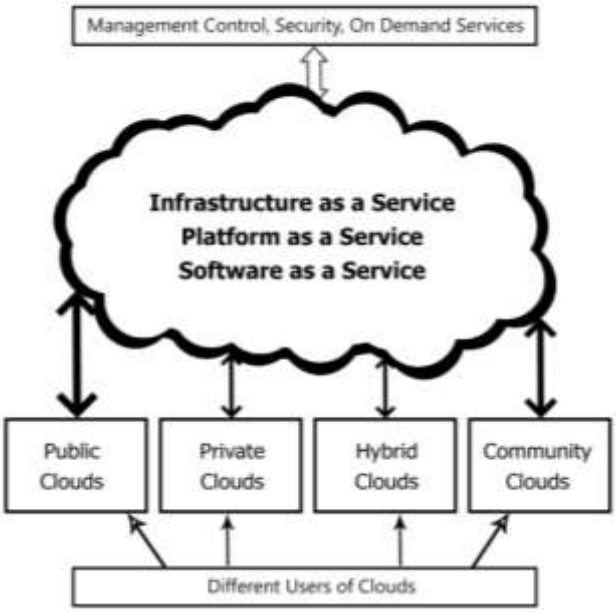

Figure 1: Cloud computing Model

C. Cloud Computing Services

Various types of services are provided by cloud computing[18] , some of them are as follows

1. IaaS: Infrastructure as a service in this cloud service model resources and infrastructures are distributed as a service It is highly scalable and flexible. Here highly scalable and automated[19]. Its infrastructure are rented to compensate the need of physical resources and workstations .Here large amount of sensitive data is being hosted so it is essential to ensure security. In [20]a framework is proposed that ensures security in IaaS

2. PaaS: platform as a service[21] .It provides both hardware and software tools which are used by developers to build application and services. PaaS is very scalable cloud computing service . It suits different type of businesses according to resources. It provides the business organisations and individuals a complete development and deployment environment. The users purchase these resources as they need and access them over a secure internet connection.

3. SaaS: software as a service it allows software and its functions available in pay-per-use model .It is a service that hosts software to be available for users. SaaS is highly scalable cloud computing service. It suits small and medium level and enterprise level business. SaaS allows applications to run on SaaS providers' server without installing them on local machine[22] .

II. COMPARATIVE STUDY

Due to security risks and issue in cloud computing, there is a strong need of authentication and authorization in cloud computing. Various authentication techniques and protocols exists provided by researchers all over the world. This paper provides literature survey of Various existing authentication protocols. A biometric based authentication scheme was given[23] to provide authentication of users based on elliptical key cryptography. In[24] a model was proposed that used the mathematical method to provide single server and two server Password based Authentication Systems, further multi-level authentication was proposed in [25]. A three step security system was given in [26] that used steganography and cryptography techniques .In [27] an ECC based authentication technique was proposed that used digital signature based identification. A light-weight authentication method was proposed in [28] as most of the existing one had higher computation cost. A lightweight authentication system was also proposed in [29] based on message digest and location .

A multimodal based biometric authentication method was developed in[30] ,using finger print and iris.

Table 1: Literature survey of various Authentication protocols in cloud computing

S.No.	Year	Author	Keywords	Proposed Method	Pros	Cons
1	2023	Linsheng Yu[31]	blockchain, authentication, mobile cloud computing	Authentication and authorization based on blockchain	efficient and scalable. Enhanced security of the mobile cloud computing	High storage overhead
2	2022	Kaur.Sandeep[32]	a novel one way hash, two factor authentication	ID Password OTP based verification Encryption using RSA , ECC	Survived MITM attacks, brute force attack, Account and session hijacking attack, replay attacks,	Not covered man In the middle attack
3	2022	Tsu-Yang Wu[33]	Cloud computing, IOT, SGX, authentication	Intel software-guard-extensions based authentication protocol	reduce communication cost by 7.07% in comparison with best existing algorithm	Computational cost is higher slightly
4	2022	Syed Amma Sheik[34]	ANN , Authentication ,Cloud computing	Cryptography using ANN	Survived various Malicious Attack	Only ANN is not enough to provide security in cloud computing
5	2021	Diksha Rangwani1 [35]	Cloud computing, authentication, ECC	ECC and irreversible hash function	Robust against replay attack, Man in the middle attack ,nearly all attacks, lightweight	N/A
6	2020	Abdelrahman Abuarqoub [36]	smart card, Dual factor authentication , Mobile cloud computing	Smart card based password verification	successfully survived various insider and outsider attacks	can be improved further to be used in IOT and various other industries
7	2020	Feifei Wang[37]	Authentication, IOT	IoT-based three factor authentication	Achieves three factor secrecy and resilient to offline guessing, session key disclosure, repay and various other attacks	N/A
8	2019	Ghassan O. Karame, [38]	data confidentiality, Key exposure	Bastion, which offers data confidentiality even at time of	Very small overhead	Good security with high throughput

				encryption key is leaked		
9	2019	Rafael Martínez-Peláez [39]	Cloud computing, mutual authentication, IOT	IOT based authentication scheme ,J.R.P.M. ,R.M.P., V.G,L.J.M.	Better computation and communication cost, Overcome user impersonation and replay attack	N/A
10	2018	Mylara Reddy Chinnaiah et.al., [40]	Cloud security, risk and issue, authorization	Fault tolerance technique: Characteristics & Frequency if interactions(ChIFrFT), Frequency of Configuration interactions(IFrFT)	Better than NOFT scheme achieves reliability and fault tolerance in cost efficient manner	Low successful interaction about(25-40%)
11	2017	Noelle Rakotondra vony et.al. [41]	VMI ,Malware	VMI based malware analysis	Focused on invention of target and direction of attack	Listed issues but less focus on their solution
12	2016	Punam V.Maitri & Aruna Verma Et.al. [42]	Stegnography, AES	LSB stegnography with use of RC6, AES ,BRA algorithm	Tried to provide high level of security using hybridization of public key. Focused on data integrity and low delay	Not able to provide high level of security
13	2015	Primoz cigoj et.al., [43]	Authentication	Single sign on (SSO) approach	Secure and strong authentication	It needs more flexible interfaces, It attempt to remove some vulnerability only
14	2014	Nitin Nagar &Pradeep K[44]	Authentication, LDAP	LDAP authentication	Provide a secure framework and helps in protection of user data	No focus on cloud computing tool for implementation
15	2013	Umer Khalid et.al., [45]	Authorization , Authentication	Anonymous Authentication & Authorization	Survived identity theft, leakage of data and integrated with the existing systems of identity management	N/A
16	2013	Kok-Seng Wong [46]	Biometric based authentication , cloud, authentication system	Voice iris, fingerprint etc are taken as credential input for authentication	Secure against malicious user and service provider	N/A

The above table shows Literature survey of various Authentication protocols in cloud computing.

III. RESULTS AND DISCUSSION

There are several research gaps in above authentication algorithms.

Standardization: Any standardize protocol does not exist for authentication in cloud computing environment that leads to interoperability between different cloud providers and users face difficulty to switch between providers.

Usability: Most of authentication and authorization protocols are complex and difficult to use, which leads users to error which in turn results in security issues.

Threat Model: Most of authentication protocols focus on a specific threat model ignoring other existing threat models, however all existing threat models should be given equal consideration.

Ease of use: the authentication protocols should be easy to understand with user friendly interface and complex one may irritate users.

Limited research on multi cloud environment: Most authentication protocol focus on a single cloud environment, however with the increase of multi-cloud environment there is a strong need to manage keys across multiple clouds.

Lack of focus on scalability: Many protocols are designed by keeping focus on small cloud environment, as the cloud environment scales up it is required for authentication protocols to meet demands.

So there is need of research in above discussed fields.

III. CONCLUSION

Authentication and key management protocols are essential for providing security in cloud computing environment. This paper provides a survey of various authentication protocols provided by various researchers present in this world. This paper also demonstrate various cloud computing models and types of services provided by them .This paper also points out various research gaps in the exhisting systems that needs to be focused in further research.

REFERENCES

[1] F. Li, H. Lu, M. Hou, K. Cui & M. Darbandi. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technol. Soc.*, 64(July), 101487. DOI: 10.1016/j.techsoc.2020.101487.

[2] D. Jiang. (2020). The construction of smart city information system based on the Internet of Things and cloud computing. *Comput. Commun.*, *150*, 158–166. DOI: 10.1016/j.comcom.2019.10.035.

[3] M. Amani *et al.*. (2020). Google earth engine cloud computing platform for remote sensing big data applications: A comprehensive review. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, *13*, 5326–5350. DOI: 10.1109/JSTARS.2020.3021052.

[4] S. Liu, L. Guo, H. Webb, X. Ya & X. Chang. (2019). Internet of things monitoring system of modern eco-agriculture based on cloud computing. *IEEE Access*, 7(c), 37050–37058. DOI: 10.1109/ACCESS.2019.2903720.

[5] H. Tabrizchi & M. Kuchaki Rafsanjani. (2020). *A survey on security challenges in cloud computing: issues, threats, and solutions*. Springer US. DOI: 10.1007/s11227-020-03213-1.

[6] N. Subramanian & A. Jeyaraj. (2018). Recent security challenges in cloud computing/ *Comput. Electr. Eng.*, 71(June), 28–42. DOI: 10.1016/j.compeleceng.2018.06.006.

[7] M. Faheem, U. Akram, I. Khan, S. Naqeeb, A. Shahzad & A. Ullah. (2017). Cloud computing environment and security challenges: A review. *Int. J. Adv. Comput. Sci. Appl.*, 8(10). DOI: 10.14569/ijacsa.2017.081025.

[8] R. Velumadhava Rao & K. Selvamani. (2015). Data security challenges and its solutions in cloud computing. *Procedia Comput. Sci.*, 48(C), 204–209. DOI: 10.1016/j.procs.2015.04.171.

[9] M. Ramzan, M. S. Farooq, A. Zamir, W. Akhtar, M. Ilyas & H. U. Khan. (2018). An analysis of issues for adoption of cloud computing in telecom industries. *Eng. Technol. Appl. Sci. Res.*, 8(4), 3157–3161. DOI: 10.48084/etasr.2101.

[10] M. F. Hyder, S. Tooba & Waseemullah. (2021). Performance evaluation of rsa-based secure cloud storage protocol using openstack. *Eng. Technol. Appl. Sci. Res.*, *11*(4), 7321–7325. DOI: 10.48084/etasr.4220.

[11] N. Subramanian & A. Jeyaraj. (2018). Recent security challenges in cloud computing. *Comput. Electr. Eng.*, *71*(December), 28–42. DOI: 10.1016/j.compeleceng.2018.06.006.

[12] Y. Xu, G. Deng, T. Zhang, H. Qiu & Y. Bao. (2021). Novel denial-of-service attacks against cloud-based multi-robot systems. *Inf. Sci. (Ny).*, *576*, 329–344. DOI: 10.1016/j.ins.2021.06.063.

[13] Maniah, E. Abdurachman, F. L. Gaol & B. Soewito. (2019). Survey on threats and risks in the cloud computing environment. *Procedia Comput. Sci.*, *161*, 1325–1332. DOI: 10.1016/j.procs.2019.11.248.

[14] B. Shunmugapriya & Dr. B. Paramasivan. (2020). Protection against SQL injection attack in cloud computing. *Int. J. Eng. Res.*, *V9*(02), 502–510. DOI: 10.17577/ijertv9is020273.

[15] L. Chunlin, T. Jianhang & L. Youlong. (2019). Hybrid cloud adaptive scheduling strategy for heterogeneous workloads. *J. Grid Comput.*, *17*(3), 419–446. DOI: 10.1007/s10723-019-09481-3.

[16] M. Talaat, A. S. Alsayyari, A. Alblawi & A. Y. Hatata. (2020). Hybrid-cloud-based data processing for power system monitoring in smart grids. *Sustain. Cities Soc.*, *55*(January), 102049. DOI: 10.1016/j.scs.2020.102049.

[17] G. Zhao, Y. Wang & J. Wang. (2023). Lightweight intrusion detection model of the internet of things with hybrid cloud-fog computing. *Secur. Commun. Networks*, *2023*. DOI: 10.1155/2023/7107663.

[18] A. Rashid & A. Chaturvedi. (2019). Cloud computing characteristics and services a brief review. *Int. J. Comput. Sci. Eng.*, *7*(2), 421–426. DOI: 10.26438/ijcse/v7i2.421426.

[19] M. Chnar & Z. Subhi. (2021). Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. *Sci. Bus.*, *5*9(2), 17–30. DOI: 10.5281/zenodo.4450129.

[20] V. Nandina, J. M. Luna, C. C. Lamb, G. L. Heileman & C. T. Abdallah. (2014). Provisioning security and performance optimization for dynamic cloud environments. *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 979–981. DOI: 10.1109/CLOUD.2014.150.

[21] F. Wulf, T. Lindner, M. Westner & S. Strahringer. (2021). IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection - Vignettes on the post-adoption of cloud computing. *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 6285–6294. DOI: 10.24251/hicss.2021.758.

[22] M. Saraswat & R. C. Tripathi. (2020). Cloud computing: analysis of top 5 CSPs in SaaS, PaaS and IaaS platforms. *9th Int. Conf. Syst. Model. Adv. Res. Trends, SMART 2020*, pp. 300–305. DOI: 10.1109/SMART50582.2020.9337157.

[23] G. J. W. Kathrine. (2018). A secure framework for enhancing user authentication in cloud environment using biometrics. *Proc. IEEE Int. Conf. Signal Process. Commun. ICSPC 2017*, pp. 283–287. DOI: 10.1109/CSPC.2017.8305854.

[24] D. Chattaraj & M. Sarma. (2018). Dependability quantification of cloud-centric authentication frameworks. *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 840–844. DOI: 10.1109/CLOUD.2018.00117.

[25] H. A. Dinesha & V. K. Agrawal. (2012). Multi-level authentication technique for accessing cloud services. *Int. Conf. Comput. Commun. Appl. ICCCA*. DOI: 10.1109/ICCCA.2012.6179130.

[26] V. K. Pant, J. Prakash & A. Asthana. (2015). Three step data security model for cloud computing based on RSA and steganography. *Int. Conf. Green Comput. Internet Things, ICGCIoT*, pp. 490–494. DOI: 10.1109/ICGCIoT.2015.7380514.

[27] L. Wang & T. Song. (2016). An improved digital signature algorithm and authentication protocols in cloud platform. *IEEE Int. Conf. Smart Cloud, SmartCloud*, pp. 319–324. DOI: 10.1109/SmartCloud.2016.46.

[28] J. Shen, D. Liu, S. Chang, J. Shen & D. He. (2016). A lightweight mutual authentication scheme for user and server in cloud. *1st Int. Conf. Comput. Intell. Theory, Syst. Appl. CCITSA*, pp. 183–186. DOI: 10.1109/CCITSA.2015.47.

[29] S. Dey, S. Sampalli & Q. Ye. (2015). A light-weight authentication scheme based on message digest and location for mobile cloud computing. *IEEE 33rd Int. Perform. Comput. Commun. Conf. IPCCC*, *1*, pp. 1–2. DOI: 10.1109/PCCC.2014.7017041.

[30] S. K. Khatri, Monica & V. R. Vadi. (2018). Biometrie based authentication and access control techniques to secure mobile cloud computing. *2nd Int. Conf. Telecommun. Networks, TEL-NET*, pp. 1–7. DOI: 10.1109/TEL-NET.2017.8343558.

[31] L. Yu, M. He, H. Liang, L. Xiong & Y. Liu. (2023). A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services. *Sensors*, *23*(3), 1264. DOI: 10.3390/s23031264.

[32] S. Kaur, G. Kaur & M. Shabaz. (2022). A secure two-factor authentication framework in cloud computing. *Secur. Commun. Networks*, pp. 7540891. DOI: 10.1155/2022/7540891.

[33] T. Y. Wu, L. Wang, X. Guo, Y. C. Chen & S. C. Chu. (2022). SAKAP: SGX-based authentication key agreement protocol in iot-enabled cloud computing. *Sustain.*, *14*(17), 1–19. DOI: 10.3390/su141711054.

[34] S. A. Sheik & A. P. Muniyandi. (2022). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. *Cyber Secur. Appl.*, *1*, pp. 100002. DOI: 10.1016/j.csa.2022.100002.

[35] D. Rangwani & H. Om. (2021). A secure user authentication protocol based on ecc for cloud computing environment. *Arab. J. Sci. Eng.*, *46*(4), 3865–3888. DOI: 10.1007/s13369-020-05276-x.

[36] A. Abuarqoub. (200). D-FAP : Dual-factor authentication protocol for mobile cloud connected devices †. pp. 1–23.

[37] F. Wang, G. Xu, G. Xu, Y. Wang & J. Peng.

(2020). *A robust iot-based three-factor authentication scheme for cloud computing resistant to session key exposure*.

[38] K. Lichota, S. Capkun, G. O. Karame & C. Soriente. (2019). Securing cloud data under key exposure. *IEEE Trans. Cloud Comput.*, *7*(3), pp. 838–849. DOI: 10.1109/TCC.2017.2670559.

[39] R. Martínez-Peláez *et al.* (2019). An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances. *Sensors (Switzerland)*, *19*(9). DOI: 10.3390/s19092098.

[40] C. Mylara Reddy & N. Niranjan. (2018). Fault tolerant software systems using software configurations for cloud computing. *J. Cloud Comput.*, *7*(1). DOI: 10.1186/s13677-018-0104-9.

[41] N. Rakotondravony & H. P. Reiser. (2016). Visualizing and controlling vmi-based malware analysis in IaaS cloud. *Proc. IEEE Symp. Reliab. Distrib. Syst.*, pp. 211–212. DOI: 10.1109/SRDS.2016.035.

[42] P. V. Maitri & A. Verma. (2016). Secure file storage in cloud computing using hybrid cryptography algorithm. *IEEE Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET*, pp. 1635–1638. DOI: 10.1109/WiSPNET.2016.7566416.

[43] P. Cigoj & B. J. Blažič. (2015). An authentication and authorization solution for a multiplatform cloud environment. *Inf. Secur. J.*, *24*(4–6), 146–156. DOI: 10.1080/19393555.2015.1078424.

[44] N. Nagar & P. Jatav. (2014). *A secure authenticate framework for cloud computing environment*.

[45] U. Khalid, A. Ghafoor, M. Irum & M. A. Shibli.(2013). Cloud based secure and privacy enhanced authentication & authorization protocol. *Procedia Comput. Sci.*, *22*, 680–688. DOI: 10.1016/j.procs.2013.09.149.

[46] K. Wong & M. H. Kim. (2013). *Secure biometric-based authentication for cloud*, pp. 86–101.