ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

A Broad Review on Data Authentication Systems in Cloud Computing

Preeti Kushwaha[1] , Prof. Satpal Singh[2]

M.Tech. Scholar, Department of Computer Science &Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science &Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: Cloud technology has revolutionized the landscape of computing in the last decade. Benefits such as reduced costs, rapid application deployment, and elastic resources, have enticed many organizations to utilize cloud resources or host much of their data in the cloud. Recent studies have shown that over 70 percent of the world's businesses now operate at least some of their operations in the cloud, with many more expected to join in the coming years. In the past, security concerns deterred many organizations from using cloud computing services. In this paper a review of three critical cloud security threats is discussed, with the purpose of determining if the new widespread adoption of cloud computing is due to advances in security. The review revealed that although new security technologies have been introduced, many issues concerning the three threats are still present today. Because of this, continued widespread adoption of cloud computing will likely increase compromises until innovative techniques are created to address cloud computing threats

KEYWORDS*:* Cloud Computing, Distributed Computing, Data Security, SaaS, PaaS, IaaS.

I. INTRODUCTION

Cloud computing is the deliverance of computing resources on the internet. In the cloud, we can store data and use services on a remote computer rather than our own computer hard drive. With cloud services, individual and business organization utilize programming and equipment that are overseen by outsiders at remote places. Cloud administrations cases can be online document stockpiling, person to person communication destinations, webmail, and online business applications. The distributed computing model enables access to information, data and PC assets from anyplace with a system association. Distributed computing gives a common pool of assets, including information storage room, systems, PC handling power, and concentrated corporate and client applications. Distributed computing is a compensation for each utilization display for empowering access, and simple and on-request arrange access to a common asset of processing assets configurable as systems, servers, sparing assets, projects, and administrations that can be set up with a fast. The accompanying meaning of distributed computing has been created by the U.S. National Institute of Standards and Technology (NIST):

Cloud computing is a model for empowering advantageous, on-request organize access to a common pool of configurable registering assets (e.g., systems, servers stockpiling, and administration exertion or specialist organization cooperation. This cloud model advances accessibility and is made out of five basic attributes, three administration models, and four organization models.[1]

Cloud computing," basically, signifies "Web Computing."
The Internet is generally imagined as mists; consequently the expression "distributed computing" for calculation done through the Internet. With Cloud Computing, clients can get to database assets by means of the Internet from anyplace, for whatever length of time that they require, without agonizing over any support or administration of real assets. Also, databases in the cloud are exceptionally powerful and adaptable. The best case of distributed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

computing is Google Apps where any application can be gotten to utilizing a program and it can be sent on a great many PC through the Internet.

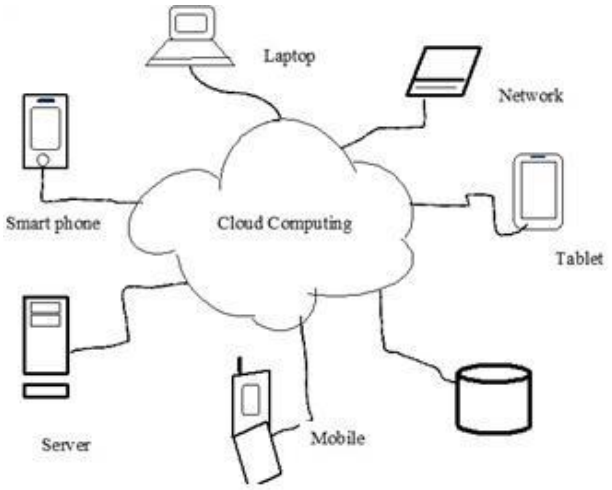

Figure 1. Cloud Computing [2]

1.1 Applications

Various applications of cloud computing are:

Business: Big Organization does business on cloud environment rather than using traditional infrastructure that was time-consuming and requires lots of space, hard work, power, and management. Users now browse their catalog and add them to the shopping cart and submit their order.

Education: Education is one the most vital requirement of current status. With cloud computing, education is delivering to each person quickly, securely, reliably and economically. Cloud computing in education opens the better option for research, discussion, and collaboration. Classes run on a remote location with cloud computing.

Online Entertainment: Consumer can entertain using online entertainment with cloud computing. Users can access games, News, Audio and Videos using Cloud computing. It provides on-demand storage and computing services to be pay per usage.

Telecommunications: Business organization can access their business using telecommunication services in cloud computing like smartphone business applications like Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) System. These Services can access from any location and linked into current services.

Finance and Banking: With the growing international market easy access to finance and banking is the basic need of the market. Cloud computing provides a platform for international business through online banking and Financial Services. This provides a quick and better option for business.

1.2 Threats in Cloud

Data Breaches: When an association's touchy interior information falls under the control of their rivals, an information rupture happens.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

Data Loss: Data misunderstands into hands while exchanging or be lost because of the hard drive disappointment.

Account Hijacking: An assailant accessing our record can control and change the information.

Insecure Application Program Interface: An aggressor picking up a token utilized by a client to get to the administration through administration API can utilize a similar token to control the client's information.

Denial of Service: Forestall clients of a cloud benefit from having the capacity to get to their information or their applications.

Malicious Insiders: Malicious insider danger to an association is a present or previous representative, temporary worker, or different business accomplice working at cloud specialist co-op , who has or had approved access to an association's system, framework, or information and deliberately surpassed or abused that entrance in a way that contrarily influenced the classification, trustworthiness, or accessibility of the association's data or data frameworks.

1.3 Some Examples of Cloud

Amazon's Elastic Computing Cloud (EC2) offering computational administrations that empower individuals to utilize CPU cycles without purchasing more PCs.

Storage administrations, for example, those gave by Amazon's Simple Storage Service (S3).Companies like Nirvanix enabling associations to store information and archives without including a solitary site server.

SaaS organizations like Salesforce.com conveying CRM administrations, so customers can oversee client data without introducing particular programming.[3]

II. TYPES OF CLOUD

Private Cloud: Private cloud is constrained to a particular group of persons and organization and only accessible to them. This type of cloud provides more security and control over resources.

Public Cloud: In the public cloud, any subscriber can access the cloud with an internet connection. So, in public cloud computing resources are accessed by the general public or organizations. This type of cloud has no control over the resources and less security over the confidential data.

Community Cloud: Community cloud is shared by more than two organization with similar cloud requirements. It is managed by a third party or the organization. It provides services to vast users as compared to private cloud and provides more security in contrast to the public cloud.

Hybrid Cloud: In Hybrid cloud an organization use resources from the private cloud as well as the public cloud. For normal use an organization access resources from the private cloud but a sudden increase in the use of resources handled by the public cloud for the purpose of scalability and cost-effectiveness.[3]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

III. CLOUD SERVICES MODEL

Cloud Services can be classified into three types:

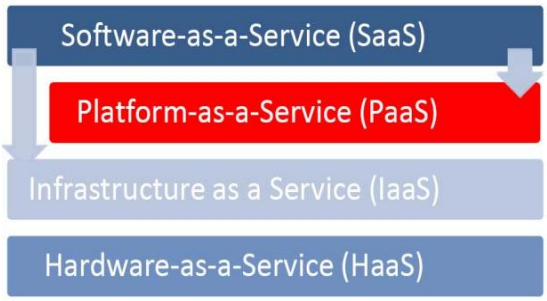

Figure 2. Cloud Services

Software as a Service (SaaS): This model provides different software required by the cloud users for performing various operations. Users access the application via a thin client interface using Web Browser. The users only make payment as per the usage of the software such as Microsoft Word, Notepad, Paint and various other applications. Various providers of SaaS are ZOHO, Google, Intuit, and Salesforce.com etc.

Platform as a Service (PaaS): In this model Platform like Operating System is given to users as a service. Users develop their own application and installed on cloud environment using Integrated Development Environment (IDE), which include a compiler, editor, build and deploy capacity.Force.com, Google App and Bungee Connect are examples for PaaS.

Infrastructure as a Service (IaaS): In this model, infrastructure is provided to the cloud user as a service such as Storage area, servers, and networks. The consumer hires these resources on the basis of their needs and pays only for use. The consumer has control over the operating system and deploys the application, however, does not oversee or control the framework of the cloud. Amazon Elastic Compute Cloud (EC2) and EMC Atmos are examples for IaaS.[4]

IV. LITERATURE SURVEY

Kai Fan et al. [5] puts forward a productive and solid RFID security validation plot in cloud condition. The convention consolidates the rationale encryption operation with a timestamp, which can oppose DoS assaults and hostile to synchronization assaults. Radio Frequency Identification (RFID) makes it a supporting innovation for the Internet of things (IoT). RFID has been generally utilized and grown quickly. With the advancement of distributed computing, cloud-based RFID framework has turned into another arrangement. Ensuring the security of RFID framework in cloud condition is especially essential. Not checking the tag or per-user when perusing message, will have genuine results, which may endure many security issues, for example, block, adjusting, replaying, DoS and synchronization. The proposed convention not exclusively can well illuminate the RFID security and protection issues, yet additionally can utilize the intense distributed computing abilities to process information.

Mohamed M. Zarad et al. [6] proposed a proficient and provably secure confirmation component to give an honest to goodness client the privilege to get to and deal with the cloud assets. The proposed authentication scheme, and key agreement protocol have been proved to be more secure and efficient than other authentication schemes. Since using the small key size of Elliptic Curve will improve the authentication process due to fast processing of the keys. Using AES-256 as an encryption algorithm protects the data exchange between the user and the server from various attacks. ECC will enhance the computational efficiency and enhance the usage of available storage resources which make it an efficient choice as the authentication protocol for cloud computing.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

Sara Alfatih Adam et al. [7] identifies the security issues of single-level authentication and the problem of a single and password. This study proposed a novel security technique for cloud computing based on multilevel verification. The planned scheme aimed to increase the security and authentication procedure in cloud computing. The planned
method comprises of three level of authentication, and the data will be splitting on this level depending on the sensitivity to confidential (C), secret (S), and top secret (TS). Data at level (C) have the lowest sensitivity. The user at this level has the single textual password to access this level data The user at level (S) has two passwords, textual and biometrics password to access this level and the lower level. A user at level (TS) has three passwords textual, biometrics password and image sequencing password. The data at this level is the more sensitive data so it is encrypted using RSA algorithm before storing in a cloud database. The results of the proposed multilevel authentication for cloud computing were promising.

Nalini S et al. [8] use multilevel authentication schemes to provide access to users in the cloud. Authentication is verified on the basis of rights given to the users. Cloud client can be a consumer, Data Owner and admin. Data owner can make changes in cloud data using password and biometric and NTP Server timestamp. Users have a right to download files basis on a token given to them that are valid for some time period. Cloud Admin maintains users on the basis of their password, fingerprints along with 64 bits NTP timestamp. Authors propose an extended 128 bits NTP timestamp for enhancing authentication in the cloud.

Basel Saleh Al-Attab et al. [9] proposes a brand new sturdy scheme for cloud computing authentication by using USB token with a combination of hash feature and Diffie- Hellman key trade. In latest years, because of the large increase in the usage of various services furnished by way of the cloud computing, there have been such a lot of issues and demanding situations confronted the cloud computing companies. Most of these are associated with a way to comfortable the user authentication that's visible as a core requirement for the cloud computing device the personal authenticating information of person will become at risk of a selection of attacks like password guessing, denial of service (DOS), replay, man-in-the - center, insider, and so forth. As an end result, there was a huge variety of techniques and strategies proposed to save such assaults and offer enough security for the user authentication within the cloud system. Yet, some of the problems along with mutual authentication, verification, and the impossibility of freely password change still continue to be unsolved. Therefore, there is a must to provide a strong person authentication scheme to solve such issues. The proposed scheme is so at ease and powerful because it attains the necessities of functionality and security.

Lo'aiTawalbeh et al. [10] used the concept of a secure cloud computing based on data classification and apply TLS, AES & SHA based on the security level of data. It enables the client to encode claim information utilizing a key that isn't accessible for the supplier. To promote programmed information arrangement and diverse cryptographic calculation, for example, asymmetric key, RSA, and Elliptic curve use to enhance the security and confidentiality.

Akanksha Upadhyaya et al. [11] provides the more control of proprietor on the information put away on the cloud by confining the entrance to a particular client for particular document with constrained benefits and for restricted day and age on the premise of mystery key utilizing symmetric and in addition asymmetric(AES) system. Integrity and confidentiality of data are achieved by giving access permission by read, write and execute permission and limiting file information using lock period and secret code.

Atulay Mahagan et al. [12] analyze the problem of insider threats has been and various detection and formation procedures are used to solve these malicious insider threats. Security enhances by giving notice as a pop-up gap that shows the content of file have been transformed by the side of the list of changes too and using One-time Password(OTP) to the respective user on their registered e-mail.

Qutaibah Athhebyan et al. [13] exhibited a model that took care of the insider risk issue in a cloud server farm. This paper utilized an information chart for every insider and received a Fat Tree as Cloud Data Center Architecture that recognized a few insiders (Host, Aggregate and Core insider). This paper exhibited the insider risk location/anticipation show at having a level of cloud server farm. In this paper, the proposed calculation is acquainted

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

with recognizing/anticipate vindictive insiders' exercises at various levels. This calculation will guarantee that insider learning won't increment as far as possible.

Manpreet Kaur et al. [14] discussed the issues associated with statistics region, storage, security, availability, and integrity. Establishing believe is the way to triumph over those protection problems as it establishes entities courting quick and accurately. Cloud computing is a trendy era that is being extensively used all around the international. Once the company takes the decision to transport to the cloud, it loses manipulate over the information. Thus, the amount of protection needed to cozy facts is at once proportional to the price of the records. Security of the Cloud is based on trusted computing and cryptography. Numbers of cloud systems are to be had now in instructional in addition to in firms circle.

Varsha et al. [15] Cloud computing is an enormous prospect both for the organizations and the assailants – every gathering be equipped to have their own one of a kind reward from distributed computing. Interminable chances of distributed computing can't be concealed just for the security issues reason – the unending assessment and concentrate for strong, typical and included security models for distributed computing is presumably the main course of the proposition. In view of this reality that the effect of security issues in distributed computing can be lower with the aid of multi- tenancy architecture.

P. Shenbagam et al. [16] used a combination of "Persuasive Cued Click-Point", "Alphanumerical authentication", "Sound Signature" and "Draw – a secret " method system to conquer the issue of ease of use and security. This improves the security by giving a transitory message to a telephone while going into the framework. It is consolidating graphical watchword, content, draw a mystery strategy and telephone message for information security in the cloud.

Faraz Fatemi Moghaddam et al. [17] offers an effective and adaptable client confirmation plot for distributed computing condition. It the proposed show, different devices, and methods have been presented and utilized by utilizing the idea of a specialist. Thusly, a customer based client verification specialist has been acquainted with affirm personality of the client in customer side. Moreover, a cloud- based programming as-a-benefit application has been utilized to affirm the procedure of verification for unregistered gadgets. Besides, there are two separate servers for putting away verification and cryptography assets from primary servers to diminish the reliance of client validation and encryption forms from the fundamental server. Cryptography operator was additionally acquainted with scramble assets before putting away on cloud servers. In generally speaking, the hypothetical examination of the proposed plot demonstrates that planning this client confirmation and access control model will upgrade the unwavering quality and rate of trust in distributed computing conditions as a developing and effective innovation in different ventures.

Rajarshi Roy Chowdhury et al. [18] said around assurance dangers and issues in different segments, which incorporates CIAA and issues identified with different administration conveyance models alongside: DoS, people group well-being, records security and territory in SaaS styles, group and host interruption in PaaS and IaaS not just contemplated in which measurements is being spared and way yet additionally included the media of realities switch is being utilized over the Internet. Alleviation of dangers and inconveniences are the critical a piece of this paper wherein characterized the suitable way to lessen perils comprising of to uphold right motivate admission to oversee, checking, inspecting and a couple of in vogue information wellbeing component. At long last, give a few clues in light of writing an assessment on various papers in current years. Along these lines, distributed computing isn't generally developing enough, thusly numerous instructional looks into and ventures are exchanging towards to distributed computing condition. Cloud innovation is still now in the cloud for clients.

Tunisha Saxena et al. [19] Cloud Computing has transformed the software program support for big systems from the server to provider oriented paradigm. This goes with the flow has evolved new demanding situations for layout and transport of offerings over heterogeneous necessities and environments. This brings approximately risks and demanding situations for structures. The device over the net is liable to performance and protection risks. The overall performance is a composite evaluation, however, risks which are related to privacy may be dealt with at distinct

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

degrees of abstraction in the cloud version. This paper addresses the safety dangers and demanding situations and analyzes the available measures to address.

Iehab ALRassan et al. [20] proposes and executes another client verification instrument of versatile cloud PC utilizing a unique finger impression acknowledgment framework. Unique mark pictures of the versatile client can be caught and process utilizing a cell phone camera to get to portable distributed computing. In this paper, the creator proposed to get to log document which will help in recognize unapproved endeavors to get to information by outsiders the cloud supplier or any gatecrasher.

Ni Zhang et al. [21] gives a review of distributed computing security. To clear up cloud security, a definition and extent of distributed computing wellbeing are displayed. A surrounding of cloud security is demonstrated to show what each capacity in big business can do this. At that point, security influences of cloud security for the two customers and administrators are broke down. To triumph over difficulties from cloud security, numerous advanced specialized arrangements, e.g., continuation assurance system, IDM, measurements wellbeing, and virtualization security are said. At long last, pleasant practices on edge of the administrator are condensed and an end is performed.

Sushmita Ruj et al. [22] underwrites another privateness holding validated get right of passage to oversee plot for securing data in mists. In the planned conspire; the cloud confirms the validness of the purchaser without knowing the client's character sooner than putting away records. This plan moreover has the acquainted capacity to getting passage with overseeing in which best substantial clients are equipped to decode the put-away certainties. The plan averts replay assaults and helps presentation, adjustment, and perusing insights spared inside the cloud. Besides, validation and gain section to power conspire is decentralized and solid, rather than various motivate admission to control plans intended for mists which can be brought together. The discussion, calculation, and capacity overheads are likened to brought together strategies.

Wentao Liu et al. [23] displays some circulated processing structures and analyses conveyed registering security bother and its system as demonstrated by the disseminated figuring musings and characters. The data assurance and provider availability in conveyed registering are the key security trouble. Single security approach cannot clear up the circulated figuring protection issue and a lot of conventional and new innovation and methodologies should be utilized all things considered for guarded the aggregate distributed computing gadget.

Santosh Kumar et al. [24] investigate cloud design and contrasts distributed computing and lattice processing. This paper likewise manages the attributes and projects of various well known distributed computing frameworks. This paper focuses to pinpoint the requesting circumstances and issues of distributed computing. They recognized various difficulties from the distributed computing reception edge and moreover featured the cloud interoperability inconvenience that benefits broad likewise studies and improvement. Be that as it may, insurance and privateness issues blessing a tough hindrance for clients to adjust to distributed computing structures. This paper look at variously distributed computing gadget bearers roughly their worries on insurance and protection issues.

Amlan Jyoti Choudhury et al. [25] proposes a solid individual confirmation system for distributed computing, where individual authenticity is firmly tried before contributing to the cloud. Distributed computing is a mix of assorted processing substances, all around isolated, and however electronically connected. As the topography of calculation is drawing nearer to corporate server rooms, it brings more inconveniences comprehensive of security, alongside virtualization assurance, apportioned figuring, application wellbeing, recognizable proof administration, get right of the section to control and validation. In any case, hearty individual confirmation is the central necessity for distributed computing that point of confinement unlawful gets right of the section to of cloud server. The proposed system gives recognizable proof control, common verification, counsel key foundation between the clients and the cloud server. A customer can exchange his/her watchword, each time requested. Moreover, wellbeing examination understands the possibility of the proposed system for distributed computing and accomplishes proficiency.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

Qian Wang et al. [26] inspected the issue of giving synchronous open auditability and information stream for remote information respectability check-in Cloud Computing. This progression is purposely wanted to meet these two essential goals while the benefit is being recalled nearly. To complete fit information development, they enhance the present verification of breaking point models by controlling the commendable Merkle Hash Tree headway for square name endorsement. To help practical treatment of various minding assignments, they likewise explore the system of the bilinear total stamp to grow our focal outcome into a multiuser setting, where TPA can play out different assessing errands in the meantime. Wide security and execution examination display that the proposed design is exceedingly profitable and provably secure.

Rabi Prasad Padhyet et al. [27] diagrams what circulated registering is the diverse cloud models and the rule security dangers and issues which can be by and by blessing inside the distributed computing industry. This examinations paper furthermore investigates the key examinations and troubles that gives in conveyed registering and gives magnificent practices to pro communities and furthermore wanders wanting to utilize cloud transporter to enhance their back line on this uncommon money related climate.

Cong Wang et al. [28] propose an assurance defending open assessing framework for information gathering security in Cloud Computing. They use the homo-morphic authenticator and subjective covering up to ensure that TPA would not take in any getting some answers concerning the information content set away on the cloud server amidst the profitable exploring process, which not just wipes out the largeness of cloud client from the dull and conceivably costly evaluating errand, yet moreover encourages the clients' dread of their outsourced information spillage. Considering TPA may at the same time oversee diverse review sessions from various clients for their outsourced information chronicles, they besides develop our security saving open evaluating convention into a multi-client setting, where TPA can play out the different breaking down errands in a gathering course, i.e., meanwhile. Sweeping examination demonstrates that the proposed plans are provably secure and uncommonly powerful.

Kai Hwang et al. [29] Trust and protection have avoided companies from totally tolerating cloud stages. To secure mists, sellers need to first casual virtualized insights center assets, maintain individual protection and keep measurements honesty. The creators propose the utilization of a trust-overlay group over two or three records offices to actualize a prominence contraption for sorting out consider among specialist organizations and records proprietors. Information shading and programming program watermarking procedures protect shared realities devices and enormously administered programming program modules. These strategies defend multi-way validations, empower single flag on in the cloud, and fix motivate section to oversee for touchy records in both open and individual veils of mist.

TABLE 4.1 COMPARISON OF TECHNIQUES

Ref.	TECHNIQUE PROPOSED	FINDINGS	LIMITATIONS
[5].	RFID security validation plot in cloud condition.	Proposed the RFID security and protection issues, and utilize the intense distributed computing abilities.	The proposed convention cannot exclusively illuminates the security and protection issues.
[6].	AES-256 an encryption algorithm	Proposes an efficient and secure authentication scheme.	Larger key size increases encryption and decryption time.
[7].	Multilevel authentication.	Enhances the security and authentication process.	Time consuming process.
[8].	An extended 128 bits NTP timestamp.	Using Password, biometric and Timestamp for enhancing authentication in the cloud.	An additional 128 bit Time stamped is need to be processed.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

[9].	USB token with a combination of hash feature and Diffie- Hellman key trade.	Detection and prevention of malicious insiders' activities at different levels.	Some of the problems along with mutual authentication, verification, and the impossibility of freely password change still continue to be unsolved.
[10].	Secure cloud computing based on data classification and apply TLS, AES & SHA based on the security level of data.	It enables the client to encode claim information utilizing a key that isn't accessible for supplier.	An additional data classification activity is an overhead.
[11].	Secret key using symmetric as well as asymmetric (AES) mechanism.	Integrity and confidentiality of data are achieved.	Secret code can be hacked.
[12].	Detection and formation procedures to solve malicious insider threats.	Security enhancement by sending notification and One time Password (OTP) to registered email ID of the user.	Focused only on malicious insiders threats.
[16].	"Persuasive Cued Click-Point", "Alphanumerical authentication", "Sound Signature" and "Draw – a secret" method system.	Enhances the security by providing an impermanent message to a telephone while going into the framework.	Similar Sound Signature can be reproduced by un authorised person.
[20].	Mobile cloud computing authentication using fingerprint recognition system.	Reorganization of unapproved endeavors to get to information by maintaining a log file.	Mobile device must have finger a print scanner.
[22].	Attribute-based encryption and Signature scheme for securing information in clouds.	The scheme prevents replay attacks and helps introduction, modification, and reading statistics saved inside the cloud.	The discussion, calculation, and capacity overheads are linked.
[25].	A solid individual confirmation system for distributed computing.	The proposed system gives recognizable proof control, shared confirmation, meeting key foundation between the clients and the cloud server.	Focused only on distributed computing gadget, their worries on insurance and protection issues.
[26].	Open audit ability for remote information checks in Cloud Computing.	Broad security and execution investigation.	Additional information required about system.
[28].	Homomorphic authenticator with random masking.	Proposed high security and execution efficiency.	Expensive

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

V. CONCLUSION

In this paper, a review of various data authentication schemes in cloud computing is presented. Cloud computing is a technology that offers computing services on the internet. Companies providing these services are called Cloud Service Providers. Cloud computing condition gives an extraordinary adaptability and accessibility of figuring assets at a lower cost. However, it brings new security concerns mainly when users understand exactly how a process is running. One of the main important challenges in cloud computing is data security, as users need to access data they share securely. So the main problem is how to employ an effective authentication procedure for ensuring data security and preventing unauthorized users to access the authorized user's data. Authentication is one of the main important challenges in the security of cloud computing. Single level authentication has many problems mainly with sensitive data, as passwords are easy to break. Various data authentication schemes are presented in this report. The different phrasings and ideas were completely looked down and in this way clarified.

REFERENCES

[1] N. Hemalatha, A. Jenis, Cecil Donald, L. Arockiam, "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing ", International Journal of Computer Applications (0975 – 8887) Volume 96– No.16, June 2014
[2] J. Kashifa khurshid1 & p. Thenmozhi " an analysis of deployment models in cloud computing" International Journal of Management, Information Technology and Engineering (BEST: IJMITE) ISSN (P): 2348-0513, ISSN (E): 2454-471X, Vol. 4, Issue 3, Mar 2016, 89-98
[3] Karandeep Kaur, "A Review of Cloud Computing Service Models", International Journal of Computer Applications (0975 –8887) Volume 140 –No.7, April 2016
[4]Supriya Mandhare, Ass. Prof. Rajkumar Shende, An Intelligent approach for data fortification in Cloud Computing", 2014 International Conference on Advances in Communication and Computing Technologies.
[5] Kai Fan, Qi Luo, Hui Li, Yintang Yang, "Cloud-based Lightweight RFID Mutual Authentication Protocol", IEEE Second International Conference on Data Science in Cyberspace, 2017, pp. 333-338.
[6] Mohamed M. Zarad, Ahmed A. Abdel-Hafez, Ahmed H.Hassanein, "Secure and Efficient Authentication Scheme for Cloud Computing", International Journal of Computer Applications, Volume 142 – No.8, May 2016, pp. 19-24.
[7] Sara Alfatih Adam , AdilYousif, Mohammed Bakri Bashir, "Multilevel Authentication Scheme for Cloud Computing", International Journal of Grid and Distributed Computing, Vol. 9, No. 9, 2016, pp.205-212.
[8] Nalini. S, Dr. J. Andres, "MLA Scheme: Multi-Level Authentication for in cloud using NTP-server and biometric" IEEE International Conference on Computational Intelligence and Computing Research,2016.
[9] Basel Saleh Al-Attab, H. S. Fadewar, "Authentication Scheme for Insecure Networks in Cloud Computing", IEEE International Conference on Global Trends in Signal Processing, Information Computing and Communication,2016, pp. 158-163.
[10] Lo'ai Tawalbeh1, * Nour S. Darwazeh2, Raad S. Al- Qassa2 and Fahd AlDosari 1 , "A Secure Cloud Computing Model based on Data Classifcation" in International workshop on Mobile Cloud Computing System, Management and Security(MCSMS-2015)
[11] Akannksha Upadhyaya, Monika Bansal, " Deployment of Secure Sharing: Authenticity and Authorization using Cryptography in cloud Environment", in International Conference on Advances in Computer Engineering and Applications(ICACEA-2015
[12] Attulay Mahajan, Sangeeta Sharma, "The Malicious Insider Threat in the Cloud", in International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015.
[13] Qutaibah Althebyan, Rami Mohawesh, QussaiYaseen and YaserJararweh, "Mitigating Insider Threats in Cloud Using a Knowledgebase Approach while Maintaining Data Availability, in the 10th International Conference for Internet Technology and Secured Transactions(ICITST-2015).
[14] Manpreet Kaur, Hardeep Singh, "A REVIEW OF CLOUD COMPUTING SECURITY ISSUES", International Journal of Advances in Engineering & Technology, June, 2015, Vol. 8, Issue 3, pp. 397-403.
[15] Varsha, Amit Wadhwa, Swati Gupta, "Study of Security Issues in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue.6, June 2015, pg.230 – 234.
[16] P. Shenbagam1, C.Namasivayam2, "4 Level Authentication Security in Cloud Computing", in International Journal of Innovative Research in computer and Communication Engineering, Vol.2, Special Issue 1, March 2014.
[17] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", IEEE, 2014, pp. 508-513.
[18] Rajarshi Roy Chowdhury, "Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 96– No.15, June 2014, pp. 24-30.
[19] Tunisha Saxena, Vaishali Chourey, "A Survey Paper on Cloud Security Issues and Challenges", IEEE 2014.
[20] Iehab AL Rassan, Hanan Al Shaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security and its Application (IJNSA), Vol.5, No.6, November 2013.
[21] Ni Zhang, Di Liu, Yun-Yong Zhang, "A Research on Cloud Computing Security", IEEE 2013 International Conference on Information Technology and Applications, pp. 370-373.
[22] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp. 556-563.
[23] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE 2012, pp. 1216 – 1219.
[24] Santosh Kumar, R. H. Goudar, "Cloud Computing –Research Issues, Challenges,Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012, pp. 356-360.
[25] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", IEEE Asia -Pacific Services Computing Conference, 2011, pp.110-115.
[26] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011, pp. 847-859.
[27] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology &Security (IJCSITS) Vol. 1, No. 2, December 2011, pp. 137-146.
[28] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM, 2010, pp. 1-9.
[29] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE 2010.