# A SURVEY ON SECURITY BREACHES OF DATA AVAILABILITY AND DATA INTEGRITY IN CLOUD COMPUTING

*R. Santhosh, Amrutha Muralidharan Nair**

**Abstract**

The new concepts of the distributed system, the user requires a large storage space for their data. So, cloud computing is the place of interest of the age and due to its exciting possibilities and disastrous affect the performance, protection and ethics, it is the brand new acute region of situation to groups. Clients relieve their data storage and maintenance pressure locally by transmitting it over the web. While the client doesn't have permission to the data directly from the server physically, without the awareness of the client, the cloud provider can change or erase data that is either not needed for a long time by the client or that consumes large space. Thus, for correction purposes there is a need to review the data periodically; reviewing data for error is called data honesty. Alternatively, cloud computing idea, provide a latest safety and protective mechanism, which is being constructed towards all threats type of problems or a community of malicious attacks which affect cloud computing's excellent of provider. Unlike standard DoS attacks, LRDOS attacker periodically injects fast continuous traffic. It causes rather poor latency TCP connections for the sender to timeout. These attacks are hard to detect and eliminated since high-rate traffic triggers most DoS threat detection systems. This paper introduces the survey of accessible strategies to identify LRDoS attacks and also examined numerous existing systems for auditing data integrity along with their risks.

**Keywords :** Data Integrity, Availability, Cloud architecture

## I. INTRODUCTION

Cloud computing has seen to be a revolutionary form of layout of records structures. It is a cost-effective computational system in which equipment and facilities are operated in a remote location. This makes the infrastructure in the cloud more volatile and vulnerable to instability at all network, server, device and flow rate of data. The cloud is defined as "a global resource pool" that can be spread with minimal management effort such as network, storage, server, apps and services." [1]. Cloud computing has so many features and benefits that enable people and businesses turn into this new concept.

Features are listed below [2]:

Flexibility: Different users can easily access or add resources of their own if they require it.

Data pooling: All the cloud carrier issuer's computing resources are pooled together to help cloud customers and the use of either multitenancy or virtualization [3]. In this feature the services are distributed and reassigned according to the user needs.

Wide network access: Heterogeneous devices such as mobile phones, tablets and PDA's are accessible on the network via the internet.

In computing, different service models are available. Users in the cloud can choose any applications those run on any platform. This program is accessible by different clients from different location. Sources are: Document provided by google (Google Docs)

Department of Computer Science and Engineering,
Karpagam Academy of Higher Education, Coimbatore Tamilnadu, India
*Corresponding Author

SaaS "Software as a Service": It gives customers less leverage over the network which optimizes the performance, repair and management after accidents.

PaaS "Platform as a Service": The user has the provision to install their own or any software in the cloud without accessing the client system providing the underlying platform required for it. PaaS is a SaaS development platform, including cloud services and apps. Therefore, the SaaS and PaaS protection specifications are interrelated. [4].
Example: Application by Google (Google Apps) and Search Engine,

IaaS "Infrastructure as a Service": Infrastructure service offers distinct form of resources together with storage, hardware, servers and networking. This is utilized by user. It allows the consumers of the cloud to operate some program that might include operating systems and programs. [2]. The network can be extended and reduced dynamically whenever needed by the user. [4].
Example: Simple Storage Services (S3) and Amazon Elastic Cloud Computing

DaaS "Data Storage as a Server": It helps user to compensate the data about "what they currently need instead of the app authorization, technology and application they need" [3]. DaaS provides an easier and faster table layout than conventional RDBMS.
Example: Amazon S3, Apache HBase, Google BigTable.

The four different kind of cloud deployment are:

Private Cloud: The cloud that is deployed, managed by a corporation in or off terms or by a additional party [2] [3]. An enterprise has complete cloud power, which in turn will make the cloud more robust and safe in its network's operations, the cloud infrastructure can leverage the organization's IT capabilities to their maximum extent.

Community Cloud: Many organizations have same features, security requirements and practices shared in cloud. It can be managed on-site or off-site [2] [3].

Public Cloud: This is available to all the users which offers different cloud services. The Service Provider itself decides the strategies, interest, benefit and expense. The data placed in the cloud service provider i.e. datacenter and the service provider are having the responsibility for managing and providing security [3].

Hybrid Cloud: It is the synthesis formation of at least two or more architectures. Organizations can leverage core talents by means of handing over peripheral enterprise features on the public cloud even as handling on premise key activities via private cloud.

In this paper, two main threats arising in cloud computing were reviewed. Those are availability of data such as DDoS attack and determining and preventing integrity of data such as replay attack. The paper is organized in different section which is described below. Section II explains issues related to cloud computing. Section III gives detail description of threats affecting availability and integrity. Section IV reviews the different data availability and data integrity proving and maintaining schemes. Section V concludes the work.

## II. ISSUE REDARING CLOUD SECURITY

Throughout cloud computing, the security issues have a significant effect. The cloud allows the data to be accessed remotely. Loading and processing of cloud information provide ability to transmit information on various servers located in diverse countries those have different rules[5]. However, multi-tenancy and capital pooling can make corporate knowledge insecure.

A. Security Parameters

Availability: On request, the data which is in the form of

any pattern that is residing in a location remotely ,should be made available to the authorized people. It will secure its customers' information .

Integrity: Integrity ensures that only authorized entities can change information assets[2]. Data Integrity applies to data protection from erasure or alteration. Cloud service companies must insure no unauthorized parties gain access to the system and can change or erase user data and compromising the system's credibility.

Confidentiality and Privacy: It applies to the idea that only authorized parties may access confidential or secured cloud information. It can maintain confidentiality by interpreting a strong authentication and also duty of the cloud provider to ensure user data privacy. Any disagreement in the privacy dissemination may be influenced by the area where the individual cloud service operates by local regulations. [2]
Authentication: It's the technique to ensure the conversations of the participants are authentic. To provide Authentication, the digital signature [6] is the best example. These are often used to insure that the parties of the correspondence do not repudiate the encrypted records or transactions. The non-repudiation means that a writer does not dispute the validity of a paper which he has created or sent.

## III. DETAIL DECRIPTION OF THREATS AFFECTING AVAILABILITY AND INTEGRITY

A. Data availability

Cloud computing has caught the eye of many research bodies as well as many businesses, owing to its capacities and cost-effectiveness [7]. High availability is crucial factor in cloud computing. Data availability includes that authorized consumers access cloud resources and services, depending on their demands [8]. Nonetheless, due to its platform multi-tenancy and its collaboration features , data security and service quality challenges may compromise cloud environment. The Distributed DoS attack is the toughest one among the security threats though there are good service in cloud computing. This assault prevents legal web customers from access to the cloud providers' infrastructure or resources [9]. This is achieved by draining the server's computing resources by overwhelming the network bandwidth which ultimately leads to cloud services or facilities becoming inaccessible and resulting in massive financial loss [10]. Current DoS security structures expect an attack in form of packet flow, however low-Rate DoS intrusion is undetected and may display and manage the system's vulnerabilities [11]. Most systems follow RFC2988[12] hints which h render synchronization which is impossible, whereas working structures with lower RTO values are still at risk of an attacker. The focus is on malicious LRDoS traffic which exploits TCP's RTO to preempt TCP traffic flows. The low-rate TCP-targeted DoS attacks are affecting external domain routing at the net in these days [13].

LRDoS attack: In LRDoS assault attacker regularly sends out brief packet bursts to overload the queue of a router and allow the legitimate users to lose their packets. A well-behaved source of TCP [14] can return to get over congestion and retransmit by using one time RTO. When, at retransmission periods, the intruder congests the network, so the real user traffic cannot get through it. Therefore, Attacker may essentially shut down the most valid TCP sources by reordering the attacking time rather considering the RTO time. Periodic square wave is one form of attack.

B. Data Integrity

Cloud storage systems provide the ability for the customer (data owner) to store, back up or preserve their domain in the data storage network. These implementations can guarantee long-term data integrity and availability. This goal involves the creation of adequate verification of remote ownership of data. The overall network model for processing

cloud data is shown in the Figure 1. In this figure, it contains three different components which are described as follows:
Client: This is the front end users who is dependent on the virtual session of the cloud for data storage and use the cloud services to execute and process their data.

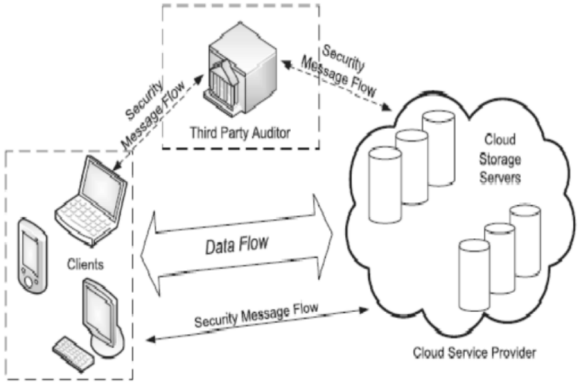


**Figure 1: Cloud network Architecture [18]**

Cloud Storage Server: It provides data storage facilities by the CSP (Cloud Service Provider), and has good sized storage capacity to store the data and process.
Middle Party Auditor known as TPA: An external agent with experience and skills will not be available to users, is authorized to evaluate and disclose the vulnerability of open access cloud storage services. Client or third party inspector may be the verifier.

## IV. REVIEW OF DIFFERENT DATA AVAILABILTY AND INTEGRITY PROVIDING SCHEMES

Ari Juels and Burton S. Kaliski [15] define the concepts "Proof of retrievability", in which they have attached the concept of error-correcting codes and spot-checking are considered to provide guarantee for "possession" and "recoverability" of stored data files on archive storage networks. Actually, for security purposes, some special blocks are labelled as "sentinels" which is arbitrarily inserted in data file F. This variable “F” is again undergoes an encryption to shield the location of this specific blocks of the packet. Furthermore, their system does not support the public audit ability.

Shacham, H. and Waters, B. [ 16] have developed an enhanced feature of PoR concepts for the completely described safety proofs. They use homomorphic authenticators which is publicly verifiable and produced from BLS signatures on the idea of which the proof may be aggregated right into a minimal authenticator meaning and the target audience's retrievability is completed. Nevertheless, the developers find only static data files.
R. Curtmola , et al [17] were the first to establish the new concept of “data possession provable " technique which allows public auditing to guarantee the ownership of information on untrusted storage server in cloud. It uses “Homomorphic Verifiable Tags” for conducting audit of data of their system. Author advised a dynamic variation of the prior PDP system issues. This system implements a priori the quantity of queries and does not take delivery of totally dynamic data.

Y. Zhu, et al [18] were the first to investigate constructions for the collections of complex proven data. The author has expanded the specified model [8] to add the feature of provable changes to store data in cloud using authenticated skip lists by considering the grades. In fact, this method is a completely interactive variant of the model Dpp solution after the removable of the indexed information in the "link" computation in G. Ateniese's, et.al Dpp model [17].

Xiang et al [19] proposed a concept of trace back and detection of low rate DDos type of attacks with a simplified entropy and related knowledge. It considers the common entropy difference between legitimate traffic and the low-Rate DDoS attacks traffic which suggest that the metric exceeds the entropy created by Shannon method. Though the length difference can be changed by adjusting $\alpha$, there is still a slight gap in distance.

Haibin Sun et al [20] define a tracking mechanism which is mounted by considering few nodes away from the victim's location on a series of routers. Growing router will detect an attack at the exit port and forward towards the victim's site. The TCP packets are observed to occur in low rate, the router needs to decide the ports of origin from which the threat traffic is sent. There is a low-rate threat traffic that is detected by using pushback technique to categorise the assault. The pushback feature minimizes the quantity of TCP flows which might be impacted.

M. H. Bhuyan et al.[21] suggested a light weight metric-based expanded "entropy" method for identification of DDoS attacks and traceback of IP. This new entropy metric is modified one to generalize entropy in for obtaining a larger distance than the metric . Nevertheless, because of the intrinsic constraint of entropy the gap is still limited.

Rodriguez et al[22] provide a combination of fuzzy logic with Hop tracking process to make it more effective in detecting the time-series packet arrival data. The mechanism MAD runs on measured time series and identify attacks faster than the "P-A-D", that depends on the nearest periodic existence of the data packet .

## V. CONCLUSION

This review provides the significance of cloud computing in this paper and its security issues. A new data sharing trend of cloud computing is leading up new security issues. This new paradigm demands that a third party agent verifies the quality that is data stored. It is observed that researchers are recommended with powerful new structures for integrity which is focused on the above schemes. PdP scheme supports the complex activity, where PoR scheme does not supports complex activity. Even though the PdP scheme does not contain error correction code, where as PoR contains error correction code. So many quantities are contained inside the PoR scheme which arises from error correction codes. Hence, it can be conclude that growing powerful, safe and completely dynamic remote information integrity spaper that various identification and prevention methods exist to prevent LRDoS Attack network which is a kind of DDoS attack. This helps to provide a simple understanding about the strategies necessary for LRDoS assault detection. It also highlights the problems that are present in LRDoS detection methods currently available. Existing identification methods are far from realistic effective solution.

## REFERENCES

[1] P. Mell and T. Grance,"The NIST definition of cloud computing", NIST special Publication, 2011. [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues" journal home page: www. Elsevier.com/locate/fgcs available online: 22 December 2010

[3] Tharam Dillon, Chen Wu, Elizabeth Chang "Cloud Computing: Issues and challenges" 2010 4th IEEE International conference on Advanced Information Networking and Applications

[4] Hoanh T. Dinh, ChonhoLee, Dusit Niyato and Ping Wang "A survey of mobile cloud computing: architecture, application and approaches" Published online 11October 2011 in Wiley Online Library Wireless Communication and mobile computing 2013

[5] Younis a Younis, Madjid Merabti and Kashif Kifayat "Secure cloud Computing for Critical Infrastructure: A Survey" MYA Younis, K Kifayat - Liverpool John Moores University, United Kingdom, 2013 - cms.livjm.ac.uk

[6] William Stallings., Cryptography and Network Security-Principles and Practice, 5th Edition. Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall.

[7] U. Oktay and O. K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing," 6th Internatıonal Informatıon Securıty & Cryptology Conference, vol. 9, pp. 71–76, 2013.

[8] J. Varia, "Best practices in architecting cloud applications in the AWS cloud", Cloud Computing. Principles and Paradigms, John Wiley & Sons, Inc. Jan 2011, pp. 459-490.

[9] K. C. Okafor, J. A. Okoye, and G. Ononiwu, "Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective," International Journal of Computer Applications, vol. 138, no. 7, pp. 18–30, 2016.

[10] G. Somani, M. Singh, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer. Communications., vol. 107, pp. 30–48, 2017.

[11] Gabriel Macia-Fernandez, Jesus E.Diaz- Verdejoand Pedro García-Teodoro, "Evaluation of a low-rate DoS attack against iterative servers", Department of Signal Theory,University of Granada, c/Daniel Saucedo Aranda, s/n, 18071 Granada, Spain (2006)

[12] Computing TCP's Retransmission Timer—RFC 2988

[13] A.Kuzmanovic and E. Knightly, "Low-Rate TCP - Targeted Denial of Service Attacks (The Shrew vs.the Mice and Elephants)", Proc. ACM SIGCOMM pp. 75-86 ( 2003)

[14] Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants In: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications Pages: 75 – 86 Year of Publication: ISBN: 1-58113-735-4 (2003)

[15] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584– 597.

[16] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[17] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598– 609

[18] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data possession for Integrity Verification in Multi Cloud Storage", vol. 23, IEEE Trans. Parallel and Distributed Systems, no. 12, pp. 2231-2244, 2012.

[19] Y. Xiang, K. Li, and W. Zhou, "Low rate DDoS attacks detection and traceback by using new information metrics," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 426–437, 2011.

[20] Haibin Sun, John C.S. Lui, David K.Y. Yau, "Defending Against Low rate TCP Attacks: Dynamic Detection and Protection", Proceedings of the 12th IEEE International Conference on Network Protocols (2004)

[21] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "ELDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric," Security and Communication Networks, vol. 9, no. 16, pp. 3251–3270, 2016.

[22] J.C.C.Rodriguez, A.P. Briones and J.A.Nolazco, "Dynamic DDoS Mitigation based on TTL field using Fuzzy logic", CONIELECOMP '07, Mexico (2007)