International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206667

Data security and integrity in cloud computing : Threats and Solutions

Rajesh Keshavrao Sadavarte[1], Dr. G. D. Kurundkar[2]

[1]Assistant Professor and Head, Netaji Subhashchandra Bose College, Nanded, Maharashtra, India

[2]Assistant Professor, Computer Science Department, Shri. Guru Buddhiswami Mahavidyalaya, Purna District Parbhani, Maharashtra, India

Author Correspondence : sadavarte2003@yahoo.com, gajanan.kurankar@gmail.com

Article Info
Volume 6, Issue 6
Page Number: 356-363
Publication Issue :
November-December-2020

Article History
Accepted : 15 Dec 2020
Published : 30 Dec 2020

ABSTRACT

Cloud computing changed the world of Internet. With the help of cloud computing user can easily share, store and retrieve their data from anywhere. Cloud computing is scalable, fast, flexible, and cost-effective technology platform for IT enabled services over the internet. Cloud computing provides hardware, software and infrastructural storage to many users at a time Most of the times cloud users don't know the exact location of their data or the sources of data stored with their data. In spite of various benefits that are provided by the cloud computing services, its users are very much afraid about the security of their data once it is over the cloud under the control of third-party vendors. Therefore, many data security and integrity concerns like access control, searchable encryption techniques, key management, ownership proofs and remote integrity check arise.

This paper discusses the security and integrity of data in cloud computing. It is a study of aspects related to data security. The paper will go in to details of few data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Going ahead the paper also discuss different techniques used for secured data storage on cloud.

Keywords : Cloud Computing, Cloud security, Security techniques, Security threats, Data security

I. INTRODUCTION

Cloud computing is an emerging technology in the field of networking. It is gaining popularity in all areas. The National Institute of Standards and Technology (NIST)[1] defines cloud computing as a model for enabling ubiquitous,convenient, on-demand network access to a shared pool of configurable computing resources. In simple words cloud computing is a computing model in which resources are provided to the users based on their demand. In cloud computing resources are provided by the cloud service provider known as CSP.

Cloud computing is the combination of many pre-existing technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take benefit from all

these technologies. Many organizations are moving into cloud because it allows the users to store their data on cloud and can access it at anytime from anywhere[2].

Cloud computing now is everywhere. In many cases, users are using the cloud without knowing they are using it. According toSubashini&Kavitha, small and medium organizations will move to cloud computing because it will support fast access to their application and reduce the cost of infrastructure[3]. The Cloud computing is not only a technical solution but also a business model that computing power can be sold and rented. Cloud computing is focused on delivering services. Organization's hugedatais hostedincloud for saving memory and getting quick accesibility. Though effective in its own way, in this system ownership of the data is decreasing while agility and responsiveness are increasing.In cloud computing, user's data is stored on remote servers owned and operated by third parties and accessed through the internet. Moreover this data may be stored with a single provider or multiple providers[4].

Organizations are now seeking to stop focusing the IT network. In order to maximize productivity they must concentrate on their business process. Therefore, cloud computing is becoming increasingly relevant, becoming a strong market and attracting much interest from academic and industrial communities. Cloud computing can be represented scematically as follows:

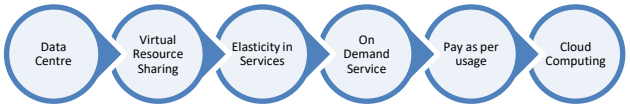


Figure 1 : Schematic definition of cloud computing[4]

However, cloud computing suffers from various security issues as data owners store their data on external servers, increasing demands and concerns for privacy protection, authentication, and access control have been raised.Cloud security is becoming a core differentiator across cloud providers giving them a competitive edge. Despite the various advantages provided by the cloud computing platforms, cloud computing service customers are very afraid of their data protection because it is managed by third-party providers in the cloud.

II. METHODS AND MATERIAL

1. Data security in cloud

In the current scenario, the data that needs to be stored is passed on to the remote service provider and the owner himself is not aware of the location of the data which raises a security concern. Thus data security, proof of ownership and recovery period and data protection becomes a prime issue to be addressed in the cloud data migration process. When it comes to cloud data security, no particularly new methods are required. Protecting data in the cloud environment is same as protecting it within a traditional data center. Encryption, access control, authentication and identity, data masking, secure deletion, and integrity checking are all data protection methods that areapplied in cloud computing.

One more security problem is the recovery period of the data at the time of disaster.It depends on the storage provider managing the data in the event of a disaster that could occur due to vulnerabilities on the cloud due to remote hard drive failures [6]. The provider handles a customer's crucial and confidential data and does not necessarily guarantee data confidentiality, protection and trust.According to the author of the paper the top threats to cloud computing are: abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious

insiders, shared technology issues, information loss or misuse, hijacking of account or operation and uncertain risk profile [5].

a) **Data Privacy:**Continuous data expansion leads to several security issues where data privacy is one of the security challenges associated with cloud computing. Cloud computing 's privacy challenges include the uncertainty associated with risk management, increasing market demands the advent of timely deployment of innovative business models and their effect onspecific regulatory compliance, customer privacy, data protection concerns in design leading to lack of clarity and poor data quality. Data privacy protocols apply to data and software communication protocols , data processing protocols impact data privacy mostly in cloud[8].

b) **Data Integrity:**Data integrity is useful for data authenticity, and guarantees data consistency and reliability as well. Lack of credibility is a big challenge in the cloud world, because of data privacy problems, there are many security threats and attacks. Data integrity ensures that the data is not modified or altered without the knowledge of the user. When the intruder or unauthorized person has control to the stored data , data privacy is at stake. The user data can be attacked by data modification, Tag forgery attack and data leakage attack. Monitoring data integrity is important to prevent data manipulation and data crashing in cloud providers.Various mechanisms are adopted to prevent cloud environment data integrity attacks such as cooperative provable data possession (CPDP), which combines hash indexing hierarchy and homomorphic verifiable response[9].

c) **Data Trust:**Trust is the key concern but mostly breaks if two issues are not handled properly one of them is lack of clarity and another is due to security and privacy infringement.Cloud service providers provide flexibility in the usage of services that attract cloud computer consumers to benefit from the service by putting their sensitive data at riskConsumers are unknowing of the technologies involved and data control, since they rely entirely on agreements and the trust process. Trust is a complex term and is based on someone else's positivebehavior or approach .Trust is dependent on the security the cloud service provider provides its clients with. Indeed, reputation plays an significant role in building trust in the relationship between cloud provider and cloud customer. Additionally, security processes must be propagated through the business process[10].Trust will be improved if the cloud provider separates the data avoiding breaching the security and privacy of the multi-tenant framework. Transparency in data storage and trying to conceal unnecessary user information will build a level of trust and understanding between cloud provider and the consumer.

2. Cloud security issues

Even though cloud computing undoubtedly provides substantial cost savings and greater effectiveness for companies, it also introduces new security challenges and uncertainty. It is definitely not easy to protect and ensure the safety of linked devices, as a variety of machines and customers are involved; this is known as multi-tenancy. Cloud service providers and cloud computing have many challenges to face, especially in security concerns. Therefore, it's quite important to understand how to mimic these problems and how to incorporate security models in order to ensure client security and create a secure cloud computing framework. The most significant threats to cloud computing are described as follows [5][6]

Lack of appropriate governance: The owner of the software has full autonomy throughout cloud computing. By handing this power to the vendor, there is a danger that the lack of control over authority criteria may result in security being

breached, leading to data access problems and resource utilization.

Data breaches: The next most effective step is to prevent data violations. The difficulty in tackling data retention and data leakage challenges is that "the steps you put in place to boost one will make the other worse". Data is encrypted to minimize a violation 's effect, but if the key to encryption is lost, then the data is lost. If data backups are chosen offline to reduce data loss, even then, exposure data breaches are boosted.

Data Loss/Leakage: There are many ways to compromise data due to insufficient authentication, authorisation and audit (AAA) checks, such as deleting or altering records without the original content being backed up. Loss of an encoding key can cause productive destruction. Unauthorized parties can gain access to data. A hacker could delete data from a target[13].

Data interception: Unlike conventional computing data is segmented and distributed in transit in cloud computing. This poses further risks because of the weakness and vulnerability of the computer technology and, in particular, sniffing and spoofing, attacks by third parties and response attacks [7].

Insecure Application Programming Interfaces APIs:APIs are integral to the security of general cloud services and their availability. These interfaces must be designed to protect against both malicious and accidental efforts.Unknown access and/or interchangeable tokens or login details, clear-text verification or content transmission, inflexible access restrictions or unsuitable authorizations, restricted monitoring and logging capabilities; are examples of this form of threat.

Malicious insiders:A vendor may not disclose how it enables employees to access physical and virtual assets, how it monitors such employees, or how it analyzes them. In cloud computing the organization does not need to know the technical aspects of the delivery of the services. The risk is high in situations. Your company can be at risk without the complete information and control.

Unknown risk Profile: Software versions, software policy , code modifications, and implementations, bug assessments, attempts to intervene and system architecture are all significant considerations in determining the security status of a organization. Knowledge on who uses the network is relevant.

Shared Technology Issues: (IaaS) is based on the shared infrastructure (e.g. disk partitions, CPU caches, GPUs, etc.) wasn't really configured to have efficient multi-tenant system insulation properties.A hypervisor for virtualization mediates the connection between guest operating systems and the physical computing infrastructure. Ignored vulnerabilities have allowed guest operating systems to access unauthorized control rates and/or command on network.

Other challenges Security-related concerns include the sharing of knowledge in different cloud computing applications, information disclosure when transferring data to the cloud, privacy and device data protection threats, misuse or unauthorized exploitation of encryption keys, and disputes between service providers and consumers about protocols and cloud computing systems operating policies. [8].

3. Data security solutions

a) Data Integrity:

In any information system data integrity is one of the most critical elements. Data integrity usually requires the security of data against unwanted fabrication, deletion or alteration . Due to the large number of entities and access points in a cloud environment, authorization is critical in ensuring that only authorised personnel are able to interact with informationBy preventing unauthorized entry, organisations can have greater trust in the integrity of data. Cloud platforms providers are committed to the

integrity and accuracy of dataNevertheless, beyond customers and cloud service providers, the third party supervisory system must be established. The perquisite for installing software is to remotely check the validity of data in the cloud.Bowers et al . suggested a technical system for "Proofs of Retrievability" to undertake remote data security assessments by incorporating error correction code with spot inspection. The HAIL system uses POR method to verify data storage in various clouds, so it can ensure the consistency of multiple copies so conduct the quality and validity search. Schiffman et al .suggested trusted platform module (TPM) to remotely test integrity of the data [16].

b) Data Confidentiality

Privacy and security of data is crucial for users to store their private or confidential information in the cloud.To ensure security of the records, authentication and access control techniques are used. Cloud storage could resolve authentication , data security and access control problems by increasing cloud trustworthiness and reliability .Owing to the non-trustworthy cloud service providers (CSP), confidentiality may also be compromised. Better encryption techniques will guarantee confidentiality. There are essentially two distinct approaches to confidentiality: cryptography and physical isolation[17].

Some techniques to enhance confidentiality are:

Biometric encryption (BE): Biometric data can be kept secret by biometric encryption which includes fingerprints iris, face recognition ,voice recognition etc.

Secret sharing scheme : This system is associated for the approach of public sector hybrid cloud computing. This is accomplished through the implementation of a stable, fully automated data storage and cloud transfer protocol between cloud storage suppliers and customers.

Dataobfuscation: In this we combine the obfuscation with the encryption. Obfuscation utilizes a cryptographic function or to disguise unauthorized users using programming techniques. The methodology depends on the data form. Encryption may be extended to alphabets, alphanumeric data types and numeric data obfuscation.

HPI_Secure: This helps the user to store the authenticated version of the data in the cloud, without breaking the system's functionality. Httprequests and answers are detected and data is encrypted before being transmitted to the cloud and decrypted after reception. This method makes use of disassociation and encryption to increase data confidentiality.

Encryption and trust based solution: This approach aims to maintain confidentiality by allowing CSUs to 1) encrypt sensitive data and check authentication from start to end, 2) determine CSP's confidentiality, 3) decide whether to authorize CSPs to conduct different computing services based on their security mechanisms.

K-NN classifier for data confidentiality :This methodology categorizes the data to be stored on the basis of their security standards, such as what data require securitynd which data doesn't require security . This is done using classification scheme K-NN. Data can be classified into sensitive and non-sensitive classes. The RSA algorithm applies to sensitive data while non-sensitive data is stored as it is. [10].

c) Data Availability

: when incidents such as hard disk destruction, IDC fire, and network errors occur, the degree to which customer data can be accessed or retrieved and how users validate their data using methods rather than relying solely on the Cloud storage provider's credit guarantee. There are two ways of ensuring availability of the data.

Reliable Storage Agreement: To support concurrent modification by multiple users, a good storage agreement is required. SPORC, proposed by Feldman et al. [19],That can enable secure and reliable real-

time connectivity and multi-user collaboration with the aid of a trustworthy cloud network and untrusted cloud servers could only access encrypted information.

Reliability of Hard-Drive: Hard-drive is currently the primary cloud storage media. Hard disk durability constructs the foundation of cloud storage[10].

d) Data Privacy

Privacy in the cloud ensures as users access confidential data, the cloud providers may prohibit possible adversaries from inferring the actions of the customer through the user's visit model (not actual data leakage).Researchers have concentrated on Oblivious RAM (ORAM) technology. ORAMtechnology encounters several copies of information to cover up visiting purposes of users. ORAM has been widely in use in software security and being used as a capable technology to protect cloud confidentiality.Stefanovetal suggested a state-of-the-art version of the ORAM route algorithm[21].Data protection issues vary according to different cloud situations and can be resolved using:

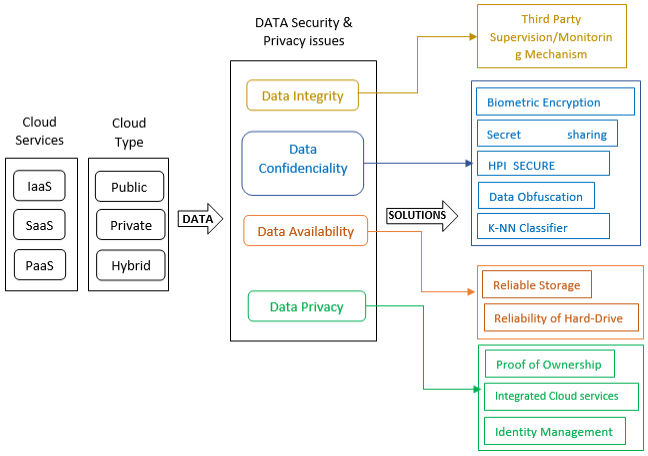
Proof of ownership: This method is suggested by C. Cachin and M Schunter to test Cloud app authentication[22].

Identity Management:A probable solution to this issue may be using a reliable impartial third-party strategy to Identity Protection to use identity data on untrusted networks.

Integrated Cloud Services: Shen et al . propose combining Trusted Computing Platform (TCP) and Trusted Application Support Services (TSS) cloud services to achieve the desired privacy of data[23].

III. FRAMEWORK

According to the above study, the cloud environment, the security issues and the solutions proposed can be formulated in the same way as shown in the following framework.



IV. CONCLUSION

Cloud computing is an emerging and promising technology for IT application to upcoming generation . Data security and integrity problems are the barrier and obstacles to the rapid growth of cloud computing.Any entitiy cannot transfer their data or information into the cloud before the relationship between cloud service providers and customers is established. Researchers have suggested a variety of data protection strategies and to achieve the highest degree of cloud information security. We presented in this paper an overview of data security and integrity issues in the current scenario of cloud platform. The purpose of this survey was to highlight the security problems associated with cloud computing and to present some solutions proposed / implemented by researchers to improve security and integrity. We have been able to build a system that poses security issues as well as potential solutions for the same. Paper discussed issues and challenges relating to cloud security. The paper also discussed and presented the proposed and effective Data Security solutions through a framework. However, by making these techniques more effective there are still many gaps to be filled. More research in the field of cloud computing is needed to make it appropriate for users of the cloud service.

V. REFERENCES

[1]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology,Vol.53,no.6, p. 50, 2009.

[2]. A. Venkatesh and . M. . S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," International Journal of Scientific Research in Computer Science, Engineering and Information Technology , IJSRCSEIT , vol. Volume 3, no. Issue 1, pp. 2456-3307, 2018.

[3]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. Vol 34, no. Issue 1, pp. 1-11, 2011.

[4]. H. Tianfield, "Security Issues In Cloud Computing," in IEEE International Conference on System, Man, Cybernetics, Seoul, Korea, 2012.

[5]. M. T. Khorshed, A. S. Ali and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation Computer Systems, vol. Vol 28, no. No. 6, pp. 833-851, 2012.

[6]. A. Shawish and M. Salama, "Cloud Computing: Paradigms and Technologies, F. Xhafa and N. Bessis (eds.), Intercooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence," Studies in Computational Intelligence, p. 495, 2014.

[7]. P. Sirohi and A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust.," 1st International Conference on Next Generation Computing Technologies (NGCT), 2015.

[8]. C. Sarvankumar and C. Arun, "Survey on interoperability, security, trust, privacy standardization of cloud computing," in Contemporary Computing and Informatics, 2014.

[9]. A. Jaberi and M. F. Zainal, "Data integrity and Privacy model in cloud computing," Biometrics and Security Technologies, pp. 280-284, 2014.

[10]. S. Pearson and A. Benameur, "Privacy, Security and Trust Isseus Arising from Cloud Computing," in 2nd IEEE International Conference on Cloud Computing Technology and Science, 2010.

[11]. Bob Violino , "CSO India: 11 top cloud security threats," 11 October 2019. Online]. Available: https://www.csoonline.com/article/3043030/top-cloud-security-threats.html. Accessed 06 May 2020].

[12]. N. A. AL-SAIYD and N. SAIL , "DATA INTEGRITY IN CLOUD COMPUTING SECURITY," Journal of Theoretical and Applied Information Technology , vol. Vol 58, no. ISSN: 1992-8645 , 2013.

[13]. G. Kulkarni, J. Gambhir, T. Patil and A. Dongre, "A security aspects in cloud computing," in IEEE International Conference On Computer Science and Automation Engineering, 2012.

[14]. H. Shah and S. S. Anandane, "Security Issues on Cloud Computing," arXiv preprint arXiv:1308.5996., 2013.

[15]. V. Winkler, "Securing the cloud: Cloud computer security techniques and tactics.," NL: Syngress Media Incorporated. , 2011.

[16]. S. Basu, A. Bardhan , K. Gupta , P. Saha, M. Pal and M. Bose , "Cloud computing security challenges & solutions - A survey," in IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018.

[17]. M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and Privacy in Cloud Computing:A Survey," in Sixth International Conference on Semantics, Knowledge and Grids, 2010.

[18]. H. Yusuf and S. Selvan, "Confidentiality Issues in Cloud Computing and Countermeasures: A Survey," in National Conference On Emerging Computer Paradigms 2016, NMAMIT, Nitte, 2016.

[19]. A. J. Feldman, W. P. Zeller, M. J. Freedman and E. W. Felten, "SPORC:group collabration using untrested cloud resources," in Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation(OSDI'10), 2010.

[20]. S. Yunchuan , Z. Junsheng, X. Yongping and Z. Guangyu, "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks, 2014.

[21]. E. Stefanov, M. vanDijk and E. Shietal, "Pathoram:an extremly simple oblivious ram protocol," in Proceding of the ACM SIGSAC Conference on Computer & Communications Security, 2013.

[22]. C. Cachin and M. Schunter, "Ac cloud you can trust," in IEEE Spectrum, 2011.

[23]. Z. Shen, L. Li, F. Yan and X. Wu, "Cloud computing system based on trusted computing platform," in Proceddings of the international Conference on Intelligent Computation Technology and Automation(ICICTA'10), 2010.

[24]. M. AlZain, E. Pardede, B. Soh and J. Thom, "Cloud computing security: From single to multi-clouds," 45th Hawaii International Conference , p. 5490–5499, 2012.

Cite this article as :

Rajesh Keshavrao Sadavarte, Dr. G. D. Kurundkar, "Data security and integrity in cloud computing : Threats and Solutions", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 356-363, November-December 2020. Available at doi : https://doi.org/10.32628/CSEIT206667
Journal URL : http://ijsrcseit.com/CSEIT206667