International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Issues and Challenges in Data Integrity and Data Storage Security in Cloud Computing

***Miss. Ankita Singh*[1], *Mr. Vedant Naidu*[1], *Prof. Deepali Shah*[2]**

[1]MCA Semester-VI, Sterling Institute of Management Studies, Nerul, Navi Mumbai
[2] Asst. Professor(MCA), Sterling Institute of Management Studies, Nerul, Navi Mumbai
ankitasingh0999@gmail.com

ABSTRACT-

Cloud Computing is providing service like servers, database management, data storage, networking, software applications, etc. to the client on demand. Data storage is one of the most widely used service provided by cloud computing. Cloud service provider hosts the data of the owner on their server, and it can be accessed by the owner from these servers whenever they want. As owners and servers are different identities, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper we will discuss about the integrity of data stored, challenges faced to secure the data and techniques used to secure data storage in cloud.

Keyword: Cloud Computing, Data integrity (DI), Cloud Security and Data Security

Introduction

Cloud Computing in delivery of computing services to individuals and businesses over the internet. Cloud services allow them to utilize system software and hardware that are managed by the cloud providers and allow them to access them anywhere, anytime through internet. Examples of cloud services contain online file storage, webmail, social networking sites, online business applications. Many companies, organizations as well small entrepreneurs are moving into cloud because it provides great services in cheap rate and it is reliable as well. Cloud providers provide only that amount of services that user has asked and charges only for that. Because of services provided by cloud the user do not have to install their own hardware and software and servers as well. It saves energy and money of the users. However big responsibility comes with bigger risks, Data breaching is possible in cloud environment since data from various users and organizations lie together in cloud. As the user not only sends data to the cloud but also transfers controls to a third person which may raise concern about its security. The major task of CSP (Cloud Service Provider) is to preserve the confidentiality, integrity, and availability of data to the users. But sometimes the CSP itself may use or corrupt the data illegally. However, to overcome this the user simply can encrypt the data before uploading it onto the cloud. This will make sure that the data uploaded is not visible to external users or the cloud administrator. However, it has limitations too that plain text-based searching algorithm are not applicable. In this paper, we discuss the security algorithms that can be used to keep the data secure and maintain its integrity.There have been arguments between police departments and some members of the public regarding the use of the device on both technical and constitutional perspectives. Therefore, this paper discusses the topic to establish the best course that should take to end dissatisfaction from the public and ensure road safety.

Literature Review

Cloud computing is “an old idea whose time has (finally) come” [2]. The term cloud is old since it was drawn in network diagrams as a metaphor representing the Internet [4]. Cloud computing is generally referred to as providing “Internet-based computing service” [2]; however, the technical meaning is richer, as cloud compu- ting builds on already-existing computing technologies, such as grid computing and virtualization, which are forms of distributed computing technology [9]. Virtualization involves masking the physical characteristics of computing resources to hide the complexity when systems, applications, or end users interact with them. Grid computing is “a model of distributed computing that uses geographically and admin stratify distant resources, and, thus, users can access computers and data transparently without concern about location, operating system, and account administration”. With the advent of cloud computing, the merits of virtualization and grid com-putting have been combined and further improved. Cloud computing shares some characteristics with virtualization and grid computing; however, it still has its own distinguishing characteristics as well as associated risks

Problem Definition

The main concern is to protect security against unauthorized access of data. Data relocation on high level has negative implications for protecting the data safety and data security as well as data accessibility. Therefore, the main apprehension with reference to safety of data residing within the Cloud is: at the remainder how to safe security and avoid authorization. Even though, customers understand the situation and no data mobility access, question with reference to security and confidentiality of data. The Cloud Computing area has no confusion become larger as a result of its accessibility and wide network access. However, we can also believe in terms of a secure and safe atmosphere for the personal data and information of the user is being needed

Objective

Cloud Computing allows the users to store their data on the storage location maintained by a thirdparty. Once the data is uploaded into the cloud the user loses its control over the data and the data can be tampered by the attackers. The attacker may be an internal(CSP) or external. Unauthorized access is also a common practice due to weak access control. The protection of information arises the following challenges: The security and privacy issues related to data storage are confidentiality, integrity and availability.The cloud computing of the security elements is detailed about Data Integrity, Data confidentiality, Data availability, and Data privacy. In this paper explain the detail explanation about security elements of cloud computing as given below.

Research Methodology

Data integrity is considered one of the most critical security elements in several information systems. In general, data integrity means that protecting data from unauthorized modification process, fabrication or deletion. Managing entity's rights and access to specific enterprise resources ensures that important data and services are not abused, illegal access, or stolen. Data integrity is definitely achieved in a standalone system with a single database. Data-integrity in the standalone system is maintained through database transactions and constraints, which is frequently finished by a database management system (DBMS). Transactions ought to follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. The majorities of databases are to support ACID transactions and can protect data integrity. Data integrity in the cloud system means that protecting information integrity. The data should not be modified or lost or by unauthorized users' access. Data integrity is the basis to give cloud computing service like SaaS PaaS, and IaaS. Moreover, data storage of large scaled data, cloud computing environment typically provides data processing service. Data integrity can be obtained by using these techniques like digital signature and RAID-like strategies.

Data Confidentiality: - Data confidentiality is very important for users to store their confidential data or private information within the cloud services. In data confidentiality is used to ensure authentication and access control strategies. The data confidentiality, authentication and access control problems are mainly to protect in cloud computing might be self- addressed by improving the cloud reliability and trustiness [8]. As a result of the users don't trust thecloud providers and cloud storage service providers. These are virtually not possible to eliminate potential corporate executive threat; it is terribly dangerous for users to store and protect their sensitive data in cloud storage directly. The simple encryption process is faced with the key type management drawback and cannot support the advanced requirements like parallel modification, query, and fine-grained authorization. The cloud computing have several techniques for enhancing and developing data confidentiality.

1. Homomorphic encryption: encryption is typically used to make sure the data confidentiality. Homomorphic encryption is a kind of encryption system to authority of the data.

2.Encrypted Search and Database: Because the homomorphic encryption algorithm is ineffective. The homomorphic encryption algorithm is the study of the applications of limited within the cloud environment researchers. Encrypted search is a general operation to protect data from unauthorized resources. 3. Distributed Storage: In the Distributive storage of data is also a promising approach in the cloud environment. 4. Hybrid Technique. A hybrid technique is projected for ensuring data integrity and data confidentiality, which uses both key sharing technique and authentication technique. 5. Data Concealment. Data concealment is mainly used to maintain the data confidentiality in the cloud. Data Availability: -Data availability mean that the following: when accidents occur like hard disk damage, IDC fire, electronic circuit failure, and network failures, the coverage that user's data are often recovered or utilized and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone. The transborder servers under the main issue of storing data is detail about a serious concern of clients for the reason that the cloud vendors are governed by the local laws and, as a result, the cloud

clients must be cognizant of these laws. In addition, the cloud service provider should make sure the data security, notably data confidentiality and data integrity. The cloud provider should share and protect all such concerns with the client and establish trust relationship with this connection establishment. The cloud marketer ought to give guarantees of data safety and build a case for jurisdiction of native laws to the client's process management. Establishing data connection can support users to extend their trust relationship on the cloud. Cloud storage affords the transparent storage service for performing with users, which can reduce the cloud complexity, however, it also reduces the control ability of data storage of users.

Limitation

•Enterprises observe different obstacles when they move their IT infrastructure into the clouds. SMEs can sacrifice the sufferings of these obstacles to some extent, since adopting cloud would be a cheaper solution compared to the cost of running an individual IT infrastructure. A perfect trade-off between costs and benefits can help SMEs to make proper judgment of adopting cloud computing [5]. In this section, we analyse all the potential problems that delay the adoption cloud computing for some of the SMEs and the large enterprises.

Conclusion

Cloud computing proves an extremely successful application for each and every organization's performance. For the reason that organizations have large amount of data to store and cloud provides that space given to user and also enables its user to access their data from anyplace anytime in a simple manner. Improved use of cloud computing for storing data is definitely increasing the trend of improving the ways
of storing data in the cloud. As peoples are saving their personal information and important data to clouds, therefore it becomes a major issue to store that data safely. Data available in the cloud can be at risk if not protected in a trustful manner. In the cloud there are a number of existing techniques used to implement security prevention. The study provided an overview and discuss about the cloud computing and security issues and how to improve the security algorithms for cloud computing.

References

[1] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, “Data Confidentiality and Integrity Verification usingUser Authenticator scheme in cloud”, Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, “Secure Storage and Access of Data in Cloud Computing”, 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, “Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management”, 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 1st International Conference on Parallel, Volume 3, Issue 1, January-February-2018 | www.ijsrcseit.com | UGC Approved Journal [Journal No: 64718] 1745 Distributed and Grid Computing (PDGC-2010).