Cloud Computing - Ensuring Data Security

Mohammad Furqan [1], **Monika Saini**[2]
Department of Computer Science,
World College of Technology and Management,
Gurugram, Haryana, India.

Abstract -Now day's Cloud figuring is rising/requesting field as a result of its Performance, high accessibility, with ease, new computational worldview that offers an imaginative plan of action. Cloud is somewhat Centralized database where numerous associations store their information, recover information and conceivably change information. In the cloud numerous Services are given to the customer by cloud. Information store is principle future that cloud administration gives to the enormous association to store colossal measure of information. Yet numerous associations are not prepared to actualize distributed computing innovation as a result of taking after reason. That is Lack of security, Data repetition, Misbehaviour of the server. So the primary goal of this paper is to understand the above reasons that are To forestall unapproved access, it should be possible with the assistance of a disseminated plan by utilizing homomorphism token to give security of the information in cloud. The cloud is backing for information excess means customers can embed, erase or can redesign information so there ought to be security component which guarantee honesty of information. This paper likewise secures the information while the acting up of the server emerge. In this report, we concentrate on Ensuring information stockpiling security in distributed computing.

Keywords: Cloud computing, cloud administration, cloud security, computer network, disseminated processing, security.

1. Introduction

Cloud Computing describes computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Cloud computing is a natural evolution of the widespread adoption of virtualization, service, autonomic and utility computing. Details are abstracted from end-users, who no longer have need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if it were a program installed locally on their own computer. Now a day Cloud Computing become so strong, because it is an Internet-based development and use of computer technology and also cheaper as well as more powerful processors, together with the software as a service (SaaS) computing architecture. Due to increase in network bandwidth it becomes faster to provide quality of services as compare to previous. Also support to moving the data between cloud and client without any complexity because of releasing the hardware complexity. Because of online base computing it provide huge amount of data storage and resources to the local machine and eliminate the local machine to maintenance separate data. As a result, users are at the thankful of their cloud service providers for the availability and integrity of their data. **Data security** is always been the important aspect of quality of services, Cloud computing every time invites the new challenges of security thread for number of reasons. Firstly, traditional cryptographic cannot be used directly data security purpose because users' loss control of data under Cloud Computing. Therefore, verification of correct data whether it store correctly or not in the cloud must be conducted without explicit knowledge of the whole data.

Due to the continuously demanding of long term storage of data with correctness and security become more challenging. Secondly, Cloud Computing is not just a third party data warehouse. In this report, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users" data in the cloud .we rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization on data errors, i.e., the identification of the misbehaving server(s)

2. Architecture Of Cloud Computing

Cloud architecture is nothing but the systems architecture of the software systems which involved in the delivery of cloud computing, generally it involves multiple cloud components communicating with each other over loose coupling mechanism like messaging queue. The most important components of the cloud computing architecture are front end and back end. Where the front end is the part seen by the client, i.e., the computer user, which includes the client's computer and the applications used to access the cloud via a user interface such as a web browser or any system application. The back end of the cloud computing architecture is the cloud itself i.e. admin of cloud, which comprising various computers, servers and data storage devices. Three various network elements can be identified as follows: Users: Who have data to be stored in the cloud and depend on the cloud for data computation, also consist of both individual consumers and organizations.

CSP (Cloud Service Provider): CSP is the person who can manage whole services as well as data storage and lot more thing of cloud computing like operate live Cloud computing system. And having optional TPA (Third Party Auditor), who has capabilities and authority that users may not have, TPA is trusted person to take a risk of cloud storage services on behalf of the users upon request.

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over application programming interfaces, usually web services and 3-tier architecture. This resembles the UNIX philosophy of having multiple programs each doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts.

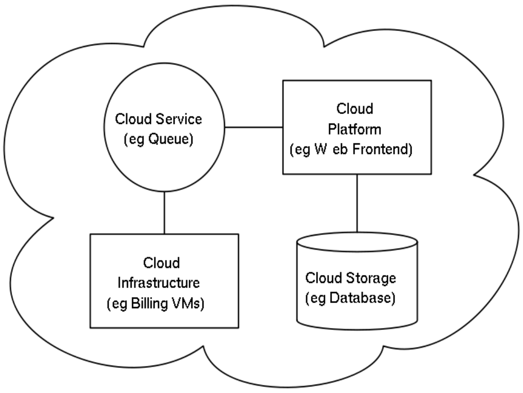

Fig 1. Architecture of Cloud Computing

The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the computer user. This includes the client's network (or computer) and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, comprising various computers, servers and data storage devices.

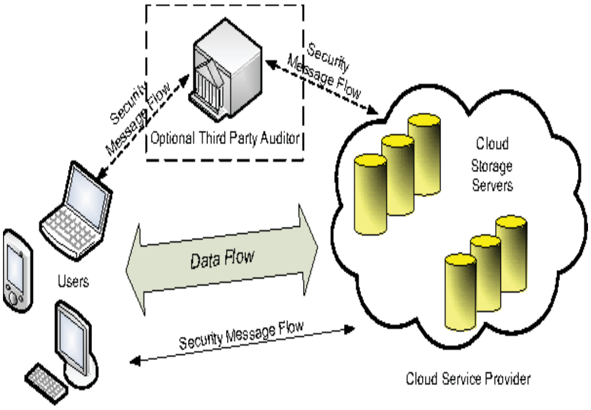

Fig 2. Security Message Flow in Cloud Computing

3. KEY SECURITY AND PRIVACY ISSUES

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models. Where possible, examples of previously exhibited or identified problems are provided to illustrate an issue. The examples are not exhaustive and may cover only one aspect of a more general issue. For many of the issues, the specific problems discussed have been resolved. Nevertheless, the broader issue persists in most cases and has the potential to be expressed again in other ways among the various service models.

The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security (Teneyuca, 2011). Area straightforwardness is one of the unmistakable adaptabilities for cloud figuring, which is a security risk in the meantime – without knowing the particular area of information stockpiling, the procurement of information assurance represent some district may be seriously influenced and damaged. Trust foundation may turn into the way to set up a fruitful cloud computing environment. The procurement of trust model is fundamental in cloud computing as this is a typical interest range for all partners for any given cloud computing situation. Trust in cloud may be subject to various variables among which some are mechanization administration, human components, procedures and arrangements. A wide range of attacks that are appropriate to a network and the information in travel similarly applies to cloud based administrations – a few dangers in this classification are phishing, eavesdropping, sniffing, man-in-the-middle attack and other comparable assaults. DDoS (Distributed Denial of Service) assault is one basic yet real assault for cloud figuring base. As cloud computing typically implies utilizing open networks and consequently putting the transmitting information presented to the world, digital attacks in any structure are foreseen for cloud processing. The current contemporary cloud based services have been found to experience the ill effects of weakness issues with the presence of conceivable security escape clauses that could be abused by an aggressor. Security and protection both are worries in distributed computing because of the way of such registering approach. The methodology by which distributed computing is finished has made it inclined to both data security and system security issues. Outsider relationship may develop as a danger for cloud environment alongside other security dangers inalienable in infrastructural and virtual machine viewpoints. Variables like delicate product bugs, social designing, human mistakes make the security for cloud a powerfully challenging one Interruption location is the most vital part in consistent system checking to lessen security dangers. On the off chance that the contemporary IDSs (Intrusion location Systems) are wasteful, the resultant outcome may be undetected security rupture for cloud environment.

The wide move to portable processing rehearses as of late has made it basic to incorporate versatile registering and its related innovations as a key some portion of distributed computing. Asset shortage and in addition different limitations of portable registering is hindrances to distributed computing. The interest of gigantic information handling is an issue for portable end-client gadgets which has been further supplemented by the security worries of versatile distributed computing. For versatile distributed computing, the gadget level impediments has roused scientists to recommend the consideration of another level of cloud termed as 'mobile cloud' to help the preparing of the particular processing what's more, preparing for portable processing gadgets. The earlier explained broadcast nature of satellite communication and related security issues are equally applicable to the mobile cloud computing due to its being wireless communication. Besides, the addition of mobile cloud into the perspective would add another cloud with all its security issues for a service provider having both mobile cloud and conventional cloud. The addition of mobile cloud in the scenario would boost performance, but it would also add another layer of security issue not only to the mobile cloud users, but also to the total infrastructure of the cloud service provider. The hierarchical arrangement of cloud computing facilitates different level of extensibility for the cloud users with varying degree of associated security issues

4. Conclusion

Cloud computing has colossal prospects, however the security dangers implanted in distributed computing methodology are specifically corresponding to its offered points of interest. Distributed computing is an extraordinary open door and lucrative alternative both to the organizations and the assailants – either gatherings can have their own particular points of interest from distributed computing. The inconceivable potential outcomes of distributed computing can't be disregarded exclusively for the security issues reason – the continuous examination and exploration for vigorous, reliable and coordinated security models for cloud registering could be the main way of inspiration. The security issues could extremely influence could bases. Security itself is conceptualized in distributed computing base as an unmistakable layer. Security for distributed computing environment is a non-bargaining necessity. Cloud computing is inescapable to wind up the perfect (and perhaps the extreme) way to deal with business processing however the security obstructions alongside different issues should be determined for distributed computing to make it more viable.

Taking into account the way that the effect of distributed computing can incorporate both the specialized and social settings, the exploration on distributed computing and its related concerns are definitely not related just with registering angles. Administration arranged engineering and different attributes of distributed computing proposes that the idea of distributed computing would require to break down the reasonableness in accordance with social, business, specialized and lawful points of view – every one of these aspects will fuse security issues either in specialized or key structure. Despite the way of security issues, it can be without a doubt presumed that the extreme antagonistic impacts as a result of security breaks in distributed computing, the organization of any type of distributed computing ought to manage the security concerns relating to those of the wellbeing basic frameworks.

Reference

[1] Chip Computer Magazine, December 2008 - Feb 2009 Edition

[2] Julia Allen et al., Security for Information Technology Service Contracts, CMU/SEISIM-003, Software Engineering Institute, Carnegie Mellon University, January 1988.

[3] Nate Anderson, Anonymous vs. HBGary: the Aftermath, Ars Technica, February 24, 2011.

[4] Michael Armbrust et al., A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, April 2010

[5] Warwick Ashford, Google Confirms Dismissal of Engineer for Breaching Privacy Rules, Computer Weekly, September 16, 2010,

[6] Frederick M. Avolio, Best Practices in Network Security, Network Computing, March 20, 2000,

[7] Simon Bradshaw, Christopher Millard, Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, Research Paper No. 63/2010, September 2, 2010

[8] Tony Bradley, Google, Skype, Yahoo Targeted by Rogue Comodo SSL Certificates, PCWorld, March 23, 2011.

[9] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2012.