International Journal of Information Technology and Management
Vol. 12, Issue No. 1, February-2017, ISSN 2249-4510

A Study on Data Security and Privacy in Cloud Computing

Abhijit Trimbak Parchure[1]* Dr. Suneel Kumar[2]

[1]Ph.D. Research Student, MUIT, Lucknow

[2]Research Guide, MUIT, Lucknow

Abstract – Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in the entire globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.

Keywords: Data Security, Privacy, Cloud Computing, Information Technology Environment, Privacy Protection, etc.

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

Cloud computing is the conveyance of computing services over the Internet. Cloud services permit people and organizations to utilize software and hardware that are oversaw by unbiased gatherings at remote areas. Illustrations of cloud services incorporate online record storage, long range interpersonal communication locales, web mail, and online business applications. The cloud computing model permits access to information and computer resources from anyplace that a network connection is accessible. Cloud computing furnishes an imparted pool of resources, incorporating data storage space, networks, computer processing power, and particular corporate and client applications.

In its broadest utilization, the term cloud computing alludes to the conveyance of adaptable IT resources over the Internet, instead of facilitating and operating those resources by regional standards, for example, on a school or college network. Those resources can incorporate applications and services, and in addition the base on which they work (Birman, et. al., 2009). By sending IT framework and services over the network, an organization can buy these resources on an as-required groundwork and maintain a strategic distance from the capital expenses of software and hardware. With cloud computing, IT limit might be balanced rapidly and effectively to accommodate changes popular. While remotely hosted, oversaw services have long been a piece of the IT scene, an uplifted investment in cloud computing is constantly powered by pervasive networks, developing norms, the ascent of hardware and software virtualization, and the push to make IT expenses variable and transparent (Armbrust, Armando Fox et. al. (2009).

Cloud computing give IT organizations a fundamentally distinctive model of operation, one that exploits the development of web applications and networks and the climbing interoperability of computing systems to furnish IT services. Cloud providers spend significant time specifically applications and services, and this mastery permits them to effectively oversee redesigns and upkeep, reinforcements, fiasco recuperation, and failover functions. Accordingly, shoppers of cloud services may see expanded unwavering quality, even as expenses decrease because of economies of scale and other generation elements (Mather, et. al., 2009). With cloud computing, organizations can monitor present needs and make on-the-fly changes in accordance with expand or decline limit, pleasing spikes popular without paying for unused limit throughout slower times (Hayes, 2008). Aside from the possibility to lower expenses, schools and

colleges addition the flexibility of having the ability to react rapidly to demands for new services by acquiring them from the cloud. Cloud computing supports IT organizations and providers to build standardization of conventions and processes so the numerous bits of the cloud computing model can interoperate fittingly and effectively. Cloud computing's scalability is an alternate key profit to higher instruction, especially for research undertakings that oblige immeasurable measures of storage or processing limit for a constrained time (Gopalakrishnan, 2009). A few organizations have fabricated data focuses close wellsprings of renewable vigor, for example, wind ranches and hydroelectric offices, and cloud computing manages access to these providers of "green IT." Finally, cloud computing permits school and college IT providers to make IT expenses transparent and in this manner match utilization of IT services to the individuals who pay for such services (Ristenpart, et. al., 2009).

REVIEW OF LITERATURE:

Cloud computing construction modeling comprises of two parts "the front end" and "the back end". The front end of the cloud computing system involves the customer's unit (or it may be computer network) and a few applications are required for gaining entrance to the cloud computing system. Back end alludes to the cloud itself which may include different computer machines, data storage systems and servers. Gathering of these clouds make an entire cloud computing system. The entire system is controlled through a focal server that is likewise utilized for monitoring customer is request and traffic guaranteeing smooth working of the system (Armbrust, et. al., 2009). An exceptional sort of software called "Middleware" is utilized to permit computers that are associated on the network to correspond with one another. Cloud computing systems additionally must have a duplicate of all its customers, data to restore the service which may emerge because of a unit breakdown. Making duplicate of data is called excess and cloud computing service providers furnish data repetition.

Cloud computing is the name given to a later example in processing administration acquisition. This example has seen the mechanical and social development of figure administration acquisition from being offered predominantly to being given remotely and by and large, by substitute get-together administration suppliers. These other social occasions offer buyers a sensible also versatile registering administration that buyers may by and large not have been open, forgotten to figure things without any other individual's information oversee. This new strategy for administration acquisition has progressed from and is the complete of research originating from (around others) passed on and organized frameworks, utility processing, the web and programming administrations investigate.

Security of Identity Data in Cloud Computing: The creating notoriety, continuing change and improvement of cloud computing administrations is a certain fact. Data spared by and large on a PC may be spared in the cloud, fusing word handling reports, spreadsheets, presentations, sound, photos, motion pictures, records, money related data, errand calendars, etc. A cloud benefit supplier (SP) is another social affair that keeps up data about, or for, a substitute component.

Trusting a substitute social event obliges taking the peril of expecting that the accepted impartial get-together will go about as it is ordinary (which may not be right continually). At whatever point some component stores or procedures data in the cloud, security or protection request may rise.

Security in cloud computing could be described as, the limit of a substance to control what data it reveals about itself to the cloud (or to the cloud SP), and the ability to control who can get to that data."

Different existing security laws constrain the models for the amassing, upkeep, use, and disclosure of specifically identifiable data (PII) that must be satisfied even by cloud Sps. (PII is normally rumored to be character data.) Due to the method for cloud computing, there is alongside zero data open in a cloud to raise where information are filed, how secure they are, who has permission to them, or if they are traded to a substitute have (if that have may be trusted).

A cloud can't be used for sparing and handling information additionally applications gave that it is unsecure. The main problem as to in cloud is the way by which to secure PII from being used by unapproved customers, how to suspect ambushes against protection, (for instance, personality robbery) really when a cloud SP can't be trusted, and how to oversee control over the exposure of private data.

Cloud Protection Problems: Security issues go under many appearances both specialized and socio-specialized in root. To cover all the security issues conceivable inside the cloud, and top to bottom, would be herculean an assignment not suited notwithstanding for Heracles himself. Existing endeavors hope to give a scientific categorization over the issues seen. The Cloud Security Alliance1 is a non-benefit association that looks to advance the prescribed procedures for giving security confirmation inside the cloud computing scene. In Hubbard, Sutton et al. the Cloud Security Alliance distinguish seven dangers to cloud computing that can be deciphered as a characterization of security issues found inside the cloud. They are:

1. Mishandle and Nefarious Use of Cloud Computing, 2. Unreliable Application Programming Interfaces, 3. Vindictive Insiders, 4. Shared Technology

Vulnerabilities, 5. Information Loss/Leakage, 6. Record, Service and Traffic Hijacking, 7. Obscure Risk Profile.

For an exchange portrayal of perils to Cloud Computing, one can direct. This part outfits a general point of view of the security issues inside the degree of the threats displayed by the Cloud Security Alliance. This part completes up with a framework of the legitimate perspectives speaking to security inside the cloud.

Predicate Based Encryption: Predicate Based Encryption (PBE), addresses a gathering of unbalanced encryption plots that considers particular fine-grained get to control as a noteworthy part of the basic cryptographic operation [ksw08]. The underlying foundations of PBE are in Identity Based Encryption (IBE) [sha85]. In IBE plans a component's encryption key is derived from a clear string that addresses the substance's open character e.g. a message address. For example, given a component Albert his contrasting encryption key will be Enc(albert) == albert@foobar.com. All through encryption, the following figure substance will sufficiently be named with the string addressing the encryption key, the component's open character. A component's decoding key will be induced from a similar string used for the encryption key e.g. Albert's decoding key will be gathered from his message address. On receipt of a cipher text message the recipient can unscramble the figure content if and just if the two identities, held inside the decoding key and figure substance, are `equal'. PBE plans offer a wealthier arrangement in which a component's `identity' could be created from an arrangement of traits and decoding is associated with get to approaches that offers a more expressive means with which to depict the association between the properties (Baek, et. al., 2008). For the most part talking, inside PBE schemes elements and figure messages are each one connected with a set of attributes. These attributes are utilized to portray some part of the element, the data that is continuously encrypted, and the environment. Matching is accomplished through predicates (access policies) that indicate: a) the set(s) of authorized attributes that a substance must have to decrypt and access the plain-content; and b) the relationship between the attributes.

Different developments of PBE schemes have been recommended that utilize general predicates (spoke to as Boolean equation) or particular predicates, for example, balance, shrouded vector or internal item. The decision of predicate will have an administer influence upon the plan, its attributes and the synthesis of the right to gain entrance policies. Additionally, the situation of the predicate has an extraordinary influence upon the workings of a PBE plan. Regular to all PBE schemes are four operations taking into account encryption, decryption and key era (Ballard, et. al., 2005). The exact esteem for encryption and decryption keys is needy upon both the development of the plan and arrangement of predicates.

The point when taking a gander at the diverse PBE schemes, three groupings (or family) of schemes develop based upon the predicates being utilized, the plan's point and the schemes development.

Encrypted Information in Cloud Computing: As of late, cloud computing is increasing much force in the IT business. Particularly, we have seen the sensational development of open mists, in which the registering assets can be gotten to by the overall population. One of the greatest points of interest of an open cloud is it's for all intents and purposes boundless information stockpiling abilities and versatile asset provisioning (Bao, et. al., 2008). Numerous IT enterprises and people are outsourcing their databases to the cloud servers, with a specific end goal to appreciate the much lower information administration cost than keeping up their own server farms. It has never been less demanding than now that an assortment of clients/customers could get to or share data put away in the cloud, autonomous of their areas. In spite of eagerness around the cloud information benefit outsourcing model, its guarantees can't be satisfied until we address the genuine security and protection worries that information proprietors have. The outsourced information may contain exceptionally touchy data, for example, Personal Health Records (PHRs), face book photographs, and business reports (Benaloh, et. al., 2009). Many individuals stay questionable about the levels of security assurance of their information when put away in a server possessed by an outsider cloud benefit supplier.

CONCLUSION:

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data

security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

REFERENCES:

A. Gopalakrishnan (2009). “Cloud Computing Identity Management,.” SETLabs Briefings, vol. 7.

Brian Hayes (2008). "Cloud Computing", Commun. ACM 51.7, pp. 9-11.

F. Bao, R. H. Deng, X. Ding, and Y. Yang (2008). Private query on encrypted data in multi-user settings. In ISPEC’08, pages 71–85, Berlin, Heidelberg, Springer-Verlag.

J. Baek, R. Safavi-Naini, and W. Susilo (2008). Public key encryption with keyword search revisited. In Proceedings of ICCSA, Part I, ICCSA ’08, pages 1249–1259.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In CCSW’09, pages 103–114.

Ken Birman, Gregory Chockler, Robbert van Renesse (2009). "Toward a cloud computing research agenda", SIGACT News 40.2 pp. 68-80.

L. Ballard, S. Kamara, and F. Monrose (2005). Achieving efficient conjunctive keyword searches over encrypted data. In Proc. of ICICS’05.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009). Above the clouds: A berkeley view of cloud computing, Feb 2009.

Michael Armbrust, Armando Fox et. al. (2009). "Above the Clouds: A Berkeley View of Cloud Computing", Tech. rep. UCB/EECS-2009-28.

T. Ristenpart, E. Tromer, H. Shacham, S. Savage (2009). “Hey, You, Get Off My Cloud: Exploring Information Leakage in Third- Party Compute Clouds,.” Proc. 6th ACM conference on Computer and Communications Security, Chicago, IL, pp. 199-212.

Tim Mather, Subra Kumaraswamy, Shahed Latif (2009). "Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance", Editor Mike Loukides. O’Reilly.

Corresponding Author

Abhijit Trimbak Parchure*

Ph.D. Research Student, MUIT, Lucknow

E-Mail – abhijitparchure@yahoo.com