International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 2, Mar-Apr 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Review Paper on "Data security issues in cloud computing"

Gagandeep Kaur

Asstt. Professor, CSE Department, Shri Rawatpura Sarkar University, Raipur (C.G.), kgagan619@yahoo.com

Abstract-

Cloud computing offers a prominent provider for facts garage called cloud storage. The go with the flow and garage of facts on the cloud environment in simple textual content format can be main protection threat. So, it is the duty of cloud provider vendors to make certain private and protection of facts on storage in addition to network level. The following three parameters confidentiality, integrity and availability determine whether protection and private of statistics saved on cloud environment is maintained or not. The proposed work is to outline cloud structure with configured samba storage and cryptographic encryption techniques. The cloud architecture deployed with samba storage makes use of operating gadget feature specifying permission values for 3 attributes (User/Owner, Group and Global) and maps it to cryptographic utility which plays cryptographic operations. Cryptography software supports symmetric and uneven encryption algorithm to encrypt/decrypt data for uploading/downloading within cloud storage. A username and password based totally authentication mechanism for users and virtual signature scheme for information authenticity are defined inside cloud architecture.

Keywords- Cloud computing security, Cloud storage, Symmetric and asymmetric cryptosystem, AES, ECC, SHA, Samba Server, Cryptographic Application.

I .INTRODUCTION

Cloud computing is a disbursed computing fashion which give integration of internet services and statistics centres. There are several predominant cloud computing carriers such as Amazon, Google, Yahoo, Microsoft and others which might be imparting cloud computing offerings. Amazon internet services became first to provide an structure for cloud based totally services in 2002 and after that improvements and new models for cloud structure were proposed and implemented. There have been many strategies of storing records on server storage. Such statistics storages supplied by means of cloud carrier carriers have to ensure consumer approximately Confidentiality, Integrity and Availability of statistics. Confidentiality: Confidentiality refers to keeping records private. Privacy is of importance as facts leaves the borders of the owner. Confidentiality is supported by technical gear inclusive of encryption and get right of entry to manipulate, as well as prison protection. Integrity: Integrity is a degree of self assurance that what statistics is meant to be in cloud, what is honestly there, and is protected against unintentional or intentional alteration without authorization. Availability: Availability manner being capable of use the device as predicted by means of cloud consumer. Cloud technologies can growth availability through full-size internet-enabled get entry to, but the consumer is dependent on the well timed and sturdy provision of resources. Availability is supported through capability constructing and precise architecture by way of the provider, in addition to well-defined contracts and terms of agreement. Cloud statistics garage safety addresses the want of enforcing selective information get admission to by using providing an method that helps the user in specification of access regulations and safety measures. Cloud Storage: Cloud garage [1] specifies the garage on cloud with almost inexpensive garage and backup option for small enterprise. The real garage location can be on single garage environment or replicated to a couple of server storage based totally on importance of information. Typical cloud storage machine architecture includes a master control server and various clients. The mechanism model of cloud storage consists of four layers: storage layer which shops the records, simple control layer which ensures safety and balance of cloud garage itself, software interface layer which affords utility provider platform, and get admission to layer which gives the access platform. The fundamental cloud garage environment represented as follows:

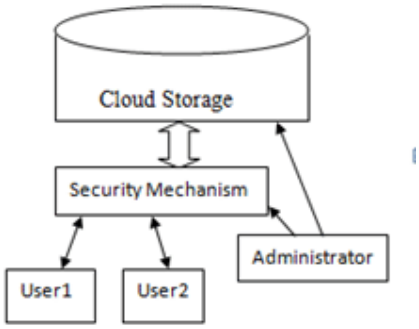

Figure 1: Cloud Storage Environment.

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.
Cloud security offers many benefits, including:

Centralized security: Just as cloud computing centralizes applications and data, cloud protection centralizes protection. Cloud-based business networks include numerous devices and endpoints that may be tough to manage when dealing with shadow IT or BYOD. Managing these entities centrally enhances visitors analysis and net filtering, streamlines the tracking of network activities and effects in fewer software and policy updates. Disaster healing plans also can be carried out and auctioned without problems when they are managed in a single place.

Reduced costs: One of the advantages of using cloud storage and security is that it gets rid of the need to put money into committed hardware. Not simplest does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were fire fighting protection troubles reactively, cloud safety delivers proactive security capabilities that offer safety 24/7 with little or no human intervention.

Reduced Administration: When you pick out a reputable cloud services issuer or cloud security platform, you may kiss goodbye to manual security configurations and almost consistent safety updates. These tasks may have a massive drain on resources, however while you flow them to the cloud, all safety administration occurs in one region and is absolutely controlled in your behalf.

Reliability: Cloud computing services offer the remaining in dependability. With the proper cloud security features in place, customers can safely access records and packages within the cloud irrespective of where they may be or what device they're using.

More and more organizations are realizing the various business blessings of transferring their structures to the cloud. Cloud computing allows groups to operate at scale, reduce technology prices and use agile structures that supply them the competitive edge. However, it is important that organizations have entire self assurance of their cloud computing security and that all data, systems and packages are blanketed from facts theft, leakage, corruption and deletion.
All cloud fashions are vulnerable to threats. IT departments are naturally careful about shifting mission-important systems to the cloud and it is important the proper safety provisions are in place, whether you are jogging a local cloud, hybrid or on-premise environment. Cloud safety gives all the functionality of conventional IT protection, and allows companies to harness the many blessings of cloud computing while final steady and also ensure that records privateness and compliance requirements are met.

II.RELATED CONCEPT

1. **CLOUD MODELS :**

- Public cloud: the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.
- Private cloud: the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.
- Community cloud: the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.
- Hybrid cloud: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

2. CLOUD BENIFITS:

- On demand service: cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.
- Ubiquitous network access: cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.
- Easy use: the most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
- Business model: cloud is a business model because it is pay per use of service or resource.
- Location independent resource poling: the providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

3. **3. CLOUD SOLUTIONS :**

- Infrastructure as a service: it delivers a platform virtualization environment as a service rather than purchasing servers, software, data centers.
- Software as a service: it is software that is deployed over internet and or is deployed to run behind a firewall in your LAN or PC.
- Platform as a service: this kind of cloud computing provide development environment as a service. You can use the middleman's equipment to develop your own program and deliver it to the users through internet and servers.
- Storage as a service: this is database like services billed on a utility computing basis, e.g., gigabyte per month.
- Desktop as a service: this is the provisioning of the desktop environment either within a browser or as a terminal server.

III. CLOUD SECURITY CHALLENGES

The cloud services gift many demanding situations to an company. When an corporation mitigates to eating cloud services, and specifically public cloud services, a lot of the computing machine infrastructure will now under the manager of cloud service issuer. Many of these demanding situations have to be addressed through control projects. These management tasks will requires absolutely delineating the ownership and obligation roles of each the cloud provider and the corporation functioning within the function of customer. Security managers must be able to decide what detective and preventative controls exist to sincerely define safety posture of the corporation. Although right safety controls must be implement primarily based on asset, threat, and vulnerability risk assessment matrices. Cloud computing security chance evaluation record specifically from the vendor's point of view about security abilities analyzed security dangers faced by the cloud. Here are security risks list.

- Regulatory compliance: cloud computing providers who refuse to external audits and security certifications.
- Privileged user access: sensitive data processed outside the organization brings with it an inherent level of risk.
- Data location: when you use cloud, you probably won't know exactly where your data hosted.
- Data segregation: data in the cloud is shared environment alongside data from other customers.
- Recovery: even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- Investigative support: investigating inappropriate or illegal activity may be impossible in cloud computing.
- Long term viability: you must be sure your data will remain available even after such an event.

1. **Security:** When multiple businesses share resources there's a hazard of facts misuse. So, to avoid threat it's miles vital to secure statistics repositories and also the facts that include storage, transit or process. Protection of records is the most important demanding situations in cloud computing. To decorate the safety in cloud computing, it is crucial to provide authentication, authorization and access manipulate for facts saved in cloud. The three essential areas in facts protection are

Confidentiality: - Top vulnerabilities are to be checked to ensure that data is protected from any attacks. So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc.

Integrity: - To provide security to the client data, thin clients are used where only few resources are available. Users should not store their personal data such as passwords so that integrity can be assured.

Availability: - Availability is the most important issue in several organizations facing downtime as a major issue. It depends on the agreement between vendor and the client.

2. ***Locality***: In cloud computing, the facts are distributed over the variety of regions and to discover the area of facts is difficult. When the facts are moved to one of a kind geographic places the legal guidelines governing on that records can also change. So there is a difficulty of compliance and information privacy legal guidelines in cloud computing. Customers have to know their information location and its miles to be intimated by means of the provider.

3. ***Integrity***: The machine must preserve safety such that records can be simplest modified via the legal person. In cloud based environment, statistics integrity should be maintained efficaciously to avoid the facts lost. In general each transactions in cloud computing need to comply with ACID Properties to preserver information integrity. Most of the web services face lot of problems with the transaction management regularly as it uses HTTP offerings. HTTP provider does now not support transaction or assure delivery. It can be dealt with the aid of imposing transaction management inside the API itself.

4. ***Access:*** Data access mainly refers to the data safety policies. In an organization, the personnel could be given get admission to the segment of information based totally on their organisation protection policies. The identical facts cannot be accessed by way of the other employee operating in the identical organization. Various encryption strategies and key management mechanisms are used to make certain that statistics are shared most effective with the valid users. The key's distributed most effective to the authorized parties using diverse key distribution mechanisms. To steady the statistics from the unauthorized customers the information safety policies should be strictly followed. Since get right of entry to is given via the internet for all cloud users, it is vital to provide privileged user get admission to. User can use records encryption and safety mechanisms to keep away from protection risk.

5. ***Confidentiality****:* Data is saved on far flung servers by the cloud customers and content such as facts, movies etc.., may be saved with the single or multi cloud providers. When statistics is stored inside the remote server, facts confidentiality is one of the important requirements. To keep confidentiality facts know-how and its classification, users have to be aware about which statistics is stored in cloud and its accessibility.

6. ***Segregation:*** One the foremost characteristics of cloud computing is multi-tenancy. Since multi-tenancy lets in to store records by more than one customer on cloud servers there is a opportunity of records intrusion. By injecting a purchaser code or by using any application, information may be intruded. So there is a need to store facts one by one from the ultimate customer's information. Vulnerabilities with facts segregation can be detected or discovered out using the tests which include SQL injection, Data validation and insecure storage.

7. ***Data Center Operation:*** In case of records transfer bottlenecks and disaster, businesses the usage of cloud computing

applications wishes to guard the user's data without any loss. If information isn't controlled properly, then there may be an difficulty of data garage and records access. In case of disaster, the cloud companies are liable for the loss of records.

IV. PROPOSED METHODOLOGY

In proposed methodology Encryption is recommended as a higher answer to stable information. Before storing facts in cloud server it's far better to encrypt facts. Data Owner can provide permission to particular group member such that data may be without problems accessed by them. Heterogeneous information centric safety is to be used to provide statistics access control. A statistics security model comprises of authentication, statistics encryption and statistics integrity, information recovery, person protection needs to be designed to enhance the data safety over cloud. To make certain private and information protection facts safety can be used as a service. To keep away from get right of entry to of facts from other customers, making use of encryption on data that makes records totally unusable and everyday encryption can complicate availability. Before importing facts into the cloud the customers are counselled to verify whether the statistics is stored on backup drives and the keywords in documents continue to be unchanged. Calculate the hash of the record before importing to cloud servers will ensure that the records isn't altered. This hash calculation can be used for facts integrity but it's far very tough to keep it. RSA primarily based records integrity check may be provided by means of combining identity based cryptography and RSA Signature. SaaS ensures that there must be clean boundaries each at the physical degree and application stage to segregate statistics from distinct users. Distributed get admission to manage structure can be used for get right of entry to management in cloud computing. To become aware of authorized users, the use of credential or attributed based policies are better. Permission as a service may be used to tell the consumer that which a part of information may be accessed. Fine grained get right of entry to control mechanism permits the owner to delegate most of computation intensive responsibilities to cloud servers without disclosing the statistics contents. A records driven framework can be designed for steady statistics processing and sharing between cloud users. Network based totally intrusion prevention gadget is used to discover threats in real-time. To compute big documents with unique sizes and to address remote facts safety RSA based totally storage security method can be used.

V. CONCLUSION

In this paper, Although cloud computing is the new emerging technology that presents an excellent range of benefits to the users, it faces lot of protection demanding situations. In this paper data protection demanding situations and solutions are provided for these demanding situations to triumph over the threat worried in cloud computing. In destiny concrete standards for cloud computing safety can be developed. To offer secure facts get right of entry to in cloud, advanced encryption techniques can be used for storing and retrieving statistics from cloud. Also right key management strategies can be used to distribute the important thing to the cloud customers such that simplest authorized folks can get entry to the data.

REFERENCES

[1]. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, 2008.p.50-55.

[2]. M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

[3]. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

[4]. P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[5]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[6]. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[7] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer

[8] Deepika Verma, Er. Karan Mahajan,(December 2014), 'To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms', International Journal of Advances in Science and Technology (IJAST) ,Vol 2, Issue 4.

[9] Ankita Ojha, Tripti Sarema, Dr.Vineet Richariya, (May 2015),'An efficient approach of sensitivearea watermarking with encryptionsecurity', International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 4 Issue 5.

[10] Honggang Wang,Shaoen Wu, Min Chen Wei Wang, (March 2014)'Security protection between users and the mobile media cloud',IEEE communications magazine.

[11] Jagruti R. Mahajan, Nitin N. Patil, (2015) 'Alpha channel for integrity verification using digital signature on reversible watermarking QR', international conference on computing communication control and automation.

[12] A.Khan, A.Siddiqui, S.Munib, and S.A.Malik, (2014), 'A Recent Survey of Reversible Watermarking Techniques', DOI:10.1016/j.ins.2014.03.118, Information Sciences.

[13] Dharini. A, R.M. Saranya Devi, and I. Chandrasekhar, (Nov. 2014), 'Data Security for Cloud Computing Using RSA with Magic Square Algorithm', International Journal of Innovation and Scientific Research,ISSN 2351-8014 Vol. 11 No. 2 pp. 439-444, 2014 Innovative Space of Scientific Research Journals.

[14] Manish gupta, Darpan Anand, Rajeev gupta, Girish parmar,(November 2012), 'A new approach for information security using asymmetric encryption and watermarking technique', international journal of computer applications (0975 – 8887), volume 57– no.14.

