A Key Based Security Technique of Cloud Computing for Processing of Data

Krishna Chauhan
Department of Computer Science & Engineering, PIT
Bhopal (M.P) India
spvarshi@gmail.com

Neha Shrivastava
AP, Department of Computer Science & Engineering
PIT, Bhopal (M.P) India
nehashriva@gmail.com

Surendra Vishwakarma
AP, Department of Computer Science & Engineering
PIT, Bhopal (M.P) India
s.vish83@gmail.com

ABSTRACT
The growth of IT based enterprises for the forthcoming generation depends on cloud computing technology. The accessibility and manageability of cloud computing infrastructure managed large database and huge amount of server for the processing of data. The processing and storage of data faced a problem of data integrity during the process of data storage and data retrieval. For maintain a data integrity and data security cloud computing adopt the process of third party auditor (TPA). The third party auditor maintains the communication between cloud service provider and user. Users only interact with TPA and TPA provides the access privilege for user.Now a day's various authors used the cryptography technique for the process of security and data integrity. The cryptography technique provides public and private cryptography technique for the processing of data.

Keywords: -Cloud Computing, SAAS, PAAS, IAAS. TPA, Stroage

INTRODUCTION
Cloud computing is a new distributed computing paradigm aiming to provide final users ready computing services. It is a natural expansion of many design principles, protocols, plumbing, and platforms that have been used over the previous 20 years. However, cloud computing brings some fresh capabilities that are represented into a software stack and are responsible for the programmability, scalability, and virtualization of resources.Cloud computing inherits some aspects of its predecessor technologies; it comes with some of their existing challenges but also with new issues, especially in the security and load balancing aspects. This latter is particularly important and critical because when providing resources to end users, blockage could be engendered due to complicacy and rising of demand. As the requests of the clients can be random to the nodes they can vary in quantity and thus the load on each node can also vary [6]. Therefore, every node in a cloud can be unevenly loaded of tasks according to the amount of work requested by the clients.

Computing is being converted to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water. As for Utility Computing is typically implemented using other computing infrastructure. In a cloud business model, a customer will pay the provider on a consumption basis, very much like the utility companies charge for basic utilities such as electricity, gas, and water, and the model relies on economies of scale in order to drive prices down for users and profits up for providers. Cloud computing is therefore a new approach based on leveraging the Internet to consume software or other IT services on demand. End users share processing power, storage space, bandwidth, memory and software. With cloud computing, the resources are shared and so are the costs. Users can pay as they consume and only use what they need at any given time, keeping charges to the user cheap[1].

In many techniques, software such as Eucalyptus, Open-Nebula and Nimbus are based on some common components. In a generic open-source cloud computing system, they can recognize six basic modules. First, they have the cloud control software whose aim is to bring together all cloud stack pieces and to ascertain enough abstraction so that a user can simply demand VMs with no harassment on how these components are created or coordinated[10].

Secondly, hardware, network and operating systems that is on the various physical machines in the system. It should be virtualized or para-virtualized depending of the virtualization framework compatibility. Para-virtualization is not adopted unless the framework could not handle the physical machines. The network includes the DNS, DHCP and the subnet organization of the physical machines. It also embraces virtual bridging and networking of the network that is required to give each VM a unique virtual MAC address. This bridging is done with the help of programs like bridgeutils, ip-tables or ebtables.

They combine advantages of the following architectures for secure cloud computing.Architecture for Signal Processing in the Encrypted Domain (SPED) in commodity computing clouds is described. SPED is based on cryptographic concepts such as secure multiparty computation or homo-morphic encryption, which enable the secure and verifiable outsourcing of the signal processing. The authors propose middleware architecture on top of a commodity cloud which implements secure signal processing by using SPED technologies. The client communicates via a special API, provided by a client-side plugin, with the middleware in order to submit new inputs and retrieve results. However, the authors do not elaborate on how to instantiate their protocols efficiently and do not answer problems regarding the feasibility of their approach. For instance, if GCs are used, they need to be transferred between the client-side plugin and the middleware which requires a large amount of communication. They parallelize the client plugin within the Trusted Cloud, provide a clear API that abstracts from cryptographic details, and give complete protocols[2].

II CLUSTER

Load balancer can be seen as the system node coordinator, it receives task processing requests from the clients, and it applies an algorithm to match each client request to a suitable cluster to process it. It has its own table of clusters, each cluster with a weight representing its average processing capacity, thus the main load balancer can choose the right cluster to transfer a client request to and the load is fairly shared between all the clusters. No job queue is needed at this level as each cluster has its own local queue[13].Each resource's cluster consists of a group of nodes (resources), it has its own local load balancer (LLB), and this latter receives requests from the MLB and deals with the load balancing inside its local cluster. It has a queue where the upcoming jobs are stored until a node inside the cluster is available to process them. The local load balancers use a scheduling algorithm to perform the load balancing; they also keep a resource table that is constantly updated if there is any change in the corresponding cluster nodes. Depending on the changes in this table, the weight of the cluster is updated in the MLB table. The local load balancer table also contains the weight of each node; hence the local load is fairly balanced between the cluster elements[2].

III PROBLEM STATEMENT

Cloud data storage and access of data faced a big security issue in concern of security and validation of user authentication. For the authentication of user used various cloud security model. All cloud security model used cryptography technique for the generation of key for access of data and retrieval of data. The data dynamics process provides the ownership of data to the user. User modified the process of data such as insertion, deletion and modification over the cloud network. The process of data dynamics precede along with cryptography and third party auditor. The third party auditor provides the access link between cloud service provider and users.The processing of cloud computing infrastructure involved three parties for the processing of data storage and data retrieval. These parties describe as problem.Client: an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations;

. Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), hasSignificant storage space and computation resource to maintain the clients' data;

. Third Party Auditor: an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

There are many types of access control mechanisms in different systems, but the main idea is controlling read and write access, which fall under confidentiality, and besides that, ensuring data integrity. Finally it is also important that the stored data is always available, but it is solely the task of the server to provide availability for the data. To sum up, we can have three levels of access permission to the stored data:

1. Verifying the integrity of the stored data
2. Verification and read access to the stored data
3. Verification read and writes access to the stored data.

IV PROPOSED METHOD

In this paper proposed a new design for cloud data storage security. The design concept basically based on shared key generation technique between clients and cloud service provider (CSP). The cloud service provider control all these mechanism and access control of data over cloud network. The accessing of data and storage of data faced a major issue in terms of public audit-ability and data dynamics. The process of data dynamics gives the ownership and authority to modification and impetration of data in cloud storage. Now a day's various authors and researcher proposed a different model for cloud security over data storage. The cryptography technique play an important role in data security in cloud computing. Many cloud storage providers claim that they provide a very solid security to their users, but we should know that every broken security system was thought once to be unbreakable.

PROCESSING OF PROPOSED ALGORITHM

There are three main party of our design model. (i) CSP (cloud service provider), who control the access and management of data control over the cloud.(ii) third party auditor(TPA) who gives the trust value of user and cloud server. UI (user interface) the user proceed the request for the data retrieval and storage in participation of cloud server provider and TPA.

Encryption Process:

Performed at UI site or CSP site, they can perform the process of encryption for the generation of session key. The process of encryption done by the cyclic shift key generation technique. the cyclic shift key generation technique is emerging key generation technique by symmetric key technique.

Verifying Data Integrity:

Simply downloading the data for integrity verification is not a practical solution due to expensiveness in I/O cost and unsafe files transfer across the network and may lead to new

vulnerabilities [49]. Moreover, legal regulations, such as (HIPAA) [50], further demand the outsourced data not to be leaked to external parties (e.g. TPA). So applying encryption before outsourcing is the most preferred way to mitigate the privacy concern. Along with MD5 and MAC, Proof of storage [48] is widely used protocol for the purpose of checking integrity of data stored on remote server. The algorithms can be run any number of times as user wants, and they do not result into too much communication or computations overhead. It produces a very small amount of information (irrespective of the size of the data file) which can be exchanged between user and Cloud, any number of times.

Other than above the Model is also provides following security goals:

a) Data dynamics: Data on to the cloud cannot be altered or modified by the user who doesn't having rights to access the data.

b) Different levels of encryption: Based on sensitivity, users' data can be divided into three Categories.

(a) Not sensitive (fully trusted model)

(b) Highly sensitive data (not trusted model) and

(c) Moderately sensitive data. So, Based on this Sensitivity level, Aim is to provide different encryption schemes.

c) Lightweight: Implementation point of view the model must consume low computation cost at client side as well low communication overhead.

(d) Incorporating the issue of Cloud dynamism: to make sure user can not extract

From dynamic of Cloud.

(e) Fake file generated in terms of user original file for wrong and illegal access of file.

MODEL DESCRIPTION

The overall operation of the entire model is divided among following main seven phases.

1. User Registration phase
2. Pre-storage phase
3. Storage phase
4. Grant access rights
5. Data download phase
6. Data verification phase

V RESULT ANALYSIS

To simulate the public auditing and data dynamics over cloud computing used java software and RMI java technology. To measure the performance of cloud computing techniques in cloud computing environment for improved the security system for stored large amount of database. For the further implementation and comparison for performance evaluation we used java programming languages with NetBeans IDE 8.0.1 tools for complete implementation/results process with database backup software as a backend my SQL also.

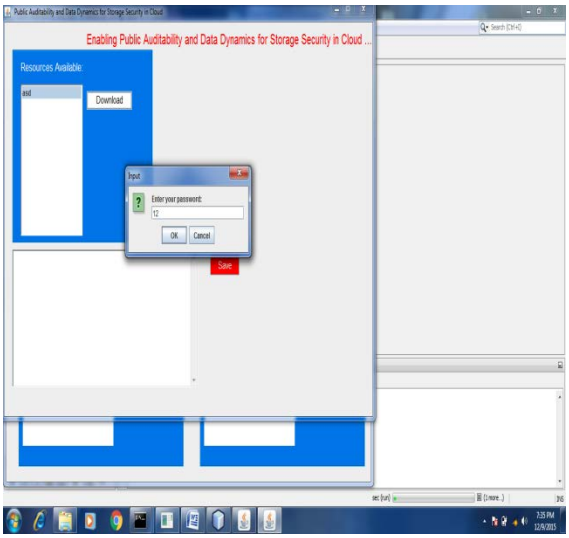

Figure 1: Shows that the file selection window and entering the key for cloud computing security system.

Types of File	File Name	Hit Ratio in %	Miss Ratio in %	Data Type value
Original File	Abc.txt	0.9	0.1	False
Fake file	Bca.txt	0.85	0.15	True

Table 1: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the Abc and Bca file.

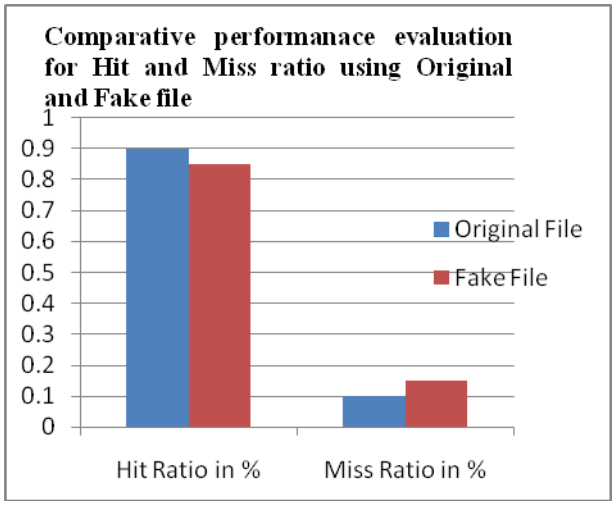

Figure 2: Shows that the comparative performance evaluation graph for original and fake files based on number of hit and miss ratio in percentage value for the Abc and Bca file.

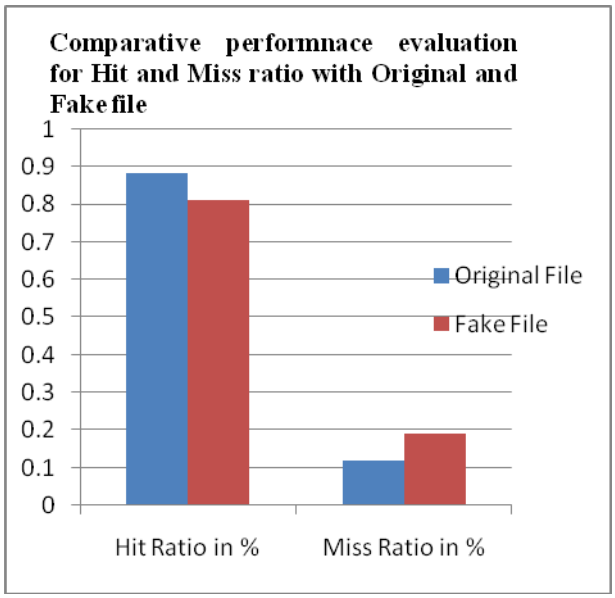

Figure 3: Shows that the comparative performance evaluation graph for original and fake files based on number of hit and miss ratio in percentage value for the Aa and Ab file.

VI CONCLUSION & FUTURE SCOPE

Security in the cloud is considered as a benefit and also a challenge. Security in the cloud is one of the greatest challenges that confront service providers and users. 62% of cloud user's ranked security is major issue in cloud storage data. It is evidently critical situation within the cloud cannot be over emphasized due to threats from within and outside of the cloud environments. Privacy and data Security responsibilities within the cloud should be a collaborative effort between both service providers and users. These responsibilities differ by the kind of cloud services been consumed. The cloud service provides is on duty to ensure the security of cloud data storage and to ensure maximum protection. Service providers have the responsibility to ensure the public data integrity and isolation protections are put in place to mitigate the risks users pose to one another in terms of data loss, misuse, or privacy violation within the cloud. The analysis and evaluation have enabled us draw some conclusions. Majority of the already available models are mature enough, but, they do not provide flexible security options for encryption based on data sensitivity for data storage over cloud. Also, verifying the integrity of data on cloud requires some computation and communication cost, which needs to be reduced drastically, due to network traffic and slow internet connectivity. Our proposed key generation demonstrates how integrity verification can be done with just transfer of few bytes and offline execution of necessary algorithms. It also offers secure access control, managing access rights mechanism, audit trail, better performance and reduced overhead.

REFERENCES:-

[1] Mohamed Belkhouraf, Ali Kartit, Hassan Ouahmane, Hamza Kamal Idrissi, Zaid Kartit and Mohamed El Marraki "A secured load balancing architecture for cloud computing based on multiple clusters", IEEE, 2015, Pp 1-6.

[2] Sven Bugiel, Stefan N¨urnberger, Ahmad-Reza Sadeghi and Thomas Schneider "Twin Clouds: Secure Cloud Computing with Low Latency", Springer, 2011, Pp 32-44.

[3] Xinwen Zhang, AnugeethaKunjithapatham, SangohJeong and Simo

[4] Mark Shtern, Bradley Simmons, Michael Smit and Marin Litoiu "An Architecture for Overlaying Private Clouds on Public Providers", IFIP, 2012, Pp 1-7.

[5] Naidila Sadashiv and S. M Dilip Kumar "Cluster, Grid and Cloud Computing: A Detailed Comparison", ICCSE, 2011, Pp 477-482.

[6] RajkumarBuyya, Saurabh Kumar Garg and Rodrigo N. Calheiros "SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions", IEEE, 2011, Pp 1-10.

[7] M. Abu Sharkh, M. Jammal, A. Shami and A. Ouda "Resource Allocation in a Network-Based Cloud Computing Environment: Design Challenges", IEEE, 2013, Pp 1-8.

[8] MayankaKatyal and Atul Mishra "A Comparative Study of Load Balancing Algorithms in Cloud Computing Environment", International Journal of Distributed and Cloud Computing, 2013, Pp 5-14.

[9] Ratan Mishra and Anant Jaiswal "Ant colony Optimization: A Solution of Load balancing in Cloud", International Journal of Web & Semantic Technology, 2012, Pp 33-50.

[10] Xun Xu "From cloud computing to cloud manufacturing", Robotics and Computer-Integrated Manufacturing, 2012, Pp 75-86.

[11] Parveen Patel, Deepak Bansal, Lihua Yuan, Ashwin Murthy, Albert Greenberg, David A. Maltz, Randy Kern, Hemant Kumar, MariosZikos, Hongyu Wu, Changhoon Kim and Naveen Karri "Ananta: Cloud Scale Load Balancing", ACM SIGCOMM Computer Communication, 2013, Pp 207-218.

[12] SushmitaRuj, Milos Stojmenovic and Amiya Nayak "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE, 2012, Pp 556-563.

[13] Fei Hu, MeikangQiu, Jiayin Li, Travis Grant, Draw Tylor, Seth McCaleb, Lee Butler and Richard Hamner "A Review on Cloud Computing: Design Challenges in Architecture and Security", Journal of Computing and Information Technology, 2011, Pp 25-55.

[14] Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, JinpengHuai, Lu Liu and K.P. Lam "CyberGuarder: A virtualization security assurance architecture for green cloud

computing", Future Generation Computer Systems, 2011, Pp 379-390.

[15] Dimitrios Zissis and Dimitrios Lekkas "Securing e-Government and e-Voting with an open cloud computing architecture", Government Information Quarterly, 2011, Pp 239-251.

[16] Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros and Yves Goeleven "Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach", Springer, 2010, Pp 3-26.

[17] A. J. Staring and G. Karagiannis "Cloud Computing Models and their Application in LTE based Cellular Systems", IEEE, 2013, Pp 750-755.