ISSN:0975-9646

Ensuring Data Security on Cloud

Jitendra Kumar Seth[1], Satish Chandra[2]

[1]*Asst. Professor, Ajay Kumar Garg Engineering College, Ghaziabad*
[2]*Asst. Professor, Jaypee Institute of Information Technology, Noida*

Abstract: In cloud users data are stored on cloud servers. Storage servers are opaque to the users even users do not know the location of their data. Users have no means to securing their data on cloud. Users data are secured as per the providers policy and SLA. Users need some means to ensure security of their data on cloud. In this paper, I proposed cryptographic techniques that ensures users data security on cloud.

Keywords: Cloud, security, AES, DES, encryption, BLS, virtual machine, etc.

1. INTRODUCTION

Cloud computing is now becoming very popular for any business (small, medium and large scale).It is an internet based computing therefore the threats and challenges to internet are also applicable to cloud either in same form or in some advance form. Security and trust in adoption of cloud are major hurdles. Cloud computing is a technology that provides online resources on pay per use basis. This computing technology is dependent on virtualization. By registering with cloud providers customers can use services (soft and hard) on pay per use basis. Customers are getting services in the form of virtual machines; they interact with these virtual machines to do their job. For each customer, distinct virtual machines are created and their controls are provided to customers. Security of these virtual machines is ensured by the providers. Clients valuable data are stored with cloud provider's data centers therefore providers must apply the desired level of security mechanism to protect these data. In recent survey it is found that security is the top most concern associated with cloud services. Customers afraid of adopting clouds services as their data are stored out of their network boundary and administration. Researchers in cloud are trying to develop security models to protect cloud services from intrusions including internal and external. Cloud is an online service hence all threats to internet are also applicable to cloud services either in the same form or in some enhanced form.

2. LITERATURE REVIEW

Cloud computing is Internet based computing where resources (software and hardware), computing power, information are available on pay per use basis and shared among cloud users. Resource provisioning and flexibility are provided by means of service level agreement. During August 08/09 by IDC IT group [1], In the Cloud Computing Services Survey security, availability and performance issues still remain in the top 3 for both years the survey was done. Security is the main issue users are concerned with when considering Cloud computing solutions Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on.

Gurdeep singh et. al. [2] critical information on cloud inspires the attacker to steal and threat them, therefore security is one of the prime concerns of cloud. Author focuses on security of VM images which are foundation of cloud security. Traditional cloud security approaches focuses on Running VM instance and integrity and privacy of customer's data.vm is not only a customer's static data it is stack of software's that boots a virtual machine into initial state.VM should be kept up to date with security patches and scanned for any malicious state. Top seven security threats to cloud are 1) abuse and nefarious use of cloud remedies ist to strict registration and validation, scanning and blacklisting the network traffic.2) Insecure interfaces and APIs remedies is consumers ensures strong authentication and access control used by provider 3) malicious insiders, remedies are transparent access by the employee, records and compliances prepared 4) shared technology vulnerabilities 5) data loss and leakage, deletion or alteration of data without any content backup is horrible. Data is lost because of loss of encoding key or by unauthorized access., remedies are encrypt and check integrity of data, strong access API ,strong key management.6)account or service hijacking, these threats are man in middle attacks, phishing and DoS attacks. Remedies are prohibit the sharing of account credentials between service and users. 7) unknown risk profile, intrusion, vulnerabilities should always kept in mind.

Many business are putting their data on cloud data centers to improve resources utilization, speed development and deployment and reduce cost, however these new platforms are having additional avenues for threats against data, systems, network and reputation. These threats are data-stealing malware, web threats, spam, phishing, Trojans, worms, viruses, spyware, bots, and more. For most of the part all these threat are presented in the same kind of attacks [3]. In a recent survey conduct by trend micro on cloud and virtualization used by industry and business worldwide almost 45 percent are using public cloud and 46 percent are using private cloud. Inter virtual machines communications are blind to the traditional security appliances. This is said to be blind spot problem. The solution is to install a virtual machine that continuously coordinates the communication between VMs. Best practice is to provide self-defending VMs. Virtual servers are using the same resources as physical server. Hypervisor manage and coordinates all VMs on the same server.one threat to hypervisor is hyper jacking in which one VM may attack hypervisor. Once hypervisor compromised it attacks on other guest VMs. VMs can remain secure by using intrusion detection and prevention, a firewall, integrity monitoring, log inspection, and antivirus capabilities. Dormant virtual machines are upgraded with latest antivirus as become active. Virtualization-aware technology is required to minimize resource usage and increase VM densities. A dedicated scanning VM can coordinate staggered scans across VMs to preserve host resources. And agent-less antivirus removes the antivirus software from the guest VMs and centralizes these functions on the dedicated security VM, enabling a massive reduction in memory footprint for security on virtual hosts.

Author has proposed multiple file data checking model suitable for cloud storage [4]. Remote data checking (RDC) is based upon challenge response protocol. RDC is divided into two categories Provable Data Possession (PDP) and Proof of Retrievability (POR). PDP provides protection from corruption against large amount of data. POR provide protection against small amount of data.

Author has analyze and identified security weakness in window and linux OSs when deployed on cloud environment [5]. In window 7 authentication is performed by local security authority (LSA).Applications used LSA component to authenticate users. LSA relies on authentication package(AP) and security support providers(SSP). Linux authentication is based upon pluggable authentication modules (PAM). An identity management system (IdM) is integrated with underlying OS images in cloud that handles the user credentials to access these images otherwise underlying OS may be attacked by brute force or dictionary attacks when the VM is powered off. IdM is included because most of the window and linux authentication mechanism do not fit in cloud. IdM system also limits number of logins. For access control in window each securable object is associated with a security descriptor.

This paper proposed a secure data sharing in cloud environment [6]. The system model includes four parties the data owner, data consumer, cloud server(CS) and private key generator(PKG). PKG generates the public key for data owner and distribute the corresponding private key to data users. Data owner stores their data to cloud servers. The proposed scheme is based upon bilinear map. Each file is described by a set of attributes. The access tree is assigned to the files. The access tree is converted into Linear Secret Sharing Scheme (LSSS) matrix. Each user has set of attributes and a unique user id as his public key. For each user attribute there is a key to the user. A user can decrypt data on cloud server if he has a set of matched attribute. There is a user list on cloud server. The scheme integrates four randomized algorithms System initialization, Encryption, Key generation, Decryption to achieve effective, scalable and privacy preserving cloud data sharing service.

This paper focuses on security policies in cloud in IaaS model [7]. Security at the application level covers authentication, authorization, message integrity, confidentiality and operational defense. In IaaS model of the cloud operating system, applications and contents are managed and secured by cloud consumer. CSP is ensuring the security of platform and underlying infrastructure. IaaS had been used to host such as botnet attack. IaaS was subject to DoS attack. There are bugs in virtualization software which causes isolation failure in VMs. An eavesdropper may hear the talk in VMs shared memory. Hosting of OSs and applications are subject to policies of hosting nation. Users does not know the location of actual data. Identifying the location of the destroyed data and determining the number of copies may not be conceivable. There are outage risks in IaaS model. Two types of risks are there a permanent outage when CSP goes out of business and temporary because of cost effectiveness and service's issues. Another issue is performance issue in which more cloud users with limited hardware or transmission bandwidth causes service unavailability.

This paper proposed a virtualization intrusion tolerance system in cloud [8].The idea of intrusion tolerance is based upon hardware or software fault tolerance in distributed system. The proposed virtualized intrusion tolerance system tolerating F faulty replica in 2F+1 replicas and ensure that only F+1 active replicas to execute during intrusion free stage and rest of F replica are in passive mode. Replica manager consists of basic component, group communication system, replication logic, voter component and other component. Replica manager is running in system domain Dom0.Service replicas are running in customer domain DomU. CC-VIT permits only at most n-1/2 replica fails in a single recovery. Replica manger intercepts client request and forward the request to all replicas through group communication. When replica manager receives a number of results from replicas it uses majority voting and sends correct result to client. Replication logic specifically realizes the instantiation and initialization of service replica. If more than F replica fails because of some adversary then proactive recovery takes place which initializes the failed replica from some secure base.

3. Proposed Data Security Model

In recent years data outsourcing on cloud has been much popular. Outsourcing of data means the data owner moves their data and stores them on remote machine that is out of owner's network boundary and administration. The consumer of cloud storage belief on cloud provider that their data are secure and will be available on demand. To avail such services customer pays to the cloud provider. Outsourcing of data on cloud saves storage and maintenance cost. A number of security research on data outsourcing had been carried out in last decade. The research is going on data authentication and integrity. How clients ensures that their data is secure and avail on cloud and had not been lost or removed or the provider is not cheating the client. In cloud environment the service provider may hide data loss incidents or it may discard data that is rarely used in order to sell the same storage for multiple times.

In my work, I have proposed a proof of data possession model. In this model a client who wants to store their data on cloud first divide their data into equal size blocks (padding is used to make the blocks equal) and then encrypt each data block by using symmetric encryption technique, I have used AES encryption technique here. Client associates a block id with each block of encrypted data and store them on cloud along with block id. Now client generates public and private key using Boneh–Lynn–Shacham (BLS) signature scheme. I have used BLS signature here over RSA because BLS signature and verification computation cost is lesser than RSA. Client issues the private key to the cloud service provider. The proposed model is shown in figure 1 and figure 2.

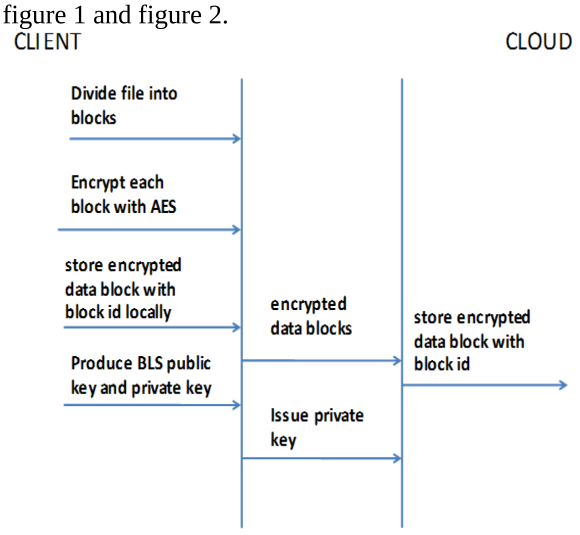
CLIENT
CLOUD
Divide file into blocks
Encrypt each block with AES
store encrypted data block with block id locally
Produce BLS public key and private key
encrypted data blocks
Issue private key
store encrypted data block with block id

FIGURE1: Data block computation and storage on cloud

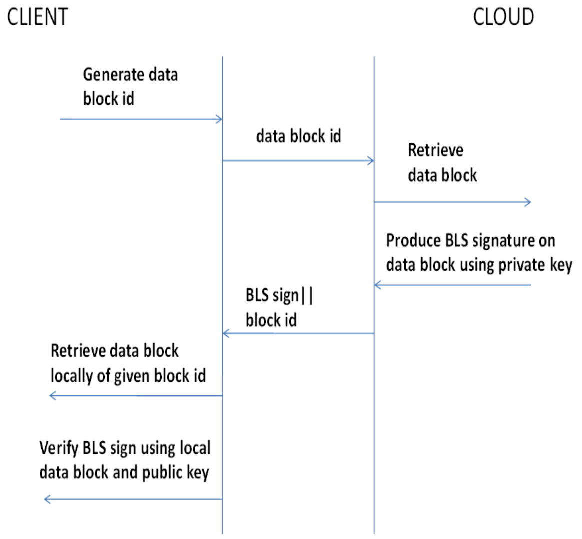
CLIENT
CLOUD
Generate data block id
data block id
Retrieve data block
Produce BLS signature on data block using private key
BLS sign||
block id
Retrieve data block locally of given block id
Verify BLS sign using local data block and public key

FIGURE2: Data block verification using BLS signature

Whenever client wants to verify their data stored on cloud, client generates a random block id and send the block id to the service provider. The cloud service provider (CSP) generates the BLS signature of encrypted data block using private key corresponding to received block id stored locally on provider side. Now the provider sends the signature appended with given block id. Now client receives the block id and verify the signature on encrypted data block stored locally on client side using public key. If the signature is verified with received signature then the client ensures that data is intact and stored securely on cloud side. Client can check their data on daily basis, a block in a day. For example suppose the file size is 1024 KB (2^{10} KB).If client divide the file into 4KB data blocks then total numbers of blocks are 256.Now client cam check one data block on daily basis for 256 days.

The aforementioned approach can also be written in following steps:

1. User divide data into equal size blocks say 4 KB.
2. User encrypt each data block by using AES encryption technique.
3. User associate a block id with each block.
4. User stores encrypted block locally and on cloud data center along with block id.
5. User produces BLS public and private key.
6. User issues private key to the cloud service provider
7. User chooses a random block and demand proof of data stored on cloud.
8. CSP receives block id and retrieve encrypted data from local store and produce BLS signature using private key.
9. CSP sends BLS signature along with block id.
10. Client receives signature and verify signature using local data block and public key.
11. If signature verifies then data stored on cloud is intact and safe.
12. Client assured data possession on cloud.

4. Experiment

Experiment is done on local server with intel core i3 2.4 GHz processor and 3GB memory. I have implemented the proposed model using java and net-beans IDE. I have used java security package for encryption and decryption. The experiments shows successful data block verification. The experiment snapshots are shown in figure3 and figure 4.

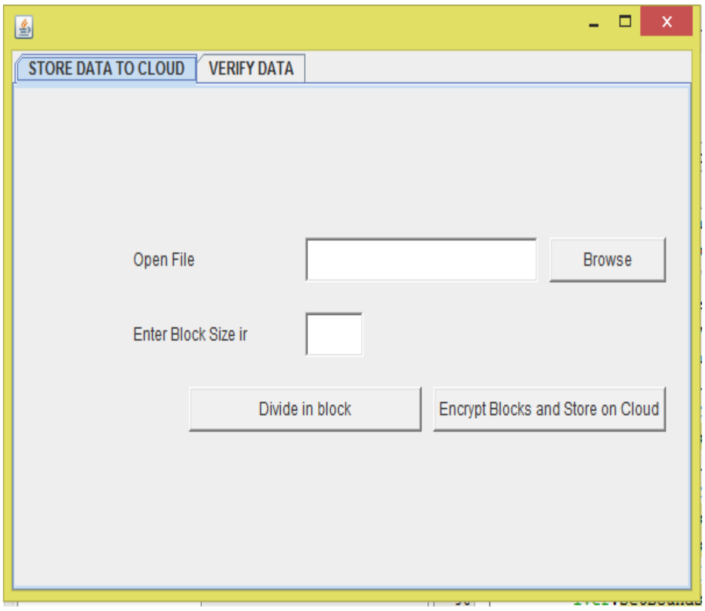

Figure 3: File division in blocks, encryption of block and store on cloud

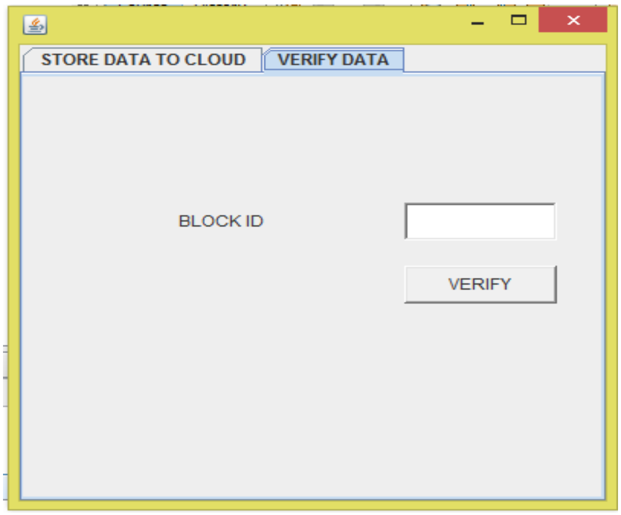

Figure 4: Data block verification

5. Conclusion

In this paper a secure data storage model on cloud is proposed and implemented using AES encryption and BLS signature. Such a data verification scheme are needed to cloud user that they can verify their cloud data locally, independent of cloud service provider. This model develops the users trust on cloud about their data security. The only overhead of this data model is time of encryption/decryption and verification that can be tolerated by using more sophisticated and optimized encryption technique.

References

[1] Jianfeng Yang, Zhibin Chen,"Cloud Computing Research and Security Issues" in IEEE-2010

[2] Gurdeep Singh Bindra et. al. "Cloud Security:Analysis and Risk Management of VM Images", 978-4673-2237-9/12 IEEE, 2012

[3] Virtualization and Cloud Computing: Security Threats to Evolving Data Centers, Trend Micro, 2012

[4] Da Xiao,"A Multiple-File Remote Data Checking for cloud storage", computers & security, Elsevier, 2011. H index: 43

[5] Khaled Salah," Analyzing the security of Windows 7 and Linux for cloud computing" computers & security, Elsevier, 2012. H index: 43

[6] Xin Dong et. al. "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing" computers & security, Elsevier, 2013. H index: 43

[7] Louay Karadsheh, "Applying security policies and service level agreement to IaaS service model to enhance security and transition" computers & security, Elsevier, 2013. H index: 43

[8] Yuesheng Tan, "CC-VIT: Virtualization Intrusion Tolerance Based on Cloud Computing" in IEEE, 2010.