2013 5th International Conference on Computational Intelligence and Communication Networks

A New Technique of Data Integrity for Analysis of the Cloud Computing Security

Rajkumar Chalse, Ashwin Selokar
Department of IT,
DMIETR, Sawangi(Meghe), Wardha
rajchalse@gmail.com, ashwin.selokar@gmail.com

Arun Katara
Department of ENTC
Sawangi(Meghe), Wardha
arunkatara@gmail.com

Abstract— **Cloud computing is a latest and fast growing technology that offers an innovative, efficient and scalable business model for organizations to adopt various information technology resources i.e. software, hardware, network, storage, bandwidth etc. Cloud Computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. It has the capability to incorporate multiple internal and external cloud services together to provide high interoperability there can be multiple accounts associated with a single or multiple service provider (SPs). So, Security in terms of integrity is most important aspects in cloud computing environment. In this paper, a detailed analysis of the cloud security problem is presented. Also the different problem in a cloud computing system and their effect upon the different cloud users are analyzed. It is providing a comparably scalable, position-independent. Low cost platform for client's data. Since cloud computing environment is constructed based on open Architecture and interface. Based on this analysis various computing system and their effect upon the system, upon organizations and also upon different cloud users are analyzed. It is providing a comparably scalable, position-independent, low cost platform for client's data. Since cloud computing environment is constructed based on open architecture and interface. Based on this analysis various researches have also presented a view of measures that can be taken to deal with the cloud security problem and prevention that must be taken into account by any organization and cloud users seeking investment in cloud computing.**

Keywords- *Cloud security, data storage, integrity verification, IaaS, PaaS, SaaS.*

I. INTRODUCTION

Many trends are opening up the era of Cloud Computing, which is an Internet–based development and use of technology. Consider the large size of the outsourced electric data and the Client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verification without the local copy of data files. Cloud computing is a flexible way to allocate information technology(IT) resources i.e. storage, software, infrastructures and bandwidth etc. out of a pool, enabling to consume processing power according to user's need. When there is a need to address peaks while saving costs when the users do not need the extra power any more. The global usage of a cloud leads to the optimization of resources so that in the end it makes them cheaper for everybody involved. The main objective of this paper is to provide security in terms of integrity and availability of client's data which is stored on cloud. This paper shall also be taken care of by allowing trusted party to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-time burden to cloud users. Cloud Computing allows computer users to have a convenient access to fully featured applications, to software development and deployment environment and to computing infrastructure assets such as network-accessible data storage and processing.

The model is also well-suited for small and medium business it helps adopting IT without upfront investments in infrastructure, software licenses and other relevant requirement.

II. DEFINITION OF CLOUD COMPUTING

The most widely used definition of the cloud computing model is introduced by National Institute of Standard Technology as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction." Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-tendency enables sharing the same services instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demand. Both characteristics focus on improving resources utilization, cost and service availability.

According to Electrical Engineering and Computer Science (EECS) University of California at Berkeley, cloud computing refers to both the application delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Services (SaaS). The data center hardware and software is what we will call a cloud. The US Department of Commerce's National Institute of Standard and Technology defined cloud computing as :"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources e.g. network, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

978-0-7695-5069-5/13 $26.00 © 2013 IEEE
DOI 10.1109/CICN.2013.103

IEEE computer society

III. NEED OF THE STUDY

Like all computing systems, cloud computing systems must have a need to consider security issues from the initial stages i.e. requirements stages and design stages of its development process. It will lead to a more robust, secure and less error prone system than those systems that identify security issues only once, when the system is place. Due to the complexity of the cloud environment, effective development of a cloud computing system needs an analysis of these security problems and requirement so that various policies could be developed earlier in the development process that will consider the entire cloud.

In cloud computing environment, internal threats have steadily increased over the past few years. Internal threat refers to those threats which occur within the organization. Internal users within an organization generally have more knowledge of the data stored there in and hence more informed about how to access that data and applications than do external users. Although internal threats cannot be entirely eliminated, some effective barriers can be developed to mitigate them.

IV. CONTRIBUTION

Our proposed agreement has two main contributions:

1) Efficiency and security: - The plan proposed by the is safer to the rely on a public and private key encryption will be clear, efficient in the use of Secret Key Gen and TagGen algorithm. In thus every time parameters are generated and key exchange takes place so more secure than symmetric and asymmetric algorithm. However, our plan is more efficient than the other techniques, because, it does not require lots of data encryption in outsourced and no additional posts on the symbol block, and ratio is more secure because we encrypt data to prevent unauthorized third parties to know its contents.

2) Public verifiability: We plan a major variation to provide public validation. Allow people other than the owner for information on the server has proved efficient because it does not need the information for each block encryption.

3) Related work: Nam Yem Li highlight PDP scheme use for verification to avoid public verification. This paper proposed initial PDP solution to RSA based Hash function to authenticate the remote server storage data. However, due to RSA based cryptography, the entire computing speed is slow.

Similarly Qian Wang et al, Proposed a protocol for Integrity verification in Multi cloud that is provided by improving the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, this paper further explore the technique of bilinear aggregate signature to extend the main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provable secure. This paper explored the problem of providing simultaneous public audibility and data dynamics for remote data integrity check in Cloud Computing. This Study proves the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block authentication. Major concern of this paper is, It is used to construct verification protocols that can accommodate dynamic data files. Subsequently Yan Zhu, focused on the Cooperative Provable possession scheme for integrity verification. This scheme is based on homomorphic verifiable response and hash index hierarchy for data access. This paper issued, to prove the security of scheme based on multi-provers zero knowledge proof system. It provides Integrity with lower computation to non cooperative approach. However, while checking for large files, integrity is affected by the bilinear mapping operations due to its high complexity. And generation of tags with the length irrelevant to t size of data blocks is a challenging task of this paper.

V. DATA INTEGRITY FOR CLOUD ENVIRONMENT

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors. To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theories that are needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded data. Subsequently, it is also shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. Finally, the procedure for file retrieval and error recovery based on erasure-correcting code is outlined. B.

The main idea is to outsource the file before the data block encryption, and validation of fixed-size tags, each tags ate included in the block information. Although ,the CPDP scheme offer a publically accessible remote interface for checking and managing the tremendous amount of data, the majority of exiting CPDP schemes are incapable to satisfy the inherent requirements from multiple clouds on terms of communication and computation costs. To address this problem, we consider a multi-cloud storage service as shown in fig.

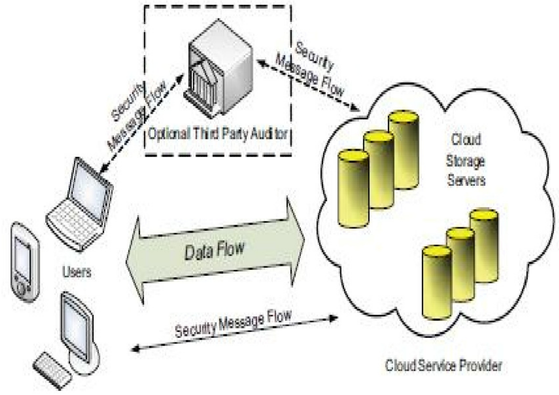


Fig. 1: Cloud data storage architecture

A. System Architecture:

In this architecture, a data storage service involves three different entities. Client who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data cloud service providers(CSP) who work together to provide data storage services and have enough storage and computation resources. And Trusted Third Party(TTP) who is trusted to store verification parameters and offer public query services for these parameters.

In this architecture, we consider the existence of multiple CSPs to cooperatively store and maintain the clients data. Moreover, a cooperative PDP is used to verify the integrity and availability of their stored data in all CSPs. The verification procedure is describe as follows: Firstly, a client(data owner) uses the secret key to pro-process a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP, transmit the file and some verification tags to CSPs and may delete its local copy; Then, by using a verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP.

Protocol Directions:

We neither assume that CSP is trust to guarantee the of the stored data, nor assume that data owner has the ability to collect the evidence of the CSPs fault after errors have been found. To achieve this the cloud for the sake of security. The verification procedure is described as follows: Firstly, a client(data owner) uses the secret key to pre-process a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP,, transmit the file and some verification tags to CSPs , and may delete its local copy. Then, by using this verification protocol, the clients can issue a challenge for one CSPs to check the integrity and availability of outsourced data either respect to public information stored in TTP.

In proposed system a cooperative provable data possession in cross cloud S=(SecretKeyGen) is a collection of two algorithm and an interactive proof system proof, as follows:

SecretKeyGen(I^K):Takes a security parameter k as input, and returns a secret key Sk or a public-secret key pair(Pk,Sk);

Proof(P,V): Is a protocol of proof of data possession between CSPs(P=Pk) and a verify (V), that is, <∑ Pk E P P^k **,** $F^{(k)}$,V_p $^{(k)}$ (Pk,V_p) where Pk takes input file $F^{(k)}$ and a set of public parameters V_p is the common input between P and V. At the end of the protocol run, V returns a bit {0/1} denoting false and true.This is proposed cross cloud scheme for key generation, tag generation and verification protocol.

VI. OBJECTIVES

The objective of the study is to analyze the security requirement and highlight the existing threats in cloud computing effective security policies for cloud computing systems. It will help the researchers to identify security requirements at multiple levels to recognize the threads in the various cloud computing models posed by both internal and external users an thus will help to clarify cloud security policies that ensure the security of the cloud environment.

VII. CLOUD COMPUTING MODELS

Basically there are two types of models of cloud computing which depends upon the way how these models are deployed and services they provide.

A. Deployment Models:

Deployment models refer to those models which are based upon the deployment of different computing resources. A cloud computing system may be deployed privately or hosted on the premises of a cloud customer, may be shared among a limited number of trusted partners, may be hosted by a third party, or may be a publically accessible service, i.e. a public cloud depending on the kind of cloud deployment, the cloud may have limited private computing resources, or may have A. access to large quantities of remotely accessed resources.

B. Service Models:

A cloud can provide access to software applications such as email of office productivity tools (the software as a Service (SaaS), or can provide a toolkit for customers to use to build and operate their own software (the platform as a Service(PaaS)model), or can provide network access to traditional computing resources such as processing power and storage (the Infrastructure as a Service(IaaS)model). The different service models have different strengths and are suitable for different customers and business objectives. Generally, interoperability and portability of customer workloads is more achievable in the IaaS service model because the building blocks of IaaS offering are relatively well-defined.

There are following type of cloud service models:

1)Cloud Software as a Service(SaaS)- The capability provided to the consumer is to use the provider's applications running on a clouds infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser e.g. web-based email. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited use-specific application configuration setting.

2) Capability provided to the consumer is to deploy on to the cloud infrastructure consumer-created or consumer acquired applications created using programming languages and tools supported by the provider. The consumer does not mange or control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possibly application hosting environment configurations.

3) Cloud Infrastructure as a Service(IaaS)- The capability provided to the consumer is to provide processing, storage,

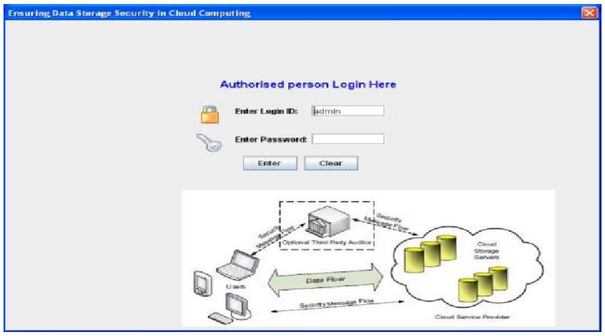
4) Networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications. In IaaS most of the services are provided virtually on virtual machines (VMs) e.g. data storage, firewalls and networks etc.

VIII. SECURITY ANALYSIS

The section will analyze the static PDP hybrid security agreement to confidentiality, integrity and confirm the analysis of three aspects. Confidentiality the owner of the file is stored on the server before will use the cryptosystem to encrypt the data to ensure that the file will not be Intercepted by an unauthorized person to get the file content. Because encryption and decryption SecretKeyGen and VeriTagGen cryptosystem uses public key and private key, security is based on calculating private key. Until and unless you don't know private key, you can't decrypt the cipher text file M.

Integrity in the verification phase, the owner would like to verification cipher text M is a complete file stored on the server at this time, the sever will calculate the value of z to prove he has complete store cipher text file M. If the server is calculated z calculated with the owner of the verification value is equal to V, it means the server does have the correct storage cipher text file M.

IX. SNAPSHOT



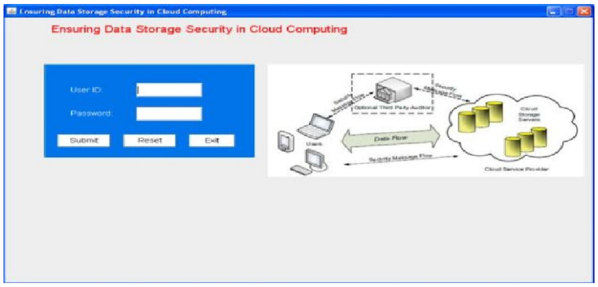
Ensuring Data Storage Security in Cloud Computing

Authorised person Login Here

Enter Login ID: admin

Enter Password:

Fig 1 Cloud Server Login



Ensuring Data Storage Security in Cloud Computing

Ensuring Data Storage Security in Cloud Computing

User ID:

Password:

Fig 2 Client Server Side

X. CONCLUSION AND FUTURE SCOPE

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage .The cloud computing model is one of the promising computing models for both cloud providers and cloud consumers. But to best utilize the cloud computing model there is a need to solve the existing security problems. We can use cooperative provable data possession scheme, which reduce the data block access, and amount of computation on the server and client. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. Our design and development is mainly based on the usage of Public and Private key encryption system. It support dynamic outsourcing of information make it a more realistic application of cloud computing .In future the work on mapping security requirement to the cloud architecture, and developing some security algorithm for cloud systems will be carried on. These security algorithms may be either Software based e.g. Encryption based or may be Hardware based e.g. Disk encryption hardware. It will help in improving the security of cloud systems and hence will lead to remove the fear of data security among users and thus adoption of cloud computing systems by business organizations.

REFERENCES

[1] Frank Gens, Revert, P Mahowald and Richard L Villars, “Cloud computing: benefits, risks and recommendations for information security”,November2009.

[2] Peter Mell and Tim Grace,” The NISTdefinition of cloud computing”, at National Institute of Standards and Technology, Gaithersburg, MD 20899-28930, September 2009.

[3] Wikipedia Contributors, The, free encyclopedia,Wikimedia foundation,inc.22July2004.Web.10Aug2004,<en.wilipedia.org./wiki/-cloud_computing_security>, Last accessed on April 2012.

[4] Jensen, Schwenk,J.Gruschka, and lacono,”On technical security issues in cloud computing”, In IEEE, International conference on cloud computing,pp.109,21-25,September 2009.

[5] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws.amazon.com, 2008.

[6] S. T. J. Fenn, M. Benaissa, and D. Taylor, “GF(2m) multiplication and division over the dual basis,” IEEE Trans. Comput., vol. 45, no. 3, pp.319–327, Mar. 1996.

[7] A. Pincin, “A new algorithm for multiplication in finite fields,” IEEE Trans. Comput., vol. 38, no. 7, pp. 1045–1049 , Jul. 1989.

[8] M. Kovac´ and N. Ranganathan, “SIGMA: a VLSI systolic array implementation of a Galois field GF(2m) based multiplication and division algorithm,” IEEE Trans. Very Large Scale (VSLI) Syst., vol. 1, no. 1, pp.22 –30, Mar. 1993.

[9] S. Y. Kung, VLSI Array Processors. Englewood Cliffs, NJ: Prentice-Hall, 1988.

[10] N. Weste and K. Eshraghian, Principles of CMOS VLSI Design: A System Perspective