ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Cloud Storage Security And Providing Integrity Proof

Prof. Avinash C Taskar*, Prof. Mangesh T Nikam

* Computer Engineering Department,Sandip Institute Of Engineering & Management,Sandip Foundation's, India

Electronics & Telecommunication Engineering Department, Sandip Institute Of Engineering & Management, Sandip Foundation's, India

avinash.taskar@gmail.com

Abstracts

Cloud computing has been envisioned as the next-generation architecture and solution to the rising storage costs of IT Enterprises. Cloud faithfully stores the data and return back to the owner whenever needed. But there is no guarantee that data stored in the cloud is secured and not altered. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed schemes. the cloud stores the clients data in comma separation form(CSV) form. As part of the verification process we assume that the TPA is reliable and independent according to the service level agreements (SLA), which does not mean that there is no space for the TPA to cheat. The approach used for the encryption in the verification process was the blowfish algorithm..Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. The aim of this research is two fold 1) ensuring the integrity of the data and 2)provides the proof that data is in secured manner.

Keywords: CSV module, Third Party Auditors, SOAP protocol, ERP system, blowfish cryptography.

Introduction

Cloud computing has been involved in everyday life. "Cloud computing is a model for enabling present, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[5].

The use of cloud computing has increased rapidly in many organizations. The small and medium companies use cloud computing services for various reasons, because these services provide fast access to their applications and reduce their infrastructure costs. Even most of us utilize cloud computing services on a daily basis. For example, we use web-based email systems (e.g. Yahoo and Google) to exchange messages with others; social networking sites (e.g. Facebook, LinkedIn, MySpace, and Twitter) to share information and stay in contact with friends. In spite of these benefits, "cloud" lack in some of the issues like data integrity, data loss, unauthorized access, privacy etc[2].

Data integrity of the data is very important. Because data integrity guarantees that data is of high quality, correct, consistent and accessible.

Basic concept

Cloud

The cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic – a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing. A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

of cloud computing is to provide easy, scalable access to computing resources and IT services. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)[1]. The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

Software as a Service (SaaS): In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere[1].

Platform as a Service (PaaS): Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure.

Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform. In short clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds[1].

Infrastructure as a service (IaaS): Infrastructure-as-a-Service like Amazon Web Services provides virtual server instanceAPI) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's sometimes referred to as utility computing. Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity[1].

Cloud Storage

The procedure of storing data in the remotely located cloud servers are said to be cloud storage.Cloud storage is much better than other traditional storage methods. Some of the reason for that are

- Companies do not need to install physical storage devices their own datacenter or offices.
- Storage maintenance task , such as back up and purchasing additional storage devices are disposed from the responsibility of a service provider allowing the organization to focus on their core business.
- Companies need to only pay for the storage they actually use.

Literature review

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited[6].

In cloud computing enormous threats are raised. One of the threats is data privacy and integrity. A lot of researchers focused on proving data integrity in the cloud and introduce many solutions to decrease the threat of the data privacy and integrity. Calce [1] says about cloud computing, putting everything into a single box will only make it easier for hackers. Moving to a virtual environment to save on costs automatically introduces fresh risk on top of existing risk. Priya Metri

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

and Geeta Sarote [2] introduce threat model to treat the privacy problem in the clouds. One of the service is third party auditing because it notify the threats in cloud computing is tampering with data in the cloud that interfere with the unauthorized modifications for the data, which lead to an effectiveness processors, data storage and data flow Proofs of Retrievability(POR) model proposed by Juels and Kaliski [3] are among the first few attempts to formulize the notion of "remotely and reliably verifying the data integrity without retrieving the data file". Archival network storage [4] presents unique performance demands. File data are large and are stored at remote sites, accessing an entire file is expensive in I/O costs to the storage server and in transmitting the file across a network. Reading an entire archive, even periodically, greatly limits the scalability of network stores. Furthermore, I/O incurred to establish data possession interferes with on demand bandwidth to store and retrieve data .Previous solutions do not meet these requirements for proving data integrity. Some schemes provide a weaker guarantee by enforcing storage complexity moreover; all previous techniques require the server to access the entire file, which is not feasible when dealing with large amount of data.

The proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data and their proposed secure provenance scheme To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information. kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment. They have claimed that there proposed security model for cloud computing is a practical model cloud computing. The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

To check the integrity of stored data without download, some researchers have proposed two basic approaches called provable data possession (PDP) and proofs of retrievability (POR) first proposed the PDP model for ensuring possession of files on untrusted storages and provided an RSA-based scheme for the static case that achieves communication costs They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the servers for data possession. This property greatly extend application areas of PDP protocol due to the separation of data owners and the authorized users. This work is motivated by the public audit systems of data storages and provided a privacy-preserving auditing protocol. Moreover, this scheme achieves batch auditing to support efficient handling of multiple auditing tasks. Although their solution is not suitable for practical applications because of lack of support for dynamic operations and rigorous performance analysis, it points out a promising research direction for checking the integrity of outsourced data in untrusted storage.

Proposed system

In this paper ,we propose ensuring the integrity of data and provides the proof that data is in secured manner. It provides a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud using blowfish algorithm.

The main objective of our work is to provide integrity using encryption and providing cryptographic key to secure the data in cloud. Hence data stored on the cloud will be in the encrypted form which can not be read by any unauthorized user. Using blowfish algorithm we are providing integrity to data and providing security by giving cryptographic key to prevent access of data by unaunothrised user. By creating ERP system through which we are storing data on cloud which is in encrypted format and it also maintains record of the data.

The system describes that, if user (cloud client) likes to store a file (F) in the cloud server . Before storing the file to the cloud, system needs to encrypt the file in order to prevent from the unauthorized access.
Company who is wishes to go for cloud storage service must be an authorized user and register themselves as a client. For every authorized user the system will generate a security key. Secret key is used while owner needs to login The proposed system ensures that unauthorized users are not permitted to login and verify the data stored by user at remote storage in the cloud is not modified by the cloud.
The interpretation of the system is shown in the fig. below

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

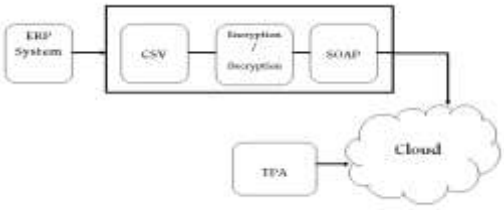

Fig.1 block diagram for system

The above block diagram describes the working of the proposed system, it includes modules such as ERP system, comma Separated values(CSV), SOAP protocol and TPA module.

ERP System : User may be an ERP system or business organizations who use cloud for data storage. We are creating ERP system through which we are storing data on cloud. In ERP system users account will be created.

CSV module: After parsing CSV file is generated from database as CSV files are known as "Comma Separated values" it is easy to upload on cloud as its file size is reduced and it provides double security. CSV Parser is used for deciphering the text.

SOAP protocol: SOAP originally defined as "Simple Object Access Protocol" is a protocol specification for exchanging structured information in the implementation of web services in computer networks. It relies on Comma separated values (CSV) files for its message format and usually relies on other application layer protocols. This SOAP protocol is used for interfacing with Cloud Service Provider (CSP).

Encryption: This system will accept normal data then it will encode the given data, after encoding it will provide encrypted data in cipher text , which is processed as this system deals with the database of ERP or organization's transactional data in real time, such as encrypted fields, records, rows, or column data in a database. Once encryption is done then that cipher text will be deciphered by CSV Parser. It will provide security to data, so that no unauthorized user can view, modify, delete the data of ERP. For encryption process Blowfish algorithm is used.

Third Party Auditor (TPA): An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to users. Also TPA will give alerts to users whenever some other person tries to attack data or unauthorized access to data in cloud storage. Once the data is stored on cloud in secured form,and if the user or ERPwants to retrieve that data, then user or ERP can use private key and can retrieve data from that cloud.

Algorithm

Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

The working of blowfish algorithm is given below

- The data provided by the user in the blowfish algorithm is act as an input.
- After that divide the complete data into large block with the block size 64 bits.
- The blowfish algorithm works in two parts first one is Key expansion and the second one is data encryption.
- In key expansion, the input key is converted into several subkey and the total array bytes are 4168
- This subkey must be pre-computed before any data encryption and decryption
- After the subkey generation data is ready for encryption.The data encryption occurs via 16-rounds of fiestel network.
- Each round consist of key dependent permutation and key 8 data substitution. All operations are perform in these algorithm are XOR and addition of 32 bit words.The only addition operations are four indexed array data lookups per round.
- In these algorithm the Decryption is perform in the same way; just we need to go in reverse order.
- Feistel Networks: A Feistel network is a general method of transforming any function (usually called an F function) into a permutation. It was invented by Horst Feistel and has been used in many block cipher designs. The working of a Feistal Network is given below:
- Split each block into halves
- Right half becomes new left half

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

- New right half is the final result when the left half is XORd with the result of applying of to the right half and the key.
- Note that previous rounds can be derived even if the function f is not invertible.

Conclusion

This we conclude by briefly explaining about the cloud storage, advantages along with its characteristics. The proposed system provides the proof of the data integrity and the owner can check the integrity of their data in efficient manner. If any modifications did by the TPA, cloud will immediately intimate to the owner of the file. So Security and data integrity is secured properly. And it reduces the access time at the cloud server and reduces the cost for retrieving the file and bandwidth consumption across the network.

References

1. E. Mykletun, M. Narasimha, and G. sudik,"Authentication and integrity in outsourced databases,"Trans. Storage, vol. 2, no. 2, pp. 107-138, 2006.
2. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data,"in SP ’00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA:IEEE Computer Society, 2000, p. 44.
3. A. Juels and B. S. Kaliski, Jr, "Pors: proofs of retrievability for large files," in CCS ’07: Proceedings of the 14th ACM conference on Compute and ommunications security.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,andD.Song, "Provable data possession at untrusted stores,"in CCS ’07: Proceedings of the 14th ACM conference on Computer and communications security.
5. ACA Research, Software-as-a-Service (SaaS) in Australia: Is it the Next Big thing?
6. Paul Zimski, Cloud computing faces security storm in 2009.
7. Jia xu and Ee-chien chang, Towards efficient proofs of retrievibility in cloud storage
8. A. Juels and B.S. Kaliski, Jr., Pors: proofs of retrievability for large files, In CCS07 Proceedings of the 14th ACM conference on Computer and communications security.
9. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, Provable data Possession at untrusted stores, in CCS 07.[10] Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and eciently searchable encryption. Advances in Cryptology { CRYPTO, pages 535{552, August 2007