ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Ensure Security of Data in Storage Nodes in Cloud

[I]Mr.S.Samsudeen, [II]Mr.M.Vadivel
[I,II]Asst.Professor, Dept.of CSE, Sethu Institute of Technology, Kariapatt, Tamilnadu, India

Abstract
Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could beused andmisused by amiscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers(CSPs), often without users' authorization and control. Self-destructing data mainly aims at protecting the user data's privacy. All thedata and their copies become destructed or unreadable after a user-specified time, without any user intervention. In addition, the decryp-tion key is destructed after the user-specified time. In this paper, we present SeDas, a system that meets this challenge through a novelintegration of cryptographic techniques with active storage techniques based on T10 OSD standard. We implemented a proof-of-con-cept SeDas prototype.

Keywords
Cloud Service Providers(CSPs), Storage Nodes, Time to Live(TTL), Time Stamp

I. Introduction

SEVERAL trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. The computing resources are maintained by the provider, the total cost of ownership to the consumers can be reduced Ownership to the consumers can be reduced. In cloud computing, a resource provisioning mechanism is required to supply cloud consumers a set of computing resources for processing the jobs and storing the data. Cloud providers can offer cloud consumers two resource provisioning plans, namely short term on demand and long-term reservation plans. Amazon EC2 and Go Grid are, for instances, cloud providers which offer IaaS services with both plans. In general, pricing in on-demand plan is charged by pay-per-use basis (e.g., 1 day). Therefore, purchasing this on-demand plan, the consumers can dynamically provision resources at the moment when there sources are needed to fit the fluctuated and unpredictable demands. For reservation plan, pricing is charged by a one-time fee (e.g., 1 year) typically before the computing resource will be utilized by cloud consumer. With the reservation plan, the price to utilize resources is cheaper than that of the on-demand plan. In this way, the consumer can reduce the cost of computing resource provisioning by using the reservation plan. For example, the reservation plan offered by Amazon EC2 can reduce the total provisioning cost up to 49 percent when the reserved resource is fully utilized (i.e, steady-state usage) .With the reservation plan, the cloud consumers a prior I reserve the resources in advance. As a result, the under-provisioning problem can occur when the reserved resources are unable to fully meet the demand due to its uncertainty .Although this problem can be solved by provisioning more resources with on-demand plan to fit the extra demand, the high cost will be incurred due to more expensive price of resource provisioning with on-demand plan. On the other hand, the over provisioning problem can occur if the reserved resources are more than the actual demand in which part of a resource pool will be underutilized.

II. Problem Definition

A. Existing System

People rely more and more on the Internet and Cloud technology, security of their privacy takes more and more risks. When data is being processed, transformed and stored by the current computer system or network, systems or network must cache, copy or archive it. These copies are essential for systems and the network.

B. Limitations of Existing system

1. People have no knowledge about these copies and cannot control them, so these copies may leak their privacy.
2. Privacy also can be leaked via Cloud Service Providers (CSPs') negligence, hackers' intrusion or some legal actions.
3. These problems present formidable challenges to protect people's privacy.

III. System Design

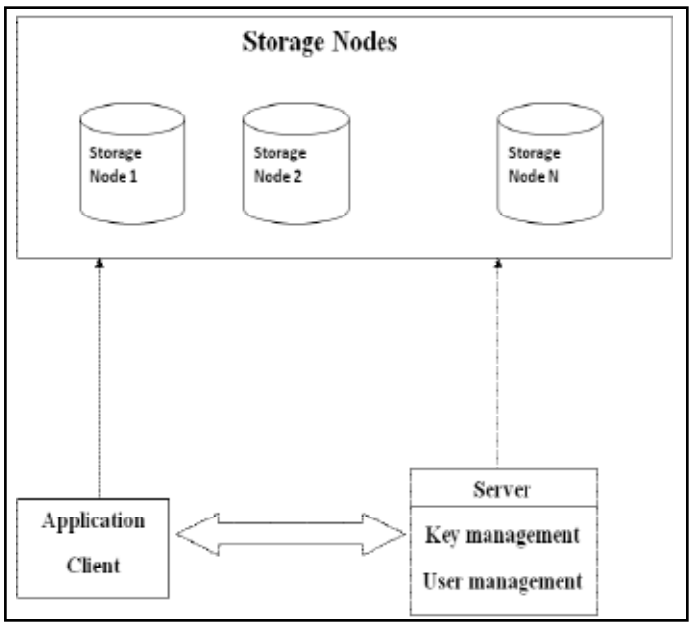
A. Proposed System

1. Shamir's algorithm is used as the core algorithm to implement client distributing keys in the object storage system.
2. Storage interface is used to store and manage the equally divided key.
3. It supports security erasing files and random encryption keys stored in a hard disk.
4. All the data and their copies become destructed or unreadable after a user-specified time, without any user intervention.

B. Merits of Proposed System

1. SeDas can meet the requirements of self-destructing data with controllable survival time while users can use this system as a general object storage system.
2. It is practical to use and meets all the privacy-preserving goals and imposes low overhead.

Architecture Diagram



IV. Modules Description

Our Proposed work has the following modules. There is Listed Below

1. User and Storage node Key Sharing
2. Data Process
3. Active Storage Object
4. Self Destruction Model

A. User and Storage node Key Sharing

- Generate random keys from user
- Sharing of keys between the meta server and the User application
- Enable N storage node for storing the data's
- Sharing the storage node with meta server for shaminar key sharing technique

B. Data Process

Data processing in the sedas will have two main phases

C. Upload and Download

File Uploading process will send the Upload request to the serverAfter accepting get the N keys randomly from the user key.Spling the File into the N parts using shaminars shard keys. Encrypt the file using the Key value.Provide the Time Stamp (TTL) for the File

File Downloading Process will send the download request to the server.If the file available in the network accept the download request.Downloading the file And Merge it.

D. Active Storage Object

1. It will be held at Storage node.
2. For this one first we receive the File split from the user application.
3. Get the Time stamp for the user application file
4. Create the interface
5. Store the files to the storage node and apply the security mechanism.

E. Self Destruction Model

1. Time monitoring process will held
2. If the time stamp exceed the document will be automatically destroyed
3. The Store space will be refreshed
4. Details of the document also removed from the Metaserver.

V. Conclusion & Future Enchancement

Data security is very important in the cloud computing. Using our system we can provide security to the data. The active storage framework is used to delete the data from the storage node without asking any permission from the client. The data in cloud contains the sensitive information such as account numbers, passwords etc. The security of the data in the cloud must be improved . For that the Blowfish algorithm is best suited for data security. And then the integrity of the data is also very important. The MACis used for confirm the data integrity. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits and making it ideal for securing data. It is a variable-length key block cipher. Blowfish is a symmetric block cipher, was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Much faster than DES and AES. Besides, it is unpatented and no license is required. Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. In cryptography, a message authentication code (often MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin. A MAC algorithm, sometimes called a keyed hash accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content.

References

[1] *R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasingdata privacy with self-destructing data," in Proc. USENIX SecuritySymp., Montreal, Canada, Aug. 2009, pp. 299–315.*

[2] *S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman,C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanishwith low-cost sybil attacks against large DHEs," in Proc. Network andDistributed System Security Symp., 2010.*

[3] *L. Zeng, Z. Shi, S. Xu, and D. Feng, "Safevanish: An improved dataself-destruction for protecting data privacy," in Proc. Second Int. Conf.Cloud Computing Technology and Science (CloudCom), Indianapolis,IN, USA, Dec. 2010, pp. 521–528.*

[4] *L. Qin and D. Feng, "Active storage framework for object-basedstorage device," in Proc. IEEE 20th Int. Conf. Advanced InformationNetworking and Applications (AINA), 2006.*

[5] *Y. Zhang and D. Feng, "An active storage system for high performancecomputing," in Proc. 22nd Int. Conf. Advanced InformationNetworking and Applications (AINA), 2008, pp. 644–651.*

[6] *T. M. John, A. T. Ramani, and J. A. Chandy, "Active storage usingobject-based devices," in Proc. IEEE Int. Conf. Cluster Computing,2008, pp. 472–478.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[7] *S. W. Son, S. Lang, P. Carns, R. Ross, R. Thakur, B. Ozisikyilmaz,W.-K. Liao, and A. Choudhary, "Enabling active storage on parallelI/O software stacks," in Proc. IEEE 26th Symp.Mass Storage Systemsand Technologies (MSST), 2010.*

[8] *Y. Xie, K.-K. Muniswamy-Reddy, D. Feng, D. D. E. Long, Y. Kang,Z. Niu, and Z. Tan, "Design and evaluation of oasis:An active storage ramework based on t10 osd standard," in Proc. 27th IEEE Symp.MassiveStorage Systems and Technologies (MSST), 2011.*

Author's Profile and Image

Samsudeen S, Asst.Professor, Dept. of CSE, Sethu Institute of Technology, Kariapatt, Tamilnadu, India