ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

DATA SECURING IN CLOUD COMPUTING BY USING MIRRORING CONCEPTS

S.NAGASUNDARAM[1]
[1]Research Scholar, Department of Computer Science and Applications,
SCSVMV University, Kanchipuram -631 561.
Tamil Nadu, India.
naga.smec@gmail.com

DR.S.K.SRIVATSA[2]
[2]Professor(Retd.),Anna University, MIT Campus, Chennai – 600 025
Guide,SCSVMV University,Kanchipuram-631561.
Tamil Nadu, India.
profsks@rediffmail.com

Abstract— Cloud Computing is vast and tremendous development and the security levels also enhanced. The security methodologies are different levels and types. We can use some mathematical algorithms, cryptography method and encryption methods. I have implemented one of the algorithms for storing the data in mirroring data in another location the users. Data storage are different levels, that can manually and automatically. The mirrored data are duplicate copy of dummy record will be stored, the third person will hacking the data it will display the dummy file but it contain the wrapper of original file name.

Keywords: Cloud Computing, Security, Storage, Mirrored object and types.

Introduction

In the earlier sections, we discussed the common techniques of how application developers check for a rooted device and then how an attacker can bypass some of the techniques used by the developers. In this section, we will discuss different methods being used by Android developers to store data in the mirroring object, and then we will see how secure these methods are. Cloud computing is a model that enables the development,

In this method we have to store the data in cloud systems. The original data are stored in main cloud, as well as the same type of file or data type in the form of duplicate will be stored in additional cloud in the method mirroring objects. When ever the valid user accessing the original data or files are retrieved. If the hackers or unauthorized person enter the cloud it will display the duplicate files or data.

The duplicate data or files are contain label of content but the file or data are empty. This is one of the best example of the virus will create a duplicate folder. The valid user access and modification are done in the original files. The unauthorized person always getting a dummy or duplicate files. A random number generated to create a duplicate files from the source of original files. The hackers or unauthorized person always to find the dummy files or without content of empty file. The main source of content always available in main cloud and user location.

Fake cloud computing is a response to the popular cloud computing software buzz. Many companies are taking their on-premise applications and creating a "cloud version." The only problem is that the claims of being cloud computing financial software are often false and misleading. An example of this is Microsoft, who is taking their Dynamics Software Suite and attempting to put it in the cloud.

The Gartner Group recently commented on this trend by stating, "…because SaaS and cloud computing are hot concepts in the market, many suppliers are re-branding their hosting or application management or application outsourcing capabilities asSaaS or are claiming their solutions are available 'in the cloud'…suppliers run the risk of confusing and antagonizing buyers if they persist with this approach."

The Dangers of Fake Cloud Computing

In fake cloud computing, on-premise software is hosted by a value-added reseller (VAR) or another service provider. The risks with this model are related to waiting for upgrades, process integration and the business viability of your service provider. VAR's that host fake clouds are consolidating regularly and there is no guarantee how long they will be around. Also, they cannot afford to purchase equivalent security systems that a real cloud solution uses.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

I. IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. It can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

The convergent encryption technique has been proposed to encrypt the data before outsourcing. To better protect data security, this paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. We also present several new deduplication constructions supporting authorized duplicate check in a hybrid cloud architecture. Security analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement a prototype of our proposed authorized duplicate check scheme and conduct test bed experiments using our prototype. We show that our proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

Convergent encryption:

Convergent encryption provides data confidentiality in deduplication. A user (or data owner) derives a convergent key from each original data copy and encrypts the data copy with the convergent key. In addition, the user also derives a *tag* for the data copy, such that the tag will be used to detect duplicates. Here, we assume that the tag correctness property holds, i.e., if two data copies are the same, then their tags are the same. To detect duplicates, the user first sends the tag to the server side to check if the identical copy has been already stored. Note that both the convergent key and the tag are independently derived, and the tag cannot be used to deduce the convergent key and compromise data confidentiality. Both the encrypted data copy and its corresponding tag will be stored on the server side. Formally, a convergent encryption scheme can be defined with four primitive functions:

• KeyGen CE (M) $\rightarrow K$ is the key generation algorithm that maps a data copy M to a convergent key K;

• Enc CE (K , M) $\rightarrow C$ is the symmetric encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a ciphertext C;

• Dec CE (K , C) $\rightarrow M$ is the decryption algorithm that takes both the ciphertext C and the convergent key K as inputs and then outputs the original data copy M; and

• TagGen (M) $\rightarrow T$ (M) is the tag generation algorithm that maps the original data copy M and outputs a tag T (M).

Proof of ownership.

The notion of proof of ownership (PoW) enables users to prove their ownership of data copies to the storage server. Specifically, PoW is implemented as an interactive algorithm (denoted by PoW) run by a prover (i.e., user) and a verifier (i.e., storage server). The verifier derives a short value ϕ (M) from a data copy M. To prove the ownership of the data copy M, the prover needs to send ϕ' to the verifier such that $\phi' = \phi$ (M). The formal security definition for PoW roughly follows the threat model in a content distribution network, where an attacker does not know the entire file, but has accomplices who have the file. The accomplices follow the "bounded retrieval model", such that they can help the attacker obtain the file, subject to the constraint that they must send fewer bits than the initial min-entropy of the file to the attacker.

Identification Protocol.

An identification protocol Π can be described with two phases: Proof and Verify. In the stage of Proof, a prover/user U can demonstrate his identity to a verifier by performing some identification proof related to his identity. The input of the prover/user is his private key skU that is sensitive information such as private key of a public key in his certificate or credit card number etc. that he would not like to share with the other users. The verifier performs the verification with input of public information pkU related to skU. At the conclusion of the protocol, the verifier outputs either accept or reject to denote whether the proof is passed or not.

Private Cloud:

Compared with the traditional deduplication architecture in cloud computing, this is a new entity introduced for facilitating user's secure usage of cloud service. Specifically, since the computing resources at data user/owner

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

side are restricted and the public cloud is not fully trusted in practice, private cloud is able to provide data user/owner with an execution environment and infrastructure working as an interface between user and the public cloud.

The private keys for the privileges are managed by the private cloud, who answers the file token requests from the users. The interface offered by the private cloud allows user to submit files and queries to be securely stored and computed respectively. Notice that this is a novel architecture for data deduplication in cloud computing, which consists of a twin clouds (i.e., the public cloud and the private cloud). Actually, this hybrid cloud setting has attracted more and more attention recently. For example, an enterprise might use a public cloud service, such as Amazon S3, for archived data, but continue to maintain in-house storage for operational customer data. Alternatively, the trusted private cloud could be a cluster of virtualized cryptographic co-processors, which are offered as a service by a third party and provide the necessary hardware based security features to implement a remote execution environment trusted by the users. [5] discussed about Enhancement of TCP Throughput using enhanced TCP Reno Scheme. Mobile Ad-Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread application in military and civilian communications. Based on the analysis, we proposed two simple yet effective ways, namely, TCP Few and ROBUST, to improve the system performance. It was shown via computer simulation that TCP performance can be significantly improved without modifying the basic TCP window or the wireless MAC mechanism. Thus, the TCP window mechanism can still be a viable solution for IEEE 802.11 ad-hoc networks.

Data Users:

A user is an entity that wants to outsource data storage to the S-CSP and access the data later. In a storage system supporting deduplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users. In the authorized deduplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized deduplication with differential privileges.

Design Goals:

In this paper, we address the problem of privacy preserving deduplication in cloud computing and propose a new deduplication system supporting for

• ***Differential Authorization***. Each authorized user is able to get his/her individual token of his file to perform duplicate check based on his privileges. Under this assumption, any user cannot generate a token for duplicate check out of his privileges or without the aid from the private cloud server.
• ***Authorized Duplicate Check***. Authorized user is able to use his/her individual private keys to generate query for certain file and the privileges he/she owned with the help of private cloud, while the public cloud performs duplicate check directly and tells the user if there is any duplicate.

List of modules:

- Endorsement(Login, Registration)
- Create data with random number
- Checks duplication
- Approve data
- View data

Endorsement (Login, Registration):

In this authentication system the login process will provides the security to the system. It doesn't accept any other login which contains unauthenticated ids. This module involves the registration process to create login id to everyone who all are using this system. It creates id and it should be a login id to use the service.

Create data with random number:

This module involves the data creation of particular user. It also requires post name, keyword, category, notes, and image file to creation data. It also save the data with the security of random key generation. It provides more security to the user data.

Checks duplication:

In this process the server checks the duplication occurred in that data. Because the database bandwidth needs to protect. So it checks the data replication.

Approve data:

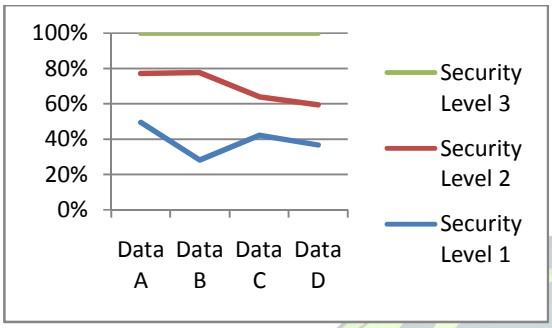
The reloading will be done by someone else then the past uploaded details are sent to the user. If they need to view that then the data owner should approve the user. In this module the server approves the data.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

View data:

Here the user can view the registered data with this module. It will provide the whole details of the system uploaded files.



CONCLUSION AND FUTURE WORK

Today, cloud computing is the technology being talked across industries due to its efficiency, the flexibility of resources, pay-per-use model, dynamic scalability, faster time-to-market, increased collaboration and cost efficiency. Despite its advantages, many organizations are still not adopting it because of security reasons associated with it. This paper analyzes the problem of security associated with cloud. Encryption is the foremost option for securing the data and this paper highlights comparative analysis of symmetric as well as asymmetric encryption algorithms for providing security in cloud computing systems.

REFERENCES

[1] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari. 'A secure cloud computing model based on data classification.' Elsevier, pp 1153-1158, 2015.

[2] N. Sengupta and R. Chinnasamy. 'Contriving hybrid DESCAST algorithm for cloud security.' Elsevier, pp47-56, 2015.

[3] S.K. Sood. 'Hybrid data security model for cloud.'International Journal of Cloud Applications and Computing, pp 50-59, 2013.

[4] J.J. Hwang, Taoyuan, Taiwan, Y.C. Hsu and C.H. Wu. 'A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service.'International Conference on Information Science and Applications (ICISA), pp 1-7, 2011.

[5] Christo Ananth, Shivamurugan. C.,Ramasubbu. S, "Enhancement of TCP Throughput using enhanced TCP Reno Scheme", International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Volume II, Special Issue XXV, April 2015.

[6] F. Moghaddam F, Karimi O and Alrashdan M T. 'A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments.' Proceedings IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, pp 185-189, 2013.

[7] W. Liu. 'Research on cloud computing security problem and strategy.' IEEE, pp 1216-1219, 2012.

[8] A. Behl and K. Behl. 'An analysis of cloud computing security issues.' IEEE World Congress on Information and Communication Technologies, pp 109-114, 2012.

[9] Ryan K L Ko et al.. 'Trustcloud: a framework for accountability and trust in cloud computing.' IEEE World Congress on Services, pp 584-588, 2011.

Mr.S.Nagasundaram, Assistant Professor/MCA from Sakthi Mariamman Engineering College and Research Scholar of Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, Kanchipuram, He has 13 Years experience in Engineering college, He has published 6 International Journal papers.

Dr. S.K. SRIVATSA received the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, Calcutta, India. Master's degree in Electrical Communication Engineering and Ph.D from the Indian Institute of Science, Bangalore, India. He was a Professor of Electronics Engineering in Anna University, Chennai, India, and he has 39.5 years of Post Doctoral teaching experience. He was a Research Associate at Indian Institute of Science. He has taught twenty eight different courses at undergraduate and forty two courses at the post graduate level. His current research activities pertain to computer networks, Design and Analysis of algorithms, coding Theory and Artificial Intelligence & Robotics. He has produced seventy Ph.D's and is the author of over 750 publications.