International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 12(B); December 2018; Page No. 16473-16475
DOI: http://dx.doi.org/10.24327/ijcar.2018.16475.3047

Research Article

INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS

Sai Manoj K[1]., Mrudula K[2]., Maanasa G[3] and Phani Srinivas K[4]

[1]CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
[2]Director, Innogeecks technologies, Vijayawada, AP, India
[3]Acharya Nagarjuna University, Guntur Dist, AP, India
[4]Director R&D Amrita Sai Institute of Science and Technology and Innogeecks Technologies, Vijayawada, AP, India

A R T I C L E I N F O

Article History:
Received 12th September, 2018
Received in revised form 23rd October, 2018
Accepted 7th November, 2018
Published online 28th December, 2018

Key words:
Security, Biometrics, Cloud Computing. Encryption algorithms

A B S T R A C T

With the rapid increase in the usage of cloud computing, it is very important to address the security issues also. Many Developers are designing so many techniques. Still there are some problems related to authentication in cloud environment. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. This research paper Point out clearly on such problems and their solution with the use of Biometric techniques.

INTRODUCTION

In the traditional model of computing, both data and software are fully contained on the user's computer; in cloud computing, the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser, display terminal for processes occurring on a network).Cloud computing is based on five attributes: multi-tenancy(shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources, it makes new advances in processors, Virtualization technology, disk storage, broadband Internet connection, and fast, inexpensive servers have combined to make the cloud a more compelling solution.

The main attributes of cloud computing are illustrated as follows:

1. ***Multi-tenancy (shared resources):*** Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.
2. ***Massive scalability:*** Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
3. ***Elasticity:*** Users can rapidly increase and decrease their computing resources as needed.
4. ***Pay as you used:*** Users to pay for only the resources they actually use and for only the time they require them.
5. ***Self-provisioning of resources:*** Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

Corresponding author:* **Sai Manoj K
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India

Main Concepts

New cloud computing challenging security threats for number of reasons

1. Traditional cryptographic primitives for the purpose of data security protection cannot 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.
2. 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.

System Model for Cloud Data Storage

There are three different network entities in the model:

1. ***Users:*** Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

2. ***Cloud Service Provider (CSP):*** A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
3. ***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.

Data Security Problem in Cloud Computing

A security threat faced by cloud data storage can come from two different sources.

1. A CSP can be self-interested; untrusted and possibly malicious and it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.
2. There may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period.

There are two types of adversary with different level of capability:

- ***Weak Adversary:*** The adversary is interested in corrupting the user's data files stored on individual servers.
- ***Strong Adversary:*** This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent.

Design Goals

There are certain goals for ensuring the security and dependability for cloud data storage under the aforementioned adversary model. They are:

- ***Storage Correctness:*** To ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.
- ***Fast localization of data error:*** To effectively locate the malfunctioning server when data corruption has been detected.
- ***Dynamic data support:*** To maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
- ***Dependability:*** To enhance data availability against Byzantine failures, malicious data modification and server colluding attacks.

Algorithm of Correctness Verification and Error Localization

Simple Error correcting and error detecting codes

In an error correcting code, a message M is encoded as a sequence of symbols a1, a2……an, called a codeword. The set of possible symbols is fixed in advance; for instance each symbol might be a byte (8 bits) of binary data. The code incorporates some redundancy, so that if some of the symbols in a codeword are changed, we can still figure out what the original message must have been. Usually, the number of symbols in the codeword, n, is also fixed, so each message carries a fixed amount of data. To encode larger amounts of data, one would break it up into a number of messages and encode each one separately.

Algebraic Code (Reed-Solomon code)

Encoding using Reed-Solomon Code

Let p be a prime number and let m <= n <= p. The Reed-Solomon code over the field Zp with m message symbols and n code symbols is defined as follows. Given a message vector[x1x2 . . . xm], let P(t) be the polynomial

$$P(t) = x_m t^{m-1} + x_{m-1} t^{m-2} + \ldots\ldots\ldots x_2 t + x_1$$

with coefficients given by the message symbols. Thus P (t) is a polynomial of degree at most m-1 in one variable t, with coefficients in Zp . Then the code vector a for this message vector is the list of the first n values of the polynomial P (t):

= [a1a2. . .an] = [P(0) P(1) . . . P(n-1)]
(Evaluated using modular arithmetic in Zp).

The Reed -Solomon code over Zp with m message symbols and n code symbols is the linear code with matrix

$$C = \begin{matrix} 1 & 1 & 1 & \ldots\ldots\ldots & 1 \\ 0 & 1 & 2 & \ldots\ldots\ldots & (n-1) \\ 0^2 & 1^2 & 2^2 & \ldots\ldots\ldots & (n-1)^2 \\ \vdots & \vdots & \vdots & \ldots\ldots\ldots & \vdots \\ 0^{m-1} & 1^{m-1} & 2^{m-1} & \ldots\ldots\ldots & (n-1)^{m-1} \end{matrix}$$

all entries taken (mod p).
Now encoding can be done as
a = xC (1)

where, a = encode matrix , x = original message matrix, and C = Reed-Solomon code matrix.

Decoding Reed-Solomon Codes

The discussion in this section will always refer to the Reed-Solomon code over Zp with

m = number of message symbols;
n = number of code symbols
n= m + 2e;
e = number of errors the code can correct.

Ensuring Security in Cloud Data Storage

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 theory that is 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.

Biometrics

Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities.

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below:

Identification: One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification: One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

Use of Biometrics

In this work biometric is used to extract the features from a finger print and use it to generate the key for pseudorandom function and pseudorandom permutation which are going to be used for implementing the model to enhance data security in cloud computing.

CONCLUSION

To ensure the correctness of users' data in cloud data storage we rely on erasure -correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s).

Acknowledgements

This paper heartily dedicated to beloved Honble Secretary and Correspondent Sri. K.Ram Mohan Garu, & Smt.K.Bhavani Devi Garu Amrita Sai Institute of science and technology. Also to all the respected Amrita Sai Management members. Our special thanks to the Innogeecks technologies, Vijayawada for their technical support in all the aspects.

References

1. Cong Wang, Qian Wang, and KuiRenand Wenjing Lou "*Ensuring Data Security in Cloud Computing*" Illinois Institute of Technology.
2. Cong Wang, Qian Wang, KuiRen, Ning Cao, and Wenjing Lou *"Towards Secure and Dependable Storage Service in Cloud" IEEE Journal*.
3. A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli, *International Journal of Computer Science and Mobile Computing* - Vol.6 Issue.11, November- 2017, pg. 7-11
4. Cloud Security Risk Factors and Security Issues in current trends research paper by Dr.K.Sai Manoj accepted and Presented in Scopus Based 2nd International Conference on Materials, Applied physics and Engineering (ICMAE 2018) at Indore. Proceedings of the 2018 First international conference on Materials, Applied physics and Engineering. After Clear scientific check this Paper was already Promoted to Science Publication Corporation.
5. Literature survey on the destruction of attaches with MH HOP to HOP to HOP-AODV Routing Protocol in Vehicular Ad-hoc Network, Dr.K. Sai Manoj, Mrudula Kudaravalli, © December 2017 | IJIRT | Volume 4 Issue 7 | ISSN: 2349-6002
6. Conceptual oriented study on the cloud computing architecture for the full-security Dr.K.Sai Manoj 1 *, Ms.K.Mrudula 2, G.Maanasa 3, K.Phani Srinivas 4 *International Journal of Engineering & Technology*, 7 (4) (2018) 2491-2493.Science Publication Corporation.

How to cite this article:

Sai Manoj K *et al* (2018) 'Investigation on The Data Security In Cloud Computing Using Biometrics', *International Journal of Current Advanced Research,* 07(12), pp. 16473-16475. DOI: http://dx.doi.org/10.24327/ijcar.2018. 16475.3047

****