IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Implementation of HASH Algorithm in Cloud Watermarking Techniques

I.Sudha[1], N.Vijayalashmy[2], G.Rupavani[3]

[1]Assistant Professor, Department of Computer Science and Engineering, Achariya College of Engineering Technology, Puducherry

[2, 3]Student, Department of Computer Science and Engineering, Achariya College of Engineering Technology, Puducherry

Abstract

Cloud computing provides various kinds of favorable services to the different users. Besides the several benefits of cloud computing, there are lots of issues to the users. One of the most challenging issue in the cloud computing is the security between the provider and the users. Cloud Computing face the tremendous challenges to ensure the proper physical, logical and personnel security controls, especially while moving huge volumes of data and software to the large data centers. The data owners can trust the service providers by establishing cloud security. So we provide a data coloring technique using cloud watermarking that can make the system robust as well as secure user's data. The intruders can misusing the data so by using cloud watermarking techniques strengthen the authentication mechanism for accessing the data in the cloud service provider. To enhance the data's security, we propose a method of providing security by using HASH algorithm for the periodic authentication to ensure whether the legitimate users are accessing the data.

Keywords-*Cloud computing, cloud security, data coloring, cloud watermarking, HASH algorithm.*

1. Introduction

Cloud computing is an internet based computing where the servers can provide services such as software, infrastructure, platform, devices and other resources to the user. In the cloud computing model, users can access the services which available on the "internet cloud". Today cloud computing is very familiar to the user because they processing in the data centric facilities. It provide computation software data access and storage services that do not require end-user knowledge.

The cloud computing services are:

1. **Software as a Service (SaaS) –** provide the software to the user over a network.
2. **Platform as a Service (PaaS)** – It is the set of tools and services designed to make coding.
3. **Infrastructure as a Service (IaaS)** - providing the processing, storage and network capacity.

In addition, the platform provides on demand services that are always on, anywhere, anytime and anyplace.

Pay for use and as needed, elastic scale up and down in capacity and functionalities. The hardware and software services are available to general public, enterprises, corporations and businesses markets. Simply put, cloud computing provides a variety of computing resources , from servers and storage to enterprise applications such as email, security, backup/DR, voice, all delivered over the Internet. The Cloud delivers a hosting environment that is immediate, flexible, scalable, secure, and available – while saving corporations money, time and resources.

Fig 1: Cloud computing services

2. Security Issues In Cloud Computing

Time, cost, innovation leads to the success of cloud computing but still there are certain security concerns that need to be addressed while moving critical applications and sensitive data to public and shared cloud environments. Major security issues faced by

cloud providers and by their customers are discussed below:

1. *Location of Data*: Various organizations located in different places have different needs and controls placed on access. Because the data is in the cloud, one may not realize that the data must reside in a physical location. The cloud provider should provide the level of security required for different customers and their needs.

2. *Access to data*: Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone using the cloud need to look at who is managing their data and what types of controls are applied to these individuals.

3. *Data classification:* Is the data classified? How is your data separated from other users? What is the type of Encryption mechanism?

4. *Service level agreement (SLA) terms:* Organizations need to ensure the security and integrity of their data, even when it is held by service providing the cloud. They also need to prove conformity with security standards regardless of the locations of their data and applications. This could be achieved by Service Level Agreements (SLA), Loss of service, Audit, and service conformity

5. *Security breach:* If a security incident occurs, what support received from the cloud provider?

6. *Privileged access*: This is the question about who has the privilege to access the data. Who is responsible for hiring & management of the administrators, which handles the information?

7. *Authentication and authorization:* Every organization has its own way to manage authentication and authorization.

Every organization must determine if its current authentication system could also work in a secure and reliable way for users in a cloud environment. Apart from that what is the best way to authenticate cloud services but also be insured.

Security concerns based on delivery and deployment models are data integrity, data locality, data confidentiality, and data access. Some more security related concerns are Sign on process, Authentication & authorization, network security, identity management and especially multi-factor authentication which considers multiple factors together for authenticating a user.

A. CIA triad

A security framework for an information system has three goals namely confidentiality, integrity and availability.

B. AAA

The security framework for an information system should provide authentication and authorization capabilities.

C. Defense-in-Depth

It is a risk management strategy which provides multiple layers of defense against attacks.

D. Multi-factor authentication

- **First factor:** What does a user know? For example, a password for a log in session will be what a user is required to know.
- **Second factor:** What does a user has? For example, a user needs to provide a secret key, generated by a physical device (token), which is under the user's possession.
- **Third factor:** Who is the user? For example, a biometric signature of a user can be considered as an example of who is a user id.

Some of the security issues can occur when passing the organization's data into cloud platform. They are:

1. Privileged access
2. Separation of the data from its actual location.
3. Data availability
4. Regulatory compliance
5. Long term viability

Threats in cloud computing

Some of the security management environment and possible threats are:

1. Virtualization security management
2. Trusted cloud computing
3. Trusted computing base
4. Trusted platform module

Security could prove to be a big issue: It is still unclear how safe out-sourced data is and when using these services ownership of data is not always clear.

3. Watermarking Techniques

Cloud model: It is a transform of quantitative and qualitative data.

Suppose U is a universal set of numbers, C is a qualitative concept related to the universal set U. Any variable x that belongs to universal set U i.e. x ϵ U randomly realized the concept C with the certainty degree of x for C.
A random value lies between 0 and 1.

$$\mu: U \rightarrow [0, 1], \text{for all } x \in U \quad x \rightarrow \mu(x)$$

The distribution of x on U is defined as a cloud and every x is defined as a cloud drop. In this model, the property of cloud drops is represented by

Ex – expected value
En - entropy
He - hyper entropy

Where the expected value is a mathematical representation of cloud drop. We can also say that a cloud drop is located at some point Ex is most recognizable value of qualitative concept. En connects the concepts of both randomness and fuzziness by granularly measuring the qualitative concept.

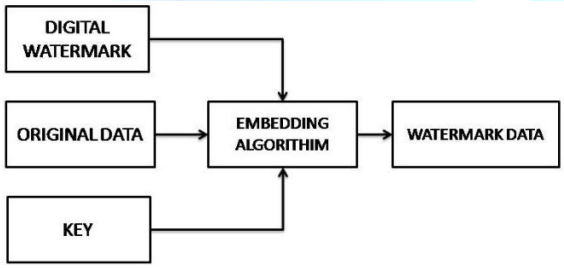


Fig .2: Cloud model

4. Base Methodology

The cloud watermarking is not only embeds the user's copyright information but it also colors all of its data. Each of the users is specified by a color that helps to protect the copyright and also avoids the manipulation of original data.
The cloud drops are added into the input photo (left) and remove color to restore the original photo (right).
The process uses three data characteristics to generate the color. The expected value (Ex) depends on the data content known only to the data owner. Whereas entropy (En) and hyper entropy (He) add randomness or uncertainty, which are independent of the data content and these three functions generate a collection of cloud drops to form a unique color that the providers or other cloud users can't detect. This technique can also be applied to protect documents, images, videos, software, and relational databases in the cloud. The color-matching process assures that the colors applied for user identification match the data colors. This process initiates authentication and authorization.

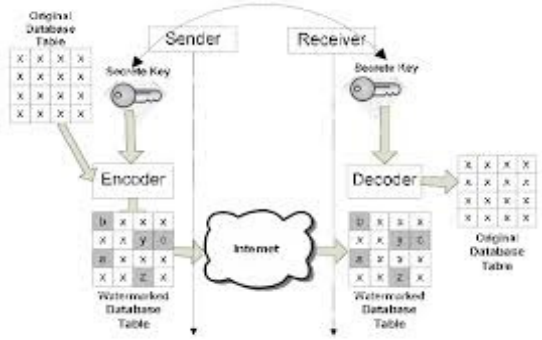


Fig .3 Encrypting the data using cloud watermarking

5. Related Works

Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. The best possible solution to deal with Security issues is Data Encryption. Various algorithms exist to encrypt the data in Cloud Computing such as DES, 3DES, blowfish, AES, RSA, etc. Cloud storage concern the user does not have control over data until the user has been gaining access. To provide control over data in the cloud data-centric security is needed. Before accessing the data it should satisfy the policy rules already defined. So cloud should enforce this scheme by using cryptographic approaches.

Each Cloud user is provided with a value called expected value which is known only to the user and the negotiated values with the CSPs are Entropy which is unique for all users in the particular group sharing the data in the cloud and Hyper-entropy is the value which is common to all the group users of the data. To provide the continuous authentication within the group, an automated validation using the tiny bit of data can be made at regular intervals of time. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public-key cryptography, involves a

public key and a private key. The public key can be known to everyone and is used for encrypting messages.

With the development of Internet and databases application techniques, the demand that lots of databases in the Internet are permitted to remote query and access for authorized users becomes common, and the problem that how to protect the copyright of relational databases arises. This paper simply introduces the knowledge of cloud model firstly, includes cloud generators and similar cloud. And then combined with the property of the cloud, a method of protecting relational databases copyright with cloud watermark is proposed according to the idea of digital watermark and the property of relational databases. Meanwhile, the corresponding watermark algorithms such as cloud watermark embedding algorithm and detection algorithm are proposed. Then, some experiments are run and the results are analyzed to validate the correctness and feasibility of the watermark scheme. In the end, the foreground of watermarking relational database and its research direction are prospected.

6. Hashing Algorithm

Based on the hash value the key value is generated the key in public-key encryption. Using hash algorithm the hash value is computed from a base input number. The hash value is an original value and it is impossible to derive the original input number without knowing the data.

Example:

Input Number
10,667
Hashing Algorithm
Input# x 143
Hash Value
1,525,381

A cryptographic hash function takes an arbitrary block of data and returns a fixed-size bit string. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest. Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The data record is also accessed by using the hashing method.

The cryptographic hash functions take a string of any length as input and produce a fixed-length hash value.

A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. It is easy to compute the hash value for any given message.

Applications

1. Verifying the integrity of files or messages
2. Password verification
3. File or data identifier
4. Pseudorandom generation and key derivation.

There is a long list of cryptographic hash functions, although many have been found to be vulnerable and should not be used. Even if a hash function has never been broken, a successful attack against a weakened variant thereof may undermine the experts' confidence and lead to its abandonment.

Properties of hash function

- Cryptographic hash functions have many security applications in digital signatures, message authentication codes (MACs), and other forms of authentication.
- They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption.
- It is infeasible to generate a message that has a given hash.
- It is infeasible to modify a message without changing the hash. It is infeasible to find two different messages with the same hash.

1. **Pre-image resistance -**

Given a hash h it should be difficult to find any message m such that h = hash(m). This concept is related to that of one-way function. Functions that lack this property are vulnerable to preimage attacks.

2. **Second pre-image resistance**

Given an input m_1 it should be difficult to find another input m_2 such that $m_1 \neq m_2$ and $hash(m_1) = hash(m_2)$. Functions that lack this property are vulnerable to second-preimage attacks.

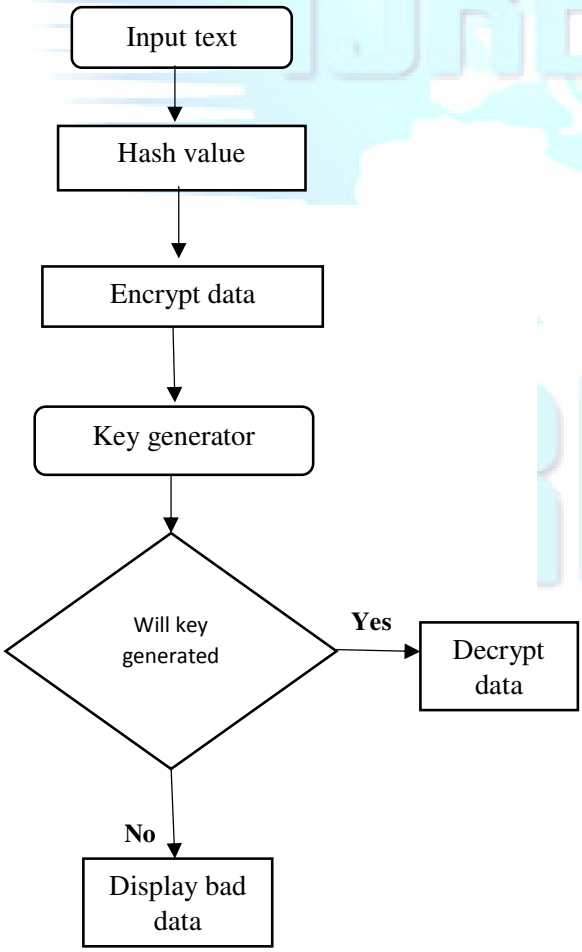
3. **Collision resistance**

It should be difficult to find two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It

requires a hash value at least twice as long as that required for preimage-resistance.

Cloud computing is revolutionizing the way business is carried out in various industries (Government, Healthcare, Software etc.), use of information technology resources and services, but the revolution always comes with new problems. One of the major problems associated with Cloud computing is Security. The proposed system has many advantages over the existing system. The proposed system has the most secure authentication mechanism in accessing the data because, a periodic authentication is made to ensure whether the legitimate users are accessing the data in the cloud. In the existing system using RSA algorithm, the key is generated to ensure whether the legitimate users are accessing the data in the cloud and continuous monitoring will be taken by providing periodic authentication.

Flow diagram



Steps in Hashing algorithm:

1. Producing hash values for accessing data or for security.
2. A hash value is a number generated from a string of text.
3. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.
4. The sender generates a hash of the message, encrypts it, and sends it with the message itself.
5. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes.
6. If they're the same, there is a very high probability that the message was transmitted intact.

7. Conclusion

One of the major problem in cloud computing is security. The user can store the data in the databases provided by the cloud service provider. The digital watermarking techniques that is helpful for cloud security. The proposed system has the most secure authentication mechanism in accessing the data because, a periodic authentication is made to ensure whether the legitimate users are accessing the data in the cloud by using HASH algorithm. This paper also discusses the advantages, features and properties of the hash algorithm. In the future, security algorithm will be implemented producing results to provide periodic authentication for cloud users.

References

[1] International Journal of Advanced Research in Computer Science and Software Engineering, Research Paper, “Data Colouring by cloud Watermarking using RSA for Periodic Authentication”.
[2] Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li, Gui-Sheng “A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking” ,IJAC Aug 2011.
[3] Kai Hwang “Trusted Cloud Computing with Secure Resources and Data Coloring” Volume: 14, Issue: 5, IEEE Sept 2010.
[4] William Stallings, —Cryptography and Network Security Principles and Practices, Prentice Hall, New Delhi.

[5] zhiguo du, dahui hu, "image watermarking technology based on cloud model", asia pacific youth conference on communication technology, pp.25.27,2010.
[6] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).
[7] Russell dean vines, "cloud computing software security fundamentals", Indianapolis, Indiana, 2010, ch.3, sec.1, pp.90