ISSN:0975-9646

Cloud Data Integrity using Password Based Digital Signatures

Ceena Mathews
Dept. of Computer Science
Prajyoti Niketan College
Pudukad, Thrissur, Kerala, India

***Abstract*— As more and more information of individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. This paper deals with a security mechanism which ensures the integrity of the data stored in the cloud. In this paper, a password based digital signature technique has been proposed. This combination mechanism provides three way security i.e. data security, authentication and verification. In this paper, I have proposed RSA encryption algorithm for confidentiality of data and for authentication hash algorithm can be implemented and PBKDF2 key derivation function for generating the key for encryption.**

***Keywords*— Security threats, RSA, PBKDF2, Digital Signature.**

I. INTRODUCTION

Cloud Computing is a type of internet based computing where different services such as servers, storage and applications are delivered to an organization's computer and devices through internet. Cloud services, sometimes called "software as a service" (SaaS), "infrastructure as a service" (IaaS), or "platform as a service" (PaaS), facilitate rapid deployment of applications and infrastructure without the cost and complexity of purchasing, managing, and maintaining the underlying hardware and software.

Organizations and institutions are increasingly driven to cloud computing as a way to increase functionality, lower cost, and enhance convenience to users by making the services and resources available anywhere there is an internet connection. With cloud computing, users have readily available a suite of applications, features, and infrastructure that would normally require significant investment if provided in the traditional in-house computing environment.

While cloud computing services have numerous potential benefits, there are also potentially significant privacy and security considerations that should be accounted for before collecting, processing, sharing, or storing organizational or personal data in the cloud.

II. SECURITY ISSUES

Security controls in Cloud Computing are no different than security controls in IT environment. However because of the cloud service models employed, operational models and technologies used to enable cloud services, cloud computing presents different risks to an organization than traditional IT solutions. The main problems cloud computing faces are securing confidentiality and integrity of data in terms of data security. The CSA (Cloud Security Alliance) has identified the top nine cloud computing threats for 2013[2].

A.Data Breaches

One of the security threat which is identified as a top threat in a survey conducted by the CSA is data breaches. The concept of data breach is that any malicious person or unauthorized person enters into a corporate network and steal the sensitive or confidential data.

B. Data Loss

Another serious threat that threatens the CSP is the potential incapacity to prevent data loss because many of the companies treat their data as a valuable asset. In our networked world, most people know that loss of data is unavoidable at one point or another. There is increasing amount of sensitive data which is relayed to cloud computing providers and this data could get lost in any number of ways, including through accidental deletion or corruption of stored data.

C.Account Hijacking

In Account Hijacking a malicious intruder can use the stolen credentials to hijack cloud computing services and they can enter on other's transactions, insert false information, and divert users to abusive web sites which resulted in legal issues for cloud service providers.

D.Insecure application programming interfaces (APIs)

If the Application Programming Interfaces which are used by the users to communicate with the cloud services are weak or not sufficiently secured, accidental or malicious attempt to violate them may expose the loud data to many security threats related to inflexible access control, scalability and limited monitoring and many other issues.

E.Denial of Service

DoS have become very serious threat when the organizations are dependent on the services for 24/7. It temporarily denies the access of data stored in the cloud to the authorized users by make an attack on the server by sending thousands of requests to it become unable to respond to the regular clients.

F. Malicious insiders

A person who enters into the cloud network to harm the organizations confidential data and assets, damage valuable brands, penalize financial damage, stop productivity is known as a malicious insider.

G. Abuse and Nefarious Use

Network hackers are always developing new technologies to extend their reach by propagating malwares or share the pirated software, escape from being detected, and improve the effectiveness of their activities. Some cloud computing providers who are weak in their security measures such as detecting the intruders are the target of the attackers.

H. Insufficient Due Diligence

CSA's basic advice is for organizations to make sure that they have sufficient resources and to perform extensive due diligence before jumping into the cloud.Due diligence refers to the care a reasonable person should take before entering into an agreement or a transaction with another party.

I. Shared Technology Issues

Cloud computing is known for its sharing technology so it is very difficult to obtain a strong isolation property for multi-tenant architecture. It is the responsibility of the CSP to provide a scalable service to the user without interfering with the other client system.

III. PROPOSED SYSTEM

Data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well. In order to avoid the above security issue, Password based Digital signatures can be used.

A.Creating a digital signature with a private key derived using PBKDF2

Data encryption using asymmetric keys is an expensive operation directly proportional to the size of the data being encrypted; it potentially doubles the size of the data increasing the processing power and bandwidth required to process and transfer the data.

A more efficient approach is to first use a secure cryptographic hash function which can take large objects of varying size and produce a unique fixed-size hash value or message digest. The much smaller hash value can then be encrypted with the private key of the originator to produce the digital signature. The private key for encryption is derived using PBKDF2 which applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. Having calculated the message digest this can be encrypted using the private key of the originator to produce the digital signature, as shown in the figure 1:

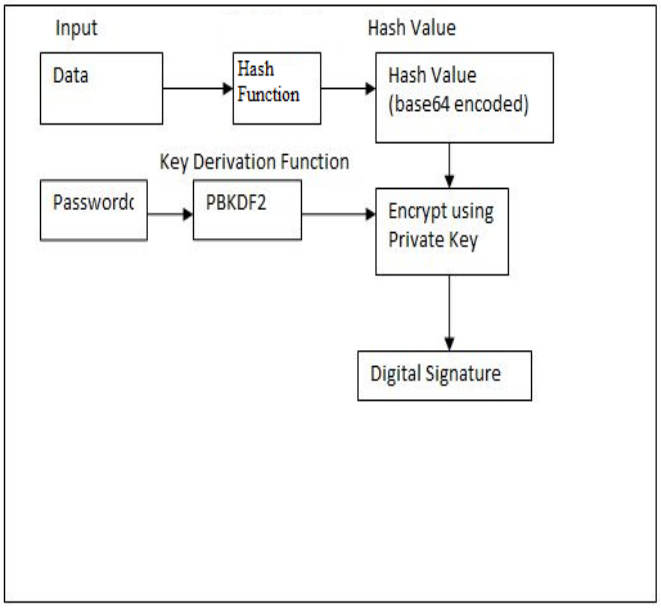

Figure 1. Creating a digital signature with a private key

B.Verifying a digital signature created with a private key

The recipient must de-crypt the digital signature using the public key of the originator and recalculate the hash value of the corresponding digital object. If the calculated hash value does not match the result of the decrypted signature, either the object has been altered since being signed, or the signature was not generated with the corresponding private key of the originator.

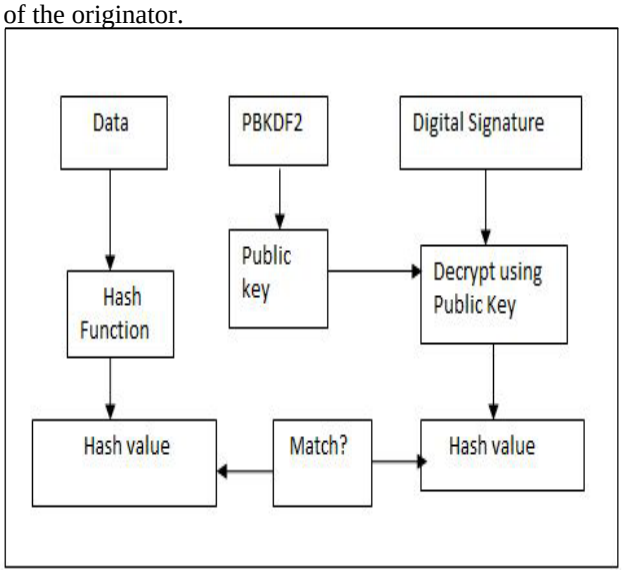

Figure 2. Verifying a digital signature

IV. CONCLUSION

This paper presented a set of security protocols to secure the data files of a data owner in the cloud infrastructure. The public key, hash, and private key ciphers that are proposed between cloud service provider, data owner, and user ensure an isolated and secure execution environment at the cloud. PBKDF requires that the number of iterations to derive a key increases the computational cost of performing a dictionary attack on a password. The computation required for key derivation by legitimate users also

increases with the number of iterations. The user may perceive this increase, for example, in the time required for authentication, or in the time to access the protected data on the storage medium. There is an obvious tradeoff: larger iteration counts make attacks more costly, but hurt performance for the authorized user. The number of iterations should be set as high as can be tolerated for the environment, while maintaining acceptable performance.

REFERENCES

[1] Meiko Jensen JorgSchwenk, Nils Gruschka,Luigi Lo Icono, "On Technical Security Issues in Cloud Computing", 2009 IEEE conference on Cloud Computing.
[2] http://www.cloudsecurityalliance.org/Top Threats Working Group the Notorious Nine Cloud Computing Top Threats in 2013.
[3] http://technet.microsoft.com/en-us/library/cc962021.aspx
[4] http://www.paradigm.ac.uk/workbook/metadata/authenticity-signatures.html
[5] http://www.scribd.com/doc/229709036/Enhancing-Data-Security-in-Cloud-Computing-Using-RSA-Encryption-and-MD5-Algorithm
[6] http://en.wikipedia.org/wiki/PBKDF2
[7] http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf