Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.357 – 360

RESEARCH ARTICLE

Data Security Issues in Distributed Cloud System

P. Raja Kaushik[1], G. Praveen Babu[2]

[1]Master Student in CNIS Stream from SIT, JNTUH, India

[2]Associate Professor of CSE Department in SIT, JNTUH, India

rajakaushik23@yahoo.com [1] pravbob@jntuh.ac.in [2]

Abstract— Latest technology for better computation and security of data is cloud computing. The key feature of this technology is proving computing services through internet as pay per use to share storage, services, applications, networks without physical acquiring them. So that time taken to organize resources and managing cost reduces a lot. As the cloud is providing pay-per-use pattern on transactions carried, bandwidth used, data transfer, processing power consumed, storage space used many industries like health, libraries, government sector, banking, education etc are moving towards cloud computing. Different cloud providers like Google, Amazon, Microsoft, Salesforce.SOM etc are in the market for providing cloud computing services. There are different cloud deployment models available in market like community cloud, public cloud, private cloud, hybrid cloud. Service providers integrate building and supporting data centre hosts and offer different services like SaaS, PaaS, IaaS etc to the consumers, re-sellers .Cloud computer entirely depend on internet through which client can save his data in data sources and use them any time he need. Due to this security for the data which is stored by the user must be maintained. Reliability, interoperability, privacy, access level agreement must be ensured. This research paper includes basic understanding of cloud system, advantages of cloud system, security issues in cloud environment. Different concepts of security like firewalls, encryption, encoding, access policy etc are discussed in this paper.

Keywords— Proxy Re-Encryption, Encoding, Distributed system, Access permissions

I. INTRODUCTION

Cloud computing plays a vital role in this modern days because of its compelling benefits, security and services. Cloud Storage system have Storage as Service which is the best service it can provide. Bunch of cloud servers for provide continuous access is actually main idea of cloud computing. Tremendous aspect in technology of world is formed with data storage. In previous days data is replicated and stored in storage devices so that user can access it at anytime and anywhere which takes so much storage and when if the storage places increases then it also increases insecurity. Mining of data could be a serious threat to security in Cloud considering that entire data of particular user is stored at single cloud. This single cloud provider technique gives the attacker an opportunity to use efficient data mining algorithms that can extract information about the user. Then distributed storage came into existence. One of the storage grid Tahoe is designed to provide secure, long term storage, such as for backup applications. In Tahoe distributed systems hardware failures can be eliminated. New secure file system Plutus maintains key distribution in decentralized manner so that data is stored in encrypted format.

© 2014, IJCSMC All Rights Reserved

Different Cryptographic schemes are maintained by the users rather than the servers. Disadvantages of this system is that replication which leads to over storage, complete key distribution is complex, cryptographic key operations maintained by user is insecure . But giving complete keys to user system may not be a secure and complex as well.

This leads to a new distributed storage system which is secured by splitting the data into blocks and encryption on each slice of data is done in storage servers and then apply re-encryption on each cipher slice of data. Erasure code is used for encoding and AES, RSA algorithms are used for encryption.

II. DISTRIBUTED APPROACH

Distributed approach is the solution for the problem with distributed single cloud systems. As all cloud providers store data on pay-per usage and give infinite computation speed and functionality we store that data in different cloud servers rather than storing in single cloud storage service system. This distributed secure storage systematic approach overcomes the problem in single cloud provider and provide security to data by using following features.

1) ***Erasure coding – encoding***

2) Proxy re-encryption.

III.PROXY RE-ENCRYPTION SCHEME

Bob's secret key can be opened by transforming cipher text of alice's public key which is allowed by proxy re-encryption technique via proxy. We have brief information about it below. All traditional systems which are asymmetric or symmetric imply functionality for proxy re-encryption. Proxy re-encryption is different than other traditional methods in below two functionalities.

A. **Delegation:**

It provides a mechanism where a message recipient (key holder) is allowed to generate a re-encryption key depends on his secret key and the key of the delegated user. This delegation is used to create a re-encryption key.

B. **Transitivity:**

Infinite number of times a cipher text is re-encrypted which is done by transitive proxy re-encryption schemes. We need one symmetric algorithm and one asymmetric algorithm. Here you use AES algorithm for re-encryption and RSA algorithm for key generation and encryption purpose.

1. **RSA**:

It is a public key algorithm. It is invented by Rivest, Shamir and Adleman. Different key is used for encryption in RSA and the key used for decryption is different but they both are related to each other.

© 2014, IJCSMC All Rights Reserved

RSA key generation algorithm

1. Generate two large random and distinct primes A and Z
2. find N = A.Q and φ = (A – 1) (Z – 1)
3. Choose a random integer B, 1 < B < φ, such that gcd (B,φ) = 1
4. Compute the unique integer D, 1 < D < φ, such that BD ≡ 1 (mod φ)
5. Public key is (N, B) and private key is (N, D)

RSA encryption algorithm can be described as $\mathbf{C = M^{E} \bmod N}$, RSA decryption algorithm can be described as $\mathbf{M = C^{D} \bmod N}$, Where C represents cipher text and M represents message.

2. **AES:**

This algorithm is based on a design principle known as a substitution-permutation network, and is fast in both hardware and software.

High level description of algorithm:

1. Key expansion – from rijandael's key schedules derives round key from its ciphers.
2. first round –

a. Add round key – by using bitwise XOR combine each bit with round key.

3. Rounds –

a. Sub bytes – each byte is replaced with another using a look up table as a non linear substitution.
b. Shift rows – each row is shifted cyclically to a number of times called transposition.
c. Mix columns – combines four bytes in each column.
d. Add round key

4. last round –

a. Sub bytes
b. Shift rows
c. Add round key

IV. A SECURE DATA STORAGE AND FORWARDING

In this paper we put forward four steps to design secure data storage and data forwarding. The four steps are,

A. Storage system setup
B. Data storage mechanism
C. Data forwarding mechanism
D. Data retrieval mechanism

A. **System setup:**

Data storage in third party servers must be given high range of security so first we design storage servers for storing data and key servers for managing key functionalities. Then generate a pair of public key and private key. Now we use asymmetric algorithm I .e RSA then produce a key pair of length 1024 bits. Now split this secret key into number of parts in key distribution we keep a part of key locally and distribute remaining keys in storage servers randomly. The below screen shows the output of the stage.

B. **Data storage:**

In this step, a file or a message is chosen and divided into blocks then perform encryption on each block then distribute them randomly to storage servers , on each block encoding is performed and then stored in servers. All the encryption and encoding is performed in this stage itself.

C. **Data forward:**

First the user chooses a file which he sends it to another user then split the file in to number of parts then each and every slice of file is encrypted using a public key which is part of the recipient of the data. Here we split the data into 3 parts and encrypted by using the public key of the user. Now AES algorithm is used to generate re-encryption keys. Here we give part of secret key which belongs to sender and public key of recipient as inputs. AES algorithm produces 256 bits length re-encryption key which is used for re-encryption purpose. These 3 encrypted slices are re-encrypted using the re-encryption keys. These re-encrypted cipher blocks are then encoded and stored in storage servers.

D. **Data Retrieval:**

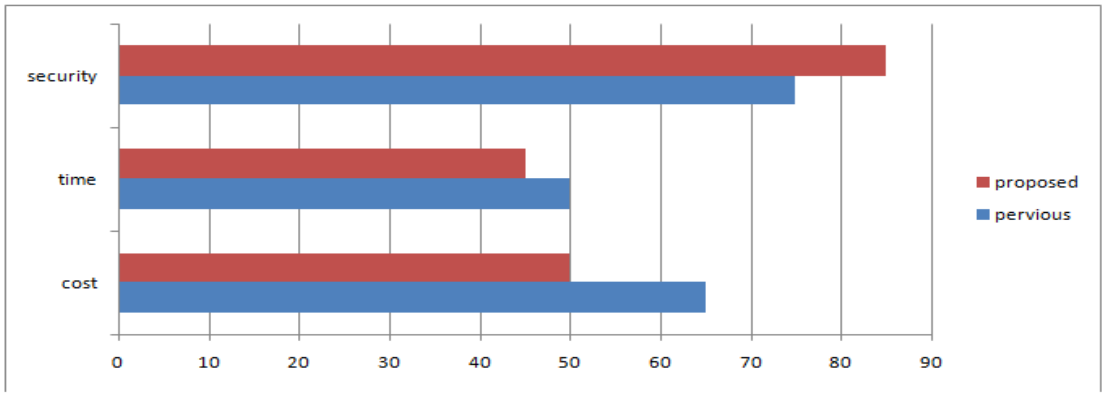
Data retrieval stage has two retrievals one for receiver and ne for sender. When sender wishes to send the data, the data which is encrypted is retrieved from data servers before decoding then sent to the sender there each

© 2014, IJCSMC All Rights Reserved

decoded encrypted parts are decrypted. Here we use the secret key of the sender which is requested from the key servers and then combined for the complete data. If user request for the data then key servers generate keys and attached with data in data servers and the regenerates the re-encryption keys. Then the receiver attaches the blocks to see the entire data.

V. EXPERIMENTAL RESULT

This experiment shows that our approach is exact and could be useful in secure data forwarding in distributed storage environment in cloud computing. The empirical results show that security, cost reduction, time consuming.



VI. CONCLUSION

In this paper we put forward the existing system for file forwarding in distributed systems and different problems related to security like dos attacks, network outages and then propose a new architecture in cloud storage system and file forwarding mechanism. Different symmetric and asymmetric algorithms like AES, RSA are explained where we use them n encryption and encoding of data so improve the security of data which is stored in third party storage systems. We sliced the data and stored in different storage servers randomly, encryption and encoding has been performed on these slices of data multiple times to achieve good security levels while maintaining robustness of the system. Access permissions are given so that receiver can get access to only the art of data which he wants , all the key functionality for this mechanism are maintained in different servers called key servers.

REFERENCES

[1] Ljiljana Brankovic,Vladimir Estivill-Castro, "Privacy Issues in Knowledge Discovery & Data Mining", Newsletter The University of Newcastle, vol 3.no2, 2008, pp.1-12.

[2] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least Authority File system," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008

[3] Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R.Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000.

[4] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE.**,"** A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE transactions on parallel and distributed systems, vol. 23, no. 6, pp.995-1003 ,june 2012.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006

[6] Ernesto Damiani, Francesco Pagano,Davide Pagano, "iPrivacy: A Distributed Approach to Privacy on the Cloud", International Journal on Advances in Security, vol 4 no 3 & 4, year 2011,pp.185-197.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29-42, 2003.

© 2014, IJCSMC All Rights Reserved