Engineering and Scientific International Journal (ESIJ)
Volume 4, Issue 3, July– September 2017
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Online Proffering Approach with Secure Manner using Scrambled Technique

A.Manjula[#1], R.Sankar[#2]
[1]*Masterof computer Application 2nd year, S. A. Engineering College, Chennai, India*
manjucool.218@gmail.com
[2]*Asst. Prof., Department of Computer Applications, S.A. Engineering College, Chennai, India*
sankar@saec.ac.in

Abstract— This paper proposes the secured cloud proffering with scrambled technique and uses the Hardware Security Module (temporary storage) to store automatic generating keys for encryption, decryption, and authentication which isolates the cloud user data from potentially malicious domains or cloud administrators. Within the secured environment, the hardware security module provides essential security functionality with automatically generated keys for data in storage. Such limitations avoid the cloud administrator from distressing the security of the Guest Users. This system not only defends against wide attacks but also for the small TCB. This paper discusses the software operation of the proposed Proffering approach with safety unit, analyzes the security and presents its performance results. This system provides three methods of cloud security. The connection is secured. There will be secured platform between the cloud user and the cloud admin.

Keywords— Scrambled Technique; Authentication; Cloud Admin; Cloud.

1. Introduction

The security alarms in the form of confidentiality of the user data by the domain and the administrator (admin) are to increase in the usage of cloud computing. To avoid the cloud administrator from disturbing the security of the guest users, the user can send the data to the cloud, it will be encrypted and the key will be assigned in the different place using the scrambling technique. In the scrambling technique, the data will be encrypted and it will generate the key in the separate place of the cloud [1]. The data stored in encrypt form protected with security key. The algorithm can be used in the paper is AES (Advanced Encryption Standard). The keys are automatically generated and stored separately in the cloud [2]. The key was only known part between the cloud user and administrator. The hash values for every data are to prevent the forgery and are verified by the device authority. This will increase more secure connection between the cloud user and the cloud administrator. The key will automatically generate for the authentication and it avoids the security breach in the cloud and also in the communication between the admin and user. Security is a primary consideration for cloud users [3]. Although security threats by cloud administrators are realistic and grave. Cloud service providers are mainly disturbed with security threats from external attacks rather than internal attacks. This viewpoint hinders the proliferation of cloud computing. By using the security key they verified the respective user of the cloud and the data stored in the cloud will be encrypted.

2. Existing System

In the existing system, using Input Output (I/O) model of hypervisor with management tool they performed the cloud storage allocation for the cloud administrators. In this module, the physical machines shared by multiple admin, so they can easily access the data of the other [4]. By I/O scheduler, they perform the bidding operations based on the storage space required by a cloud administrator. The digital signature is based on only the conventional system (i.e) using the DES (Data Encryption Standard) algorithm. While digital signature provides encryption function on more complexion function and it will more complex for users and easily attacked by malicious admin. In previous methods they used DES which uses 62 bit encrypt data self -service cloud computing. This method is efficient but the cloud user and cloud admin have equal authority to change the data. So it is insecure for the data and anybody can access the data which is stored in the database [5]. In the existing system, the key is generated the same place of an encrypted area, so the hacker can hack the data easily.

2.1. Disadvantages

While resource sharing improves hardware utilization and service reliability, this may also open doors to side channel or performance interference attacks by malicious admins. Using VMWare GSX Server and a Delian Linux host OS is not suitably high assured for a real TVMM [Trusted Virtual Machine Monitor]. By using a digital signature it may increase the difficulty of factoring and the high computational cost.

3. Proposed system

To prevent the data from the malicious admin we are providing keys from the secure isolated path for the cloud

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

administrators. The keys are automatically generated and stored separately in a cloud. The data are stored in an encrypted form protected with security key. In the proposed system we used AES-Advanced Encryption Standard which encrypts the data in a more efficient way. For each process there will be an attestation using security key to prevent the data from malicious admin. There will be hash values for every data to prevent the forgery and is verified by the device authority. This will increase the secure connection between cloud administrator and cloud provider. The key will be generated separately in the cloud using a scrambled technique. This technique can be used to create the data in a separate place and so no one can access the data. It is considered as very secure to use.

3.1. Advantages

- It will prevent the data from malicious admin.
- The data are securely stored in database in encrypted form.
- While bidding, admin details will be secured.
- In the proposed system, the AES algorithm is used and which is more efficient than the DES (Data Encryption Standard).
- This system will reduce the difficulty of factoring and computational cost.
- Admin cannot change the virtual machine status arbitrarily.

The AES Algorithm used to encrypt the data and send the data to the cloud. This algorithm can be implemented easily on simple processors. It has a strong mathematical foundation that uses substitution, transposition, and the shift, exclusive OR and the additional operations [6].

There are 10, 12 or 14 cycles for keys of 128,192 and 256 bits. It converts the data into bits. It will generate the secret key of sender and receiver. In figure 1,the key distribution is explained.

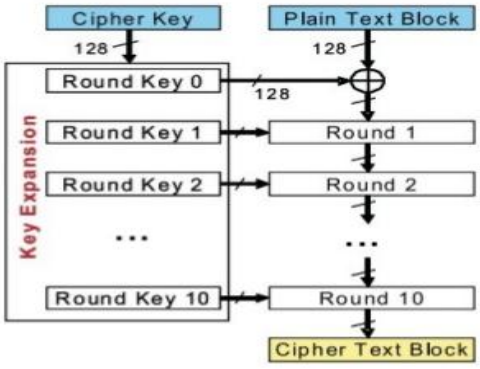

Fig.1: AES Architecture for key distribution

The key will be generated in the same place of encrypting the text, so the hacker can hack the data easily and therefore we can use the scrambled technique. In this technique, the key will be generated separately. In scrambled technique, it will send the data to the client in the encrypted format and the key value should be known only to the user and the admin. In the cloud storage, the key will be generated automatically and the key value will be sent to the user and the admin. [3]. It works in the cloud "Secret Key" and the Scrambled Technique is shown in the figure 2.

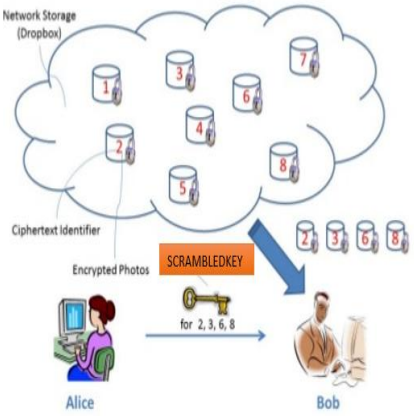

Fig. 2: Scrambled Technique

In figure 2 the client can send the file to the cloud, it will be encrypted and store in the cloud. The key will be generated in the cloud automatically. If the admin retrieve the file, it will send the file with that key value. The user can put that key value to decrypt the file easily. In this method the data will be in a secure manner and the time consumption is also less. The key length is high and so the hacker does not hack the data.

5. Result

In this paper, the key will be generated automatically in the cloud storage. It will secure the data from the hacker. Using scrambled technique, the key will be stored separately in the cloud. The data will be encrypted and decrypted using AES (Advanced Encryption standard). In this algorithm, the data will be encrypted and the key value would be stored in the cloud. It can be a cycle of round and encrypted the text [7].

Fig.3: key Encryption

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Figure 3 shows how the key is encrypting and decrypting the file. The encrypted key and decrypted key can join to produce encrypted decrypted key. In the decrypted key, the original file can be encrypted and it will be in decrypted after that the file will be stored in the cloud [8].

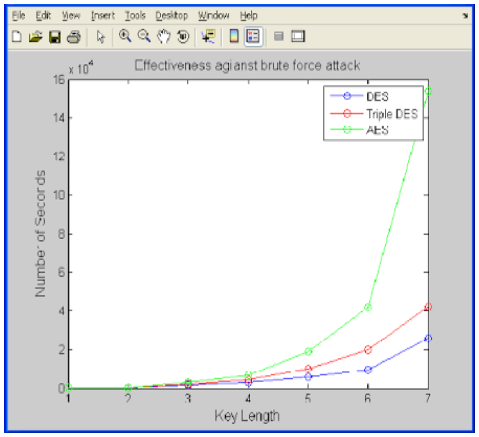

Fig.4: Comparison of AES & DES algorithm

In the existing research, they used DES (Digital Encryption Standard) algorithm. In this paper, we used the AES (Advanced Encryption Standard) algorithm. In figure 4, we compared three algorithms with the key length and number of seconds. Based on the key length and number of seconds, the AES is better than the DES and Triple DES algorithm. The speed also increased and they can transfer the data quickly. The data will be very secure in this algorithm and so the hacker cannot hack the data.

6. Conclusion

Nowadays the business people can store the data in cloud technology only. In this online proffering scheme, the bid is secured and encrypted. The key will automatically generate for the authentication and it avoids the security breach in the cloud and also in the communication between the admin and user. Security is a primary consideration for cloud users. Although security threats by cloud administrators are realistic and grave. The cloud service providers are mainly disturbed with security threats from external attacks rather than internal attacks. This viewpoint hinders the proliferation of cloud computing. By providing the security module, it supports special storage which is accessible to cloud administrators and secure critical data in the hardware isolated to prevent malicious admin. The proposed system provides a secure connection between the cloud administrator and cloud provider. The connection between an allocated VM is secured by exchanging the keys. The Key stored separately in the cloud using a scrambled key.

7. Future Work

In the proposed system, the automatically generated keys are stored in a particular storage and the other user can easily identify a particular document or application. But in the future work, the random keys are generated and the other users shouldn't identify a particular document or application. If the random key is generated, that can be stored in the separate place and so they cannot identify what key would be placed in a particular place. So no one can access the data easily. They protect the data in a secure manner and also it will be encrypted the text in the database. Random keys will be stored automatically if the user can login the account and it will be accessed at the time the key is created in the cloud. Similarly the key value will send to the user and the admin.

References

[1] Chandravathi D, Roja, P, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz"S Method", International Journal of Computer Science and Engineering, Vol.36, No.4, 2010, Pages 18-21.

[2] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", Proceedings of the 2011 International Conference on Information Science and Application, April 2011, Pages 1-7.

[3] M. Nupoor, I Yawale, V. B. Gadicha 2, "Third Party Auditing for Secure Data Storage in Cloud through Trusted Third Party Auditor using RC5", International Journal of Application or Innovation in Engineering & Management, Vol. 3, No. 3, March 2014, Pages 493-497.

[4] Qian Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactional Paper, 2011, Pages 1-5.

[5] K.S. Suresh, K.V. Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Acience and Software Engineering, Vol. 2, No. 10, October 2012, Pages 110-114.

[6] Ling Li, Lin Xu, Jing Li, Changchun Zhang, "Study on the Third-party Audit in Cloud Storage Service", International Conference on Cloud and Service Computing, 12-14 Dec. 2011, Pages 220-227.

[7] SlawomirGrzonkowski, Peter M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", IEEE Transactions on Consumer Electronics, Vol. 57, No. 3, August 2011.

[8] P. Rewagad, Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", IEEE International Conference on CSNT, April 06 – 08, 2013, Pages 437-439.