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. 5, May 2014, pg.530 – 533

REVIEW ARTICLE

A Review Report on Secured Encryption in Cloud Computing using Symmetric Cryptography

Anand D.Darne[1], Prof. Rushikesh Longadge[2], Prof. Pradnya Kambale[3]

[1]Student, G.H.Raisoni College Academy of Engineering and technology Nagpur (INDIA)

[2]Assistant Professor, G.H.Raisoni College Academy of Engineering and technology Nagpur (INDIA)

[3]Assistant Professor, Priyadarshini College of Engineering, Nagpur (INDIA)

[1] anadarne89@gmail.com; [2] rushi.longade@raisoni.net

Abstract--The paper proposes all the theoretical results related to privacy and security of cloud computing. We are implementing all these parameters in the form of basic cloud application and its deployment. Basically We are implementing attribute driven security model for cloud computing. Our application will be able to resist the attacks from various fields over confidentiality, integrity, availability, accountability, and privacy-preservability. Because these are the most attacked parameters in cloud computing.

Cloud computing provides innumerable benefits to its customers but it fails to solve information security concerns especially in public cloud. Symmetric Cryptographic Key is sensitive data and it is required to be stored at cloud platform to solve several problems of encrypted data such as searching/manipulation on encrypted data. This paper will present a technique that will manage symmetric cryptographic keys on cloud-based environment. Proposed technique is based on secret splitting technique enhanced Shamir's algorithm. Proposed technique will implemented in Open Stack private cloud environment for performance analysis.

Keywords- Public Key Cryptographic Standard (PKCS7); Public Key Infrastructure (PKI); Cryptographic Key Management (CKM); National Institute of Standard & Technology (NIST); Secure Shell (SSH).

I. INTRODUCTION

Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. We have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute. Cryptographic key management includes all operations that can be performed on cryptographic key except encryption/decryption. These operations comprise but are not limited to generation, revocation, sharing and storage of cryptographic keys. One possible solution towards cryptographic key management for cloud is, to download data on client terminals for appropriate operation, and after that operation, upload data back on cloud server. This solution deviates from the benefits of cloud paradigm since all computations are performed on client

machine. In addition, there is an overhead involved in upload and download. Section II will provide a detail analysis of other existing techniques related to cryptographic key management for cloud epitome.

II. EXISTING SYSTEM FOR SYMMETRIC CKM PROTOCOL FOR CLOUD BASED ENVIRONMENT

This research provides a protocol that will generate, store, distribute and revoke symmetric cryptographic key as per consumer requirement on cloud platform. Figure 1 shows a high-level architecture for symmetric cryptographic key management.

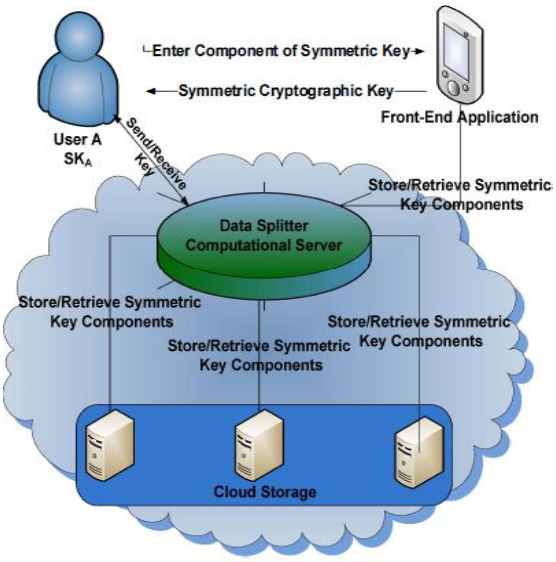

Fig 1:. Architecture of symmetric key management

III. PROPOSED SYSTEM FOR SYMMETRIC CKM PROTOCOL FOR CLOUD BASED ENVIRONMENT

A. Cryptographic Key Generation/Storage for Proposed Protocol

User can generate new symmetric cryptographic key K or can store already existing cryptographic keys as required using proposed technique. Key splitter in figure 1 will use Enhance Shamir's Algorithm to split key K in N pieces

K1, K2….Kn.

Proposed scheme store each piece on J storage disks such that each storage contain only one piece of K and

$$\sum_{J=1}^{J=n-1} \quad \mathbf{J=N-1}$$

One main piece lets Kn of key will be assigned to consumer of application. This piece of key has information of all other pieces and actual key cannot be regenerated without this piece. [f key length is less than minimum length required it will padded by some special character. Size of N will depend on available disks to store data. All data will travel on network using secure shell (SSH) for safe communication. Key will be stored in a database that store key component with its specific id and sequence number. Single storage contains one component of generated key at the same time. Different vendor's storage services on cloud can also be used. For example, one component can be stored on one cloud vendor's storage. Other can be stored on other vendor's storage and so on.

B. Key Transfer

User can transfer completely computed key or the component of key on public cloud for data processing.
Public Key Cryptographic Standard (PKCS7) will used to transfer such key that is developed by RSA Laboratories and used to wrap data in an envelope to securely transfer it. This protocol used to wrap message in an envelope and signed by sender. Receiver knows the decryption key to decrypt the encrypted message.

C. Cryptographic Key Retrieval for Proposed Protocol

On the request of key retrieval all, the components will fetch the key from key store through computational server, as shown in figure [and send to client terminal via Public Key Cryptographic Standard (PKCS7). Client machine will prompt consumer of application to enter his/her piece of key. Original Key will compute on the fly after taking information from consumer on consumer's terminal. During recalculation of cryptographic key, Enhanced Shamir's will recover all missing part and still regenerate original key if and only if count of missing part will less than threshold value and main part of key will available that is own by key owner.

K= Kl Operation K2 Operation,..., Kn

D. Proposed Enhanced Shamir's Algorithm

The goal of basic Shamir's algorithm is to divide cryptographic key K in n safe pieces K1, K2, ... Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. J is known as threshold value for this algorithm and scheme is called (K, J) threshold scheme. Proposed enhancement in Shamir's algorithm is to divide Key in n parts K1, K2, ... Kn such that there exist a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. In addition, threshold is set to h, and there exist K1, K2, .. , Kh parts on key retrieval operation and does not include Kt part in it. However, K cannot be computed without especial part Kt unlike in original Shamir's algorithm. Figure 2 describes a high-level algorithm for proposed technique.

```
Input:
    1. Secret key to store
    2. User own key component
Output:
    1. Complete key in case of key retrieval
    2. Key storage and user component in case of key storage request.
    Begin:
    If (request==”Key storage”)
{
        Split Key:
        Store on different storage;
        Display user’s component of key to user
 }
    Else if(request==”key transfer”)
 {
    Use PKCS7 protocol
  }
    Else if (request==retrieval of key)
 {
     Collect all components of specific key;
     Send to user machine;
     Take user’s part of key;
      If(all parts exist)
    {
      Generate actual key based on all          information
    }
    Else if(userpart exist&&
StoredComponentSize=collected component size-1)
 {
    Try recovery key();
  }
}
  Display output();
   End
```

Fig.2 Algorithm of proposed technique

Multiple storage disks act as key store on cloud platform. These disks can be resides in same locality as well as in different locations as shown in figure 1. These disks will play the role of nodes used in Shamir's algorithm and are assigned single piece of key. There will be N-l disks so that each disk Di contains Ki where 0> i <= n-l.

IV. RESEARCH METHODOLOGY TO BE EMPLOYED

The overall out of this whole process is the image with segmented image with ROI. We have to test efficiency of the segmentation algorithm. Improved result should get through this project work.
Summarizing, the presented solutions are promising and give a good base for our further research in the area of cytological image segmentation. Additionally, all preparation steps including pre-segmentation and the automatic nuclei localization stage can be reused with other segmentation algorithms which need such information.

V. CONCLUSION AND FUTURE WORK

We are implanting the attribute driven methodology, so this will touch every attribute of cloud computing. This attribute will be first attacked by ourselves and then we are employing the defense method based on these attacks. So possibly the efficient cloud computing model will be appeared with transparent attribute after successful implementation of this method. We can implement this model in various cloud computing platform to get the more efficient way of cloud computing such as SaaS, AaaS etc.

REFERENCES

[1] Yinqian Zhang, A. Juels, A. Oprea, and M. K. Reiter, "HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis," in 2011 IEEE Symposium on Security and Privacy (SP), 2011, pp. 313- 328
[2] E. Keller, J. Szefer, J. Rexford, and R. B. Lee, "NoHype: virtualized cloud infrastructure without the virtualization," in Proc. 37th annual international symposium on Computer architecture, New York, NY, USA, 2010, pp. 350-361
[3] H. Chen and B. Sun, "Editorial," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 65-66.
[4] M. Barua, X. Liang, R. Lu, X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing ," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 67-76.
[5] N. Jaggi, U. M. Reddy, and R. Bagai, "A Three Dimensional Sender Anonymity Metric," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 77-89.
[6] M. J. Sharma and V. C. M. Leung, "Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 90-100.
[7] N. Cheng, K. Govindan, and P. Mohapatra, "Rendezvous Based Trust Propagation to Enhance Distributed Network Security," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 101-111.
[8] A. Fathy, T. ElBatt, and M. Youssef, "A Source Authentication Scheme Using Network Coding," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 112-122.
[9] L. Liu, Y. Xiao, J. Zhang, A. Faulkner, and K. Weber, "Hidden Information in Microsoft Word," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 123-135.
[10] S. S.M. Chow and S. Yiu, " Exclusion-Intersection Encryption," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 136-146.
[11] Resch, Jason; Plank, James (February 15, 2011). "AONT-RS: Blending Security and Performance in Dispersed Storage Systems" Usenix FAST'll, 2011.

