International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-1, Issue-1, July-2014

Security Procedure for Shared Data in Cloud Computing

Nishant Rai
Assistant Professor, IISE, Department of Computer Application, Lucknow
Uttar Pradesh, India.
nishant_iise@yahoo.co.in

Deepti Gupta
Assistant Professor , IISE, Department of Computer Application, Lucknow
Uttar Pradesh, India.
deepti_182@yahoo.com

ABSTRACT
Today, data is more precious than gold. As most of the IT industries and users are migrating to cloud environment, their data is at a higher risk in terms of security. Cloud providers are implementing new security policies to provide better security to their users. Many encryption algorithms like RSA (Rivest Shamir Adleman) or DES (Digital Encryption Standard), provides security in general but in some cases these algorithms may be not so effective thus, the security threat arises when the data is shared between the cloud users. This paper aims to provide a procedure for secure data sharing between cloud users.

Keywords
RSA, Encryption, Public key, Private key, Cloud computing.

1. INTRODUCTION
Cloud computing is the delivery of computing services over the Internet. Cloud service allows individuals and businesses to use software and hardware that are managed by a remote users at remote locations. Cloud computing technology provides a shared pool of resources, which includes storage space, networks, printers, and some specialized user applications.

Cloud computing has started to obtained widespread popularity specially in small and medium size business organizations (SMB), because of their business model and inability to expense large money in an infrastructural enhancements. Therefore, cloud computing technology has started to obtain mass appeal in these small and medium size business corporate. Here, the data centers are enables the data to concentrate and operate as in internet through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner. Small business corporate can access these resources and expand or shrink services as business needs change more effectively[1].

Cloud computing technology is also popular because they can reduce the cost and complexity of not only SMB's but any organization computers network. Thus, in cloud computers technology users do not have to invest in infrastructure, hardware and software. Some other benefits to users include scalability, reliability, and efficiency. Scalability Means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via internet.

As per the experts opinion, cloud computing is going to be the face of future. But the promise of the cloud cannot be fulfilled until IT professionals have more confidence in the security and safety of the cloud. Security is a two-sided coin in the world of cloud computing. People come to the cloud from different point of views. At one side cloud providers are implementing best security policies to maintain confidentiality and integrity of data. On the other side many believe the cloud to be an unsafe place. After all once users send their data to the cloud, they lose complete control over it.

Since cloud providers have complete access to user's data, there is a strong need of security against unauthorized access of data. Encryption techniques provide a good solution to this problem. Various algorithms like RSA is one of the strongest security measures, cloud providers are adopting.

2. SECURITY IMPLEMENTATION USING RSA

RSA is widely used Public-Key algorithm. It stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data [2][3][4].

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

2.1. Key Generation
2.2. Encryption
2.3. Decryption

2.1 Key Generation
Key generation is the first step of the algorithm. This process is done between the Cloud provider and the user. It has following steps:

1. Randomly choose two distinct large prime numbers a and b.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. e is released as Public-Key exponent.
5. Determine d as follows: d = e-1(mod Ø(n))
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of (e, n).
8. The Private-Key consists of (d, n).

2.2 Encryption

Encryption is the process of converting original (plain) text into cipher text. It has following steps:
1. Cloud provider should send the Public-Key (n, e) to the user who wants to store the data on provider's site.
2. User data is now mapped to an integer by using padding scheme.
3. Data is encrypted and the resultant cipher text C is = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

2.3 Decryption

Decryption is the process of converting the cipher text to the original plain text. It has following steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme [4][5][6][7][8][9].

3. FLAW IN SECURITY

RSA algorithm ensures that confidentiality is guaranteed because the information is encrypted before it is uploaded for cloud storage, but complete privacy could not be guaranteed by these vendors if data is to be shared between two cloud users[10][11][12].
In the secure cloud storage, providers may easily issue fake identity credentials to people using the service. The providers may use a their own key to decrypt and view the private information, then re-encrypt it before sending it on to its intended recipient.
As a result, whenever data is shared with another user or group of users, the storage service may perform a man-in-the-middle attack by pretending to be another user or group member. This happens without alerting the customers, who believe that the cloud storage provider cannot see or access their data.

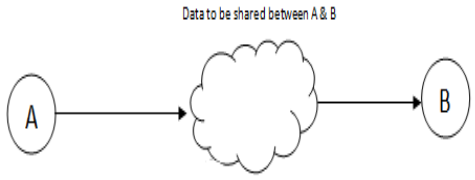


Figure 1: Data sharing in cloud

It can be explained as follows:

- A wants to share some data with B.
- A requests B's key for encryption through cloud.
- B sends its key to cloud.
- Cloud provider sends phony key to A, instead of B's key.
- A encrypts data with the key provided by cloud and store it on cloud.
- Cloud decrypts the data, reads it and re-encrypts it using B's key.
- B accesses the data without knowing that it has already been accessed by the cloud provider.

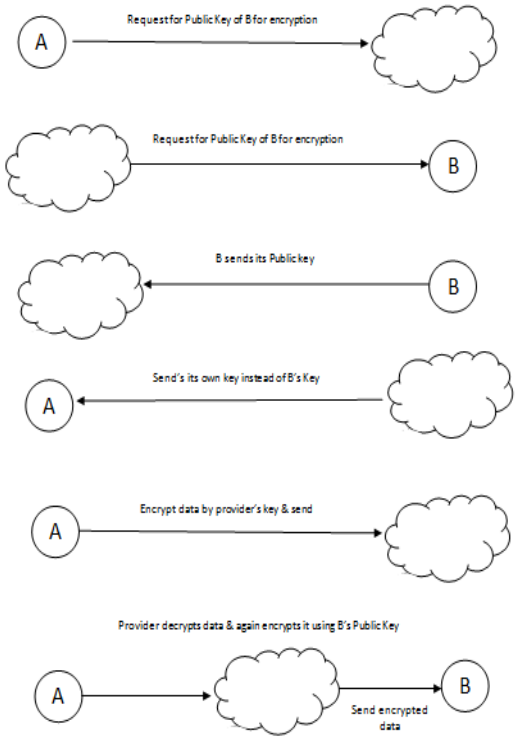


Figure 2: Process of unauthorized access of shared data

4. PROPOSED METHOD

In the above mentioned problem a middle-man (cloud provider) who issues the key to the users is same who is storing the data. So there are chances that this data can be accessed by cloud provider without any permission [10][11][12].
To resolve this problem a method is suggested in which two different entities are used for issuing the key and storing the data. Both the entities are unaware of each other. In this case users share the key with the help of a trusted third party while data is shared by cloud provider. Neither the third party nor the cloud provider will have access to both key and data. Hence there is no possibility of unauthorized access of data.

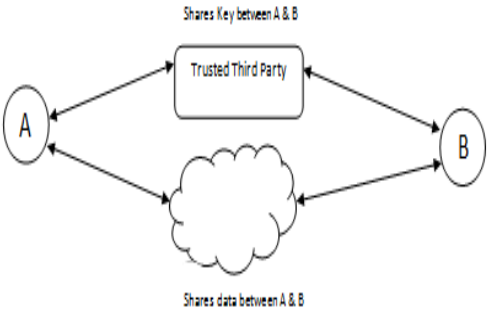
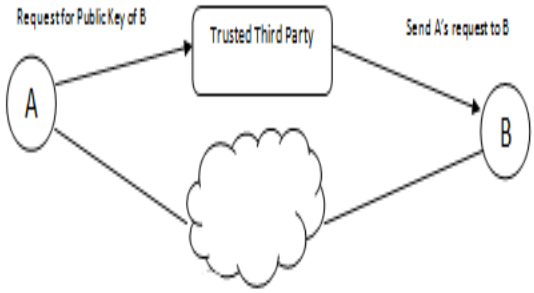
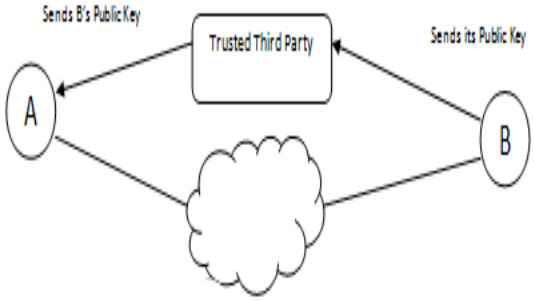


Figure 3: Data sharing with the help of third party

This can be explained as follows:

- A wants to share some data with B.
- A requests for B's key with a trusted third party, instead of cloud.
- B sends its key to A via third party.
- A encrypts the data with B's key and send it to cloud.
- B accesses the data by decrypting it with its own key.





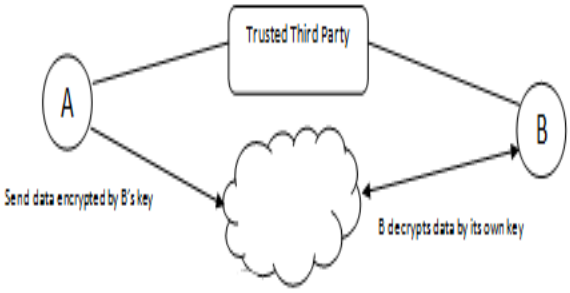


Figure 4: Process of secure data sharing

5. CONCLUSION

This paper explores a big security flaw in cloud environment, if two users want to share some data, and suggest a procedure to deal with. This paper concludes that inclusion of a trusted third party for sharing of encryption key removes any possibility of unauthorized access as sharing of key and data will be done through different channels. This procedure ensures securing sharing of data between cloud users.

REFERENCES

1. http://www.webopedia.com/TERM/C/cloud_computing.html
2. Parsi Kalpana ,et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012
3. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.
4. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.
5. Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.
6. V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2,No.6, Nov-Dec 2011.
7. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.
8. Birendra Goswani, Dr.S.N.Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices", International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.
9. G. Jai Arul Jose, C.Sanjeev, Dr. C.Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011.
10. Duane C Wilson. Giuseppe Ateniese. 'To Share or Not to Share' in Client-Side Encrypted Cloud. arXiv 2014
11. http://www.sciencedaily.com/releases/2014/04/140415125259.htm
12. http://hub.jhu.edu/2014/04/16/cloud-storage-security-flaw