International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

Cloud Data Encryption Ensuring Security

Madhavi Dhingra
Amity University
Madhya Pradesh

Abstract **– Cloud computing is providing software, infrastructure, platform services all over the world and the percentage of its clients are increasing day by day. While data is stored over the cloud to remove the complexity of the maintenance work; it becomes a matter of concern the security of the data which is now in the open network of cloud. For securing cloud data, protection strategies have to be employed. Strategy should be applied to both data at rest and data in transit. The goal of encryption is to ensure that data stored in the cloud is protected against unauthorized access. Access to sensitive user data by third parties is a violation of privacy. This paper elucidates some existing encryption schemes of different kinds for securing enterprise data in the cloud. Also, it identifies efficient techniques by highlighting their salient features.**

Keywords: Cloud Data, Secure data, Cloud Data Encryption

I. INTRODUCTION

Internet age is growing at a very rapid rate in every field of applications. All the networks transfer information amongst them. To reduce the costing of the infrastructures, software, and the applications, Cloud computing has been devised. All the data and information will be stored over the cloud from where the users can access and use it in their applications. But with cloud computing, there comes loss of control. Since data is stored at the third party, so the user cannot be sure about its security. Since networks of the internet are the main target of the attackers, cloud can also be attacked by various kinds of intruders. To protect cloud data against such threats and attacks, data over the cloud must be secured.

Therefore, 2014 could well be designated as the year of encryption, as Enterprise Networking Planet contributor Paul Rubens wrote for BBC.com.[1] Cloud data encryption solves many of the control challenges that enterprises face in the cloud. Encrypting the data over the cloud will prevent it from access by unauthorized users. Also, user will keep more focus on data instead of the infrastructure.

II. CLOUD ENCRYPTION

To protect online data over the network is a complex task which requires robust and layered protection schemes. Encryption is a powerful protection mechanism that prevents the risk of threats and attacks. Cloud Data Encryption mathematically transforms data so that it becomes impossible to break the code without the "key" that can be used to change the data back to its original form.

A Ponemon Institute study, Patient Privacy & Data Security found that the average economic impact of a data breach has increased from 0.4 million to a total of 2.3 million since 2010[2].

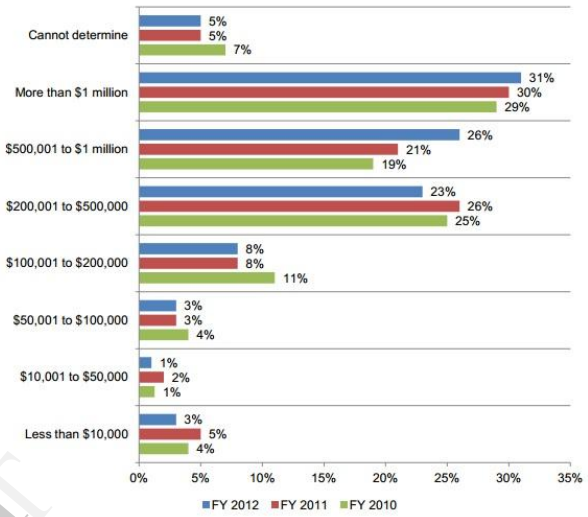

Fig. 1 Economic Impact of Data Breach incidents experienced in 2010-2012 [2]

A. *Types of Encryption*

Encryption over the cloud data can be done in two ways. First, the client can encrypt data on his side and then store it over the cloud. And second, the cloud service provider gives the encryption.

Client-side cloud data encryption

Client side cloud data encryption uses cloud encryption gateways which enable enterprises to detect and encrypt the sensitive data when it is transferred outside its network. A number of public cloud services provide these gateways like Salesforce, Box, Dropbox, etc.

Provider-side cloud encryption:

Also known as server-side encryption is most commonly used mode by which cloud service provider provide encryption on users data. This approach is implemented by various companies like Google, Yahoo etc where cloud provider manage the encryption of data. Server-side encryption limits the complexity of the environment and maintains the isolation of data.

B. *Encryption guidelines*

1. Determine the category of data to be encrypted: Various kinds of data from multiple organizations need to be secured on the cloud. Before starting the process of encryption, data must be classified in order to determine the extent and the parts of the data to be encoded. For example certain data is so confidential that the tiniest leak cannot be accepted whereas in other cases only some part of data is encrypted e.g. payment credit card number. Data can be classified as

public and non-public data. Public data is the general data whose accessing doesn't do any harm and therefore need not be encrypted.

2. Different security controls are used for data at rest and data in transit. NIST (National Institute For Standards And Technology) have given some security controls for securing stored data. Implementation of authentication mechanisms and performing encryption of stored backup data are some of the controls.

3. Securing data in transit is as important as stored data, as attacker may hack or attack the data while it is moving from one network to another. Security measures such as Use of Virtual Private Network, Two-factor authentication, SSL (Secure Socket Layer) Certificates should be used for securing the mobile data.

4. Selection of Encryption Technique: Different levels of encryption are there like storage-level encryption, database-level encryption and application-level encryption. The level is selected according to the nature of data.

5. Key Management: Strong security comes with strong key management. Accordingly different cryptographic keys are defined by NIST.

III. ENCRYPTION ALGORITHMS

In the cloud, encryption algorithms are used for securing data travelling over the network, so that malicious users can't get access to the confidential information.

Security algorithms are classified into two types – Symmetric Algorithms and Asymmetric Algorithms. Symmetric algorithms make use of one key, while asymmetric algorithms uses two keys one public and other private key. Existing algorithms used for encrypting cloud data are [3] –

A. RSA- (Rivest Shamir Adleman)

RSA is most commonly used asymmetric algorithm used for public-key cryptography. Messages encrypted by public key can only be decrypted by using the private key which will be with the authenticated user.

B. MD5- (Message-Digest algorithm 5)

A widely used cryptographic hash function algorithm with a 128-bit hash value processes a variable length message into a fixed-length output of 128 bits. First the input message is broken up into chunks of 512- bit blocks then the message is padded so that its total length is divisible by 512. In this, the sender of the data uses the public key to encrypt the message and the receiver uses its private key to decrypt the message.

C. AES- (Advanced Encryption Standard)

It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits respectively. It ensures that the hash code is encrypted in a highly secure manner.

D. Fully Homomorphic Encrypton Technique

A new data encryption technique has been invented by IBM called "Fully Homomorphic Encryption". In other encryption techniques, data is decrypted first and then analyzed. But this new technique prevents the data security without decrypting. Data can be analyzed anywhere in its original form.

This method is beneficial for cloud users, as data can be stored in secure form and manipulated whenever required in the same form without doing decryption. Private and confidential data can therefore be analyzed in the cloud without exposing data to cloud services [4].

A review paper on Encryption Techniques for Cloud Data showed the encryption approaches that have been used to ensure data confidentiality in cloud. The result of this review is the level of use of the encryption techniques.

The encryption techniques taken into account were RSA, Data Encryption Standard (DES) , SSL (Secure Socket Layer), Mixed encryption algorithms, RC5, Role Base Encryption (RBE), Geo encryption, location based encryption and decryption of data, Proxy re-encryption (PRE) and Hierarchical attribute-based encryption (HABE)[5].

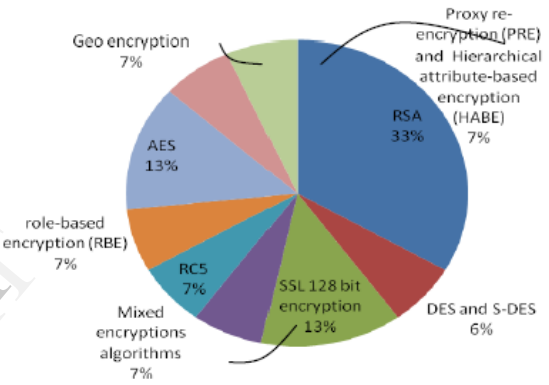

Fig. 2 Encryption Techniques for Cloud Data Security[5]

IV. CLOUD SECURITY SOLUTION PROVIDERS

Many cloud security solutions are available in the market and most notable amongst them are -

1. The AppProtex Cloud Data Protection Gateway. The provider uses cloud data encryption and tokenization to provide a vital level of SaaS (Software as a Service) security without sacrificing application functionality. It provides the ability to preserve SaaS functionality across a wide array of applications while maintaining the highest level of cloud tokenization or cloud encryption protection [6].

2. The CipherCloud Open Platform. The provider has a single platform for preventing confidential client data over cloud applications. It also makes sure that the usability, functionality and performance of the data is not affected. CipherCloud delivers a comprehensive set of protection controls including encryption, tokenization, activity monitoring, data loss prevention (DLP) and malware detection that can overcome your cloud security concerns [7].

3. Vormetric Data Security Solution. Vormetric cloud security solutions provide Cloud Security Compliance to meet security requirements, fine grained access controls to prevent unauthorized access of data, data breach protection to protect from data security breaches using secure key management system in encryption and Security Intelligence to provide the raw cloud security intelligence information [8].

4. Porticor Virtual Private Data. Porticor make use of homomorphic split-key encryption for data encryption providing more economical and secure solution for the data over the cloud [9].

V. CONCLUSION

In this paper, we have gone through the need of encryption to be done over data. Also, various encryption guidelines need to be considered to ensure better security over cloud. As networks are getting bigger, data over the cloud is multiplying, resulting in big data. Huge amount of data stored on the cloud by the enterprises needs security. Thus, Encryption as a service comes in the cloud. Various encryption algorithms are used for encoding cloud data. Furthermore there are various cloud providers that provide number of security solutions to prevent unauthorized access over the network of cloud. Still there's a need to design new techniques and refinements as organizations are seeking a perfect solution to protect their data.

REFERENCES

[1] Jude Chao, "Cloud Computing Demands Cloud Data Encryption", May 13 2014, Available at: http://www.enterprisenetworkingplanet.com/netsecur/cloud-computing-demands-cloud-data-encryption.html
[2] "Third Annual Benchmark Study on Patient Privacy & Data Security", Ponemon Institute, December 6, 2012, Available at: http://www.onlinetech.com/encryption-of-cloud-data-full-access
[3] M. Vijayapriya, "Security Algorithm in Cloud Computing: Overview", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345, Vol. 4 no. 09, Septembe 2013, Pg. 1209-1211
[4] James Sullivan, "IBM Patents Data Encryption Technique For Cloud Computing", December 26, 2013, Available at: http://www.tomsitpro.com/articles/cloud-computing-ibm-homomorphic-encryption-cloud-security,1-1506.html
[5] Aized Amin Soofi, M.Irfan Khan and Fazal-e-Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid Distribution Computing, Vol.7, no.4,2014,pp.11-20, Available at: http://dx.doi.org/10.14257/ijgdc.2014.7.4.02
[6] "AppProtex Cloud Protection Gateway", Available at: http://perspecsys.com/perspecsys-cloud-protection-gateway/appprotex-cloud-protection-gateway/
[7] "CipherCloud Products", Available at: http://www.ciphercloud.com/products/
[8] "Vormetric Data Security Solutions Data Security for Cloud Environments", Available at: http://www.vormetric.com/data-security-solutions/cloud-data-security
[9] Porticor Virtual Private Data. Available at: https://www.porticor.com/porticor-virtual-private-data/
[10] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 2, Issue 6, November – December 2013, ISSN 2278-6856, Pg. 270-274.
[11] Mohammad, John, Ingo, "An Analysis of the Cloud Computing Security Problem", In Proceedings APSEC 2010 Cloud Workshop, Sydney, Australia, 30 November 2010.
[12] Mandeep, Manish, "Implementing Various Encryption Algorithms to Enhance the Data Security of Cloud in Cloud Computing", International Journal of Computer Science and Information Technology, Vol.2 No.10 October 2012.
[13] A. Padmapriya, P. Subhasri, "Cloud Computing: Security Challenges and Encryption Practices ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 3, March 2013.
[14] Mohit Marwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing" , IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814.
[15] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (Online): 2279-0055, IJETCAS 13-123; Pg. 141-146.
[16] Jawahar Thakur, Nagesh Kumar, DES, AES and BlowFish: Symmetric Key Cryptographic Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 1, Issue 2, December 2011.