International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Survey on Cloud Computing Security Algorithms

Akash Kanthale[1], S. P. Potdar[2]

[1]Student, Department of IT, SCOE, Pune, Maharashtra, India

[2]Assistant Professor, Department of IT, SCOE, Pune, Maharashtra, India

Abstract: ***With the fantastic growth of sensitive information on cloud, cloud storage security is becoming more important than even before. The cloud data and its services reside in relatively scalable data centres and can be accessed from everywhere. The growth of the cloud users has been accompanied with a growth in malicious activities in the cloud. More and more vulnerabilities are get discovered, and nearly every day, new upcoming security advisories are published. Millions of users are surfing the Cloud system for various purposes, therefore they need purely safe and persistent services. The future of cloud, especially in extending the range of applications, involves a much higher degree of privacy, and authentication. Any technology can't be said perfect until it is 100% free from any vulnerability. So whenever a new technology is introduced the security is the first feature that is countable. There are many technologies that are used for online data storage, accessing the data at any location and provide the online usage of any software. Cloud computing is the technology that provides the online data storage and the most important services that it provides software on hiring facility. In this paper, a survey on some of the cloud security algorithms is performed and compared.***

Keywords: Cloud, Algorithms, public, private, encryption, decryption

1. Introduction

Cloud computing is emerging as a new key computing platform for sharing resources which include infrastructure, software, and applications processes. Gartner predicts in 2015, 10% of overall IT security capabilities will be delivered in the cloud system, with focus on messaging, web technology security and remote vulnerability assessment. Some of the other focus areas will include data-loss detection and prevention, encryption, and authentication. As technologies aimed to support cloud computing mature[1]. Cloud computing is delivery for computing services over the Internet. Cloud services provides individuals and businesses to use software and hardware that are managed by any legal third party at remote locations. Examples of cloud services include online file storage and social networking sites etc. Cloud computing provides a shared pool of high end resources, including storage space, networks, computer processing power, and some of the specialized corporate and user applications. The main notion behind cloud computing is that work done on the client side can be moved at some unseen cluster of resources on the internet. Cloud Service Provider (CSP) maintains system database and applications for the users on a remote server and provide independence for accessing them from any place through a connected network. Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [12] as a model for convenient and on-demand network access to a shared pool of configurable computing resource (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimum management effort. "The NIST definition is one of th e finest and most comprehensive definition of cloud computing and is widely used in US government documents and projects.

There are three basic cloud service categories: software as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). Cipher is an algorithm for encrypting and decrypting a message. It becomes very difficult for a hacker if the data present in cloud is in encrypted form, as the data files or encrypted data blocks are too useless for any person unless he knows the method for decrypting it. Generally companies with critical data sets, encrypt data using an appropriate cipher algorithm before storing it to the server.

Four different cloud deployment models are used currently and along with 3 types of integration systems among them:

- Public Clouds
  It is very common type of cloud deployment model. Customers uses the services offered by cloud service providers. Most of the companies providing these services today such as sky drive, Google drive and iCloud services. Customers never have idea about the infrastructure and working of the computing mechanism. Consumers can add data or retrieve the data at any moment as required. Security aspects are taken care by the service providers.
- Private Clouds
  This type of cloud is mainly used at large companies and enterprises. People are given a completely private environment for storage and they can use the security measures best suited for them. Disadvantages of this model is the cost of such deployment is high. Mostly used in banks for provide private services to customers and employers.
- Hybrid Clouds
  This type of deployment is basically used when it need both the private and public deployment model simultaneously. The security strategies are mostly independent for both type of services. The cost required is less as both type of models are integrated in one system. Best example can be Amazon's simple storage service.
- Community Cloud

More than one single infrastructures are used by this type of model. More than one organizations can control service deployment model. The control may be administered by more than a single provider. Used when many organizations may have a shared interest to use a single cloud model.

- IaaS - Infrastructure as a service Cloud infrastructure services are used to maintain and monitor the cloud data, networking or network services. The requirements can be based on consumption of resources by the users.

- PaaS - Platform as a service Cloud platform services are used in the development of applications and for providing cloud components in them. Framework for further development can be achieved using such services.
- SaaS – Software as a service Cloud software service is used to manage third party software on the client side. Such applications can run directly using the web plugins and no downloads or such installations are required for using such services.

2. Related Work

In Cloud Storage, any organization's or individual's data can be stored in and accessible from multiple distributed and connected resources or locations that comprises cloud. To provide secured communication over distributed and connected resources, encryption algorithms [5] plays a vital role. It is the basic tool or method for protecting the data. Encryption algorithm converts the data into scrambled form by using "key" and only authorized user have the key to decrypt the data. In Symmetric key encryption, one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption in which two keys-private and public keys are used. Public key is used for encryption and private key is used for decryption [6]. User's data can be made secured in the cloud using encryption. But the question arises that is user's data really encrypted when it is stored in the cloud? If CSP does provide encryption, what encryption algorithm is to be used? What is the key's length? Not all encryption algorithms are created equal. Cryptographically, some of the algorithms provide insufficient security; especially non genuine algorithms should not be trusted. Most secure data encryption solutions support all of the major business use cases: full disk encryption [4], database encryption [5], file system encryption [5], distributed storage encryption and even row or column encryption. CSP cannot provide such encryption granularity to each user in each level.

In [1], the Advance Encryption Standard is proposed for cloud Security. AES is a block cipher having block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. Generally AES with 128 bit key length is significant. The encryption process contains 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical [1]. 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words [6]. The 4 x 4 matrix of bytes made from 128-bit input block is referred as the state array. Before any round-based processing for encryption can begin, input state must XORed with the first four words of the schedule.

For encryption, each round consists of the following steps:

- SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
- ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times
- MixColumns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

In [2], a hybrid approach is used in which two algorithms used one after another to make the encryption complex. It uses advance encryption standard followed by RSA algorithm. An integrated approach is used to secure the data on the cloud using two different techniques. As the double encryption is used by the system, then if the attacker is tries to attack on the data, then it would be difficult for decode the data for the attacker. RSA is used after AES here because there is a big advantage of RSA algorithm. If the attacker may able to decrypts the data of RSA cipher then it will give the results which will be different from the original data. In this hybrid technique the steps that will be performed under the hybrid algorithm are Key Generation, Data Encryption, Private Key Encryption, Private Key Decryption, and Data Decryption.

In [3], another hybrid approach is used which is again integration of two algorithm DES (Data encryption standard) and RSA. The proposed system is designed to maintain security of text files or non-text files. This proposed system uses DES & RSA algorithm together to generate encryption when user uploaded the text files in Cloud Storage and inverse the DES & RSA algorithm to generate decryption when user download that file from Cloud Storage, for increasing security[10]. The proposed system is designed to maintain security for text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) For Encryption of text files:

- Upload Text file.
- Implementing the DES algorithm of Encryption to generate first level encryption.
- Implementing the RSA algorithm of Encryption to generate second level encryption.
- Store Cipher Text into Database. 2) For Decryption of text files:
- Read Cipher Text from Database.
- Implementing the RSA algorithm of Decryption to generate first level decryption.
- Implementing the DES algorithm of Decryption to generate Plain text.
- Display Plain Text to User.

3. Literature Survey

Table 1: Literature Survey

Title	*Author*	*Conference/Journal*	*Mechanism*	*Limitation*
1] Enhancing Cloud Computing Security using AES Algorithm	AbhaSachdev, MohitBhansali	International Journal of Computer Applications	Uses AES Standards which is block cipher algorithm. Uses 128, 192, or 192 bit key [1].	It requires more computing cost as compared to DES.
2] A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks	Navdeep Singh, Pankaj Deep Kaur	International Journal of Database Theory and Application	It use AES followed by RSA algorithm. AES(128, 192,256 bit key) RSA (1024 bit key).	Most complex system. Need high end processors [7]. Need more costly hardware. Time efficiency is less on slow hardware
3] Security in Cloud Computing using Cryptographic Algorithms	Shakeeba S. Khan, Prof.R.R. Tuteja	International Journal of Innovative Research in Computer and Communication Engineering	It uses DES followed by RSA algorithm. DES (64 bit key), RSA (1024 bit key).	DES is weaker than AES. Key size for DES is small, can get access to system under Brute force attack[9]

4. Conclusion

This paper is a survey report on various algorithms and there combinations for cloud storage security using encryption. It shows the limitations like need of extra processing power or need of high end processors and hardware. It highlights the shortcomings of these some of the algorithms. The future scope of this paper is to overcome these limitations by eliminating the need of high end hardware and securing the cloud data significantly.

References

[1] AbhaSachdev, MohitBhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.
[2] Navdeep Singh and Pankaj Deep Kaur, "A Hybrid Approach for EncAgudo, Isaac and Nuez, David and Giammatteo, Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing,
[3] Data Management, and Applications, pages 190–197, Springer Berlin
[4] Heidelberg, 2011.rypting Data on Cloud to prevent DoS Attacks", International Journal of Database Theory and Application Vol.8, No.3 (2015), pp.145-154.
[5] Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.
[6] AishwaryaAsesh, "Encryption Technique for a Trusted Cloud Computing Environment", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. V (Jan – Feb. 2015), PP 53-60.
[7] Talbot, David (2009). "How Secure Is Cloud Computing?" Technology Review [Online]. Available:
[8] http://www.technologyreview.com/computing/23951/
[9] Agudo, Isaac and Nuez, David and Giammatteo, Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing,
[10] Data Management, and Applications, pages 190–197, Springer Berlin Heidelberg, 2011.
[11] J.Daemen, L. R. Knudsen, and V. Rijmen, "The Block Cipher Square", FSE'97, volume 1267 of Lecture Notes in Computer Science, (1997) , pp. 149–165.
[12]] R.Pahal, V. Kumar in "Efficient Implementation of AES" Dept. ECE, SGISamalkha, Haryana, India, International Journal of Advanced Research in Computer Science and Software Engineering.
[13] S C Rachana, Dr. H S Guruprasad, "Emerging Security Challenges in Cloud Computing ", International Journal of Engineering Science and
[14] Innovative Technology (IJESIT), Volume 3 Issue 2, pp.485-490, March 2014.
[15] G. Devi, M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal of Computer Trends and Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596, 2012.
[16] RashmiNigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.