Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms

Papri Ghosh
Research Scholar
Pacific University,
Rajasthan, India

Vishal Thakor
Asst. Professor
AURO University,
Gujarat, India

Dr. Pravin Bhathawala
UGC Visiting Professor
HNG University, Patan,
Gujarat, India

Abstract: ***The main usage of cloud computing is data storage. Enterprises are depending more on cloud. But security is a question which always arises in mind. Due to the vast amount of data storage on the cloud servers, cloud service providers become an attractive target and may get many threats. Security and privacy are the key issues and challenges for cloud storage. This paper discusses about cloud computing security issues and presented a comparative study of various security algorithms.***

Keywords: security, privacy, encryption algorithm, cloud computing.

I. INTRODUCTION

The first form of web based data storage is called cloud storage. This is a form of networked data storage where data files are stored on multiple virtual servers. Cloud computing isn't just about accessing applications over the web. The cloud can also be used to store documents either as a large pool of backup drive or as primary store of file storage. The servers used for cloud storage are hosted by third party companies who operate large data centers. When we subscribe to cloud storage we lease storage capacity from the cloud storage. The data may be stored across multiple servers and at multiple locations. The "cloud" is composed of hardware, storage, networks, interfaces and services [1]. Users can access the computing power, infrastructure, software applications and services on demand and they are independent of locations. Cloud computing is a pay-per-use model that enables real time delivery of highly scalable resources to different companies using the internet. The cloud computing concept is service oriented architecture. The cloud providers are maintaining the user's data in cloud environment. Security and privacy are one of the issues which users are concerned about as the data are with the providers. This paper studies the different security algorithms which are used to eliminate the concerns regarding data loss, privacy while accessing web application on cloud. Comparisons have been made between different algorithms to find the best security algorithm.

II. SECURITY ISSUES IN CLOUD DATA STORAGE

- The physical security with the data is lost as soon as we upload the data in the cloud. The resources are also shared among different companies. Users do not have any knowledge or control of where the resources are running and where the data's are being stored.
- Though the data transfer, storage and retrieval are done in response to authorized transaction. Common standard for data integrity not yet exist.
- The user's data personal data and information can be used or passed to other parties.
- The encryption and decryption is being done by the cloud service provider and even the keys are with them. Users do not have any control on their data once the data are being submitted to the cloud service provider. Logically the keys should be present with the users.

The above security issues discussed above shows that there are various policies issues and threats present in cloud computing technology. These issues include privacy, data segregation, reliability, storage, security, access control and many more. Looking into the different issues we realized that security is one of the main issues. It may be any enterprise data, an academics data or any simple users data, security is the main issue is security. So we can propose some encryption algorithm using some knowledge of existing algorithm.

III. ALGORITHMS USED IN CLOUD COMPUTING

- **RSA**

The most common asymmetric public key algorithm is RSA. [2] This algorithm is named after Rivest, Shamir and Adelman. In this algorithm the public key is shared and distributed to all which is used for encryption of the message and the other key is a secret key which is also called a private key and used for decryption.

RSA algorithm is used to ensure the security of data in cloud computing. We have encrypted our data to provide security with the help of RSA algorithm. The purpose of securing data is the only concerned so that only authorized users can access it. The encrypted data is stored in the cloud. When required a request can be placed to cloud provider to get access to the data . Cloud provider authenticates the user and delivers the data to user. As RSA is a Block Cipher in which every message is mapped to an integer. In the proposed cloud environment, Public key is known to all, whereas Private Key known only to 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 will be decrypted using the corresponding Private Key only.

- **AES**

Advanced Encryption Standard (AES) [2], also known as Rijindael named after Joan Daemen and Vincent Rijmen is used for securing information. AES is a symmetric block cipher that uses the basic techniques of substitution and Transposition. AES, symmetric key encryption algorithm is used with 128 bit block and key length of 128-bits. The implementation procedure is such that, User decides to use cloud services and will migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. When migration of data to the chosen CSP happens and in future whenever an application uploads any data on cloud, the data will first be encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This includes all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as as the 56 bit keys of DES were no longer considered safe.

- **DES**

The Data Encryption Standard (DES) [2] is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm.

- **BLOWFISH**

Blowfish [2] is a very strong symmetric key cryptographic algorithm. Blowfish encrypts 64 bit blocks with a variable length key of 128-448 bits. According to Schneier, Blowfish was designed with the followings objectives in mind:

a) Fast- Blowfish encryption rate on 32-bit microprocessors is 26 clock cycles per byte.

b) Compact- Blowfish can execute in less than 5 kb memory.

c) Simple-Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple.

d) Secure- Blowfish has a variable key length up to maximum of 448-bit long, making it both secure and flexible.

Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching).

IV. RESULTS

We have compared the above algorithms are the results are compiled as

	RSA	**AES**	**DES**	**BLOWFISH**
Key used	Asymmetric key	Symmetric key	Symmetric key	Symmetric key
Key size	1024 bits	128,19 2,256 bits	56 bits	32-448 bits
Initial vector size(plain text)	1024 bits	128 bits	64 bits	64 bits
Data encryption on capacity	Small amount of data can be encrypted	Large data can be encrypted	Data less than AES can be encrypted	Data less than AES can be encrypted
Security	Secured only for user	Secured for both user and provider	Secured for both user and provider	Secured for both user and provider
Authentication provided	Robust authentication	Best authentication provided	Somewhat less than AES	Can be compared with AES
Memory usage	Highest memory usage	Low RAM required	More memory usage as compared to AES	Can execute in less than 5 kb
Execution time	Requires maximum time	Faster	Requires same time as AES	Requires less time

V. CONCLUSION

Through this paper different encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges. The comparisons between AES, DES, Blowfish and RSA algorithms are shown. Comparison is done to find the best security algorithm, which has to be used in cloud computing for making cloud data

secure which cannot be hacked by attackers. Encryption algorithms play an important role in data security on cloud. Through the comparison, it has been found that

- AES algorithm uses least time to execute cloud data.
- Blowfish algorithm has least memory requirement.
- DES algorithm consumes least encryption time.
- RSA consumes longest memory size and encryption time.

By doing implementation for all algorithms, the desired output for the data on cloud computing has been achieved. As the demand of cloud is increasing in today's world so the security of the cloud is the top concern of the user. Hence, proposed algorithms are helpful for today's requirement. The comparison shows the effectiveness of different algorithms. In future such type of more comparisons with different approaches can be done to show effectiveness different algorithms. Looking into the comparisons a framework can also be proposed.

REFERENCES

[1] W. Stallings, Network Security Essentials (Applications and Standards), Pearson Education, 2004.
[2] A. Kahate, Cryptography and network Security, McGraw Hill Education (india) private limited, 2013.
[3] T. G. Peter Mell, "http://dx.doi.org/10.6028/NIST.SP.800-145," september 2011. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-145. [Accessed 2014].
[4] P. M. a. T. Grance, "http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf," 10 7 2009 . [Online]. [Accessed 15 april 2014].
[5] e. l. ITL, Introduction to Information Technology, new delhi: pearson, 2013.
[6] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, Pearson Education, 2004.
[7] N. Balkish, A. M. Prasad and V. Suma, "An Efficient Approach to Enhance Data Security in Cloud Using Recursive Blowfish Algorithm," ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I (2014-01-01) , pp. 575-582, 1 january 2014.
[8] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems Volume 25, Issue 6, June 2009, Pages 599–616, 2009.
[9] M. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, "Cloud computing distributed internet computing for IT and scientific resarch," IEEE, 2010.
[10] D. L. Dimitrios Zissis, "Addressing cloud computing security issues," Elsevier, 2010.
[11] H. S. S. E.-E. Eman M.Mohamed, "Data Security Model for Cloud Computing," in ICN 2013 : The Twelfth International Conference on Networks, pp. 66-74, 2013.
[12] D. Jamil and H. Zaki, "SECURITY ISSUES IN CLOUD COMPUTING AND COUNTERMEASURES," International Journal of Engineering Science and Technology vol 3 no 4, pp. pp 2672-2676, 2011.
[13] S. C. Kevin Curran, "cloud computing Security," in International Journal of Ambient Computing and Intelligence, 3(1), 14-19, , January-March 2011.
[14] M. lorga and A. karmel, cloud computing security: foundations and challenges, CRC press, Boca Raton, FL, 2016.
[15] S. S. Rohit Bhadauria, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," International Journal of Computer Applications, vol. Volume 47, no. Number 18, p. 47, 2012.
[16] A. S. Sambyal, D. Jamwal and G. S. Sambyal, "Cloud computing:A growing edge," in international conference on Upcoming Trends in IT, Punjab, 2010.

.

