Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926

# Secure User Data in Cloud Computing Using Encryption Algorithms

**Rachna Arora*, Anshu Parashar ****
*(Research Scholar, HCTM, Kaithal, Haryana)
** (Associate Professor, HCTM, Kaithal, Haryana)

## ABSTRACT

**Cloud Computing is transforming information technology. As information and processes are migrating to the cloud, it is transforming not only where computing is done, but also fundamentally, how it is done. As increasingly more corporate and academic worlds invest in this technology, it will also drastically change IT professionals' working environment. Cloud Computing solves many problems of conventional computing, including handling peak loads, installing software updates, and, using excess computing cycles. However, the new technology has also created new challenges such as data security, data ownership and trans-code data storage. In this paper we have discussed about cloud computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of various security algorithms.**

***Keywords*** **-** Algorithms: AES, Blowfish, DES, RSA, Cloud Computing, Data Security

## I. INTRODUCTION

Cloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. It is not a new technology but a way of delivering computing resources based on long existing technologies such as server virtualization. The "cloud" is composed of hardware, storage, networks, interfaces, and services that provide the means through which users can access the infrastructures, computing power, applications, and services on demand which are independent of locations. Cloud computing usually involves the transfer, storage, and processing of information on the 'providers' infrastructure, which is not included in the 'customers' control policy.

The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service oriented architecture [1]. Here comes the first benefit of the Cloud Computing i.e. it reduces the cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location. So instead of buying the whole infrastructure required to run the processes and save bulk of data which You are just renting the assets according to your requirements.

The similar idea is behind all cloud networks [2]. It uses remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way.

The advantage of cloud computing over traditional computing include: agility, lower entry cost, device independency, location independency, and scalability [1]. In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models [2], [3], [4], [5], [6]. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. Considering the role of the verifier in the model all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.

## II. SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues.

One issue with cloud computing is that the management of the data which might not be fully trustworthy; the risk of malicious insiders in the cloud and the failure of cloud services have received a strong attention by companies.

Whenever we discussed about security of cloud computing, there are various security issues arise in path of cloud. Some of the security concerns and solutions of them are listed and directed below**:**

### 2.1 SECURITY CONCERN 1

With the cloud physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run.
ENSUE: Secure Data Transfer

### 2.2 SECURITY CONCERN 2

Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exists.
ENSUE: Secure Software Interfaces

### 2.3 SECURITY CONCERN 3

Customer may be able to sue cloud service providers if privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.
ENSUE: Data Separation

### 2.4 SECURITY CONCERN 4

Who controls the encryption/decryption keys? Logically it should be the customer.
ENSUE: Secure Stored Data

### 2.5 SECURITY CONCERN 5

In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provide to security mangers and regulators [6], [7], [8].
ENSUE: User Access Control

## III. PROBLEM FORMULATION

There are various policies issues and threats in cloud computing technology which include privacy, segregation, storage, reliability, security, capacity and more. But most important among these to concern is security and how service provider assures it to maintain. Generally cloud computing has several customers such as ordinary users, academia and enterprises who have different motivations to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises most important problem is also security but with different vision. So, we mainly concentrate on USER_CLOUD security of cloud computing using encryption algorithm using particular proposed plan.

## IV. PROPOSED WORK PLAN

We have proposed different security algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits.
Using Net beans IDE 7.3, and Java Run Time Environment, we have implemented our idea in the form of encryption and decryption algorithms which have discussed above and also we have made comparison between them on the basis of their characteristics.

## V. SECURITY ALGORITHM USED IN CLOUD COMPUTING

### 5.1 RSA ALGORITHM

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone.

How RSA is going to work in cloud environment is explained as: RSA algorithm is used to ensure the security of data in cloud computing. In RSA algorithm we have encrypted our data to provide security. The purpose of securing data is that only concerned and authorized users can access it. After encryption data is stored in the cloud. So that when it is required then a request can be placed to cloud provider. 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.

### 5.2 AES ALGORITHM

Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. How AES works in cloud environment? AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, 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 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 approved standard for a wide range of applications.

### 5.3 DES ALGORITHM

The Data Encryption Standard (DES) 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.

### 5.4 BLOWFISH ALGORITHM

Blowfish is a 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:

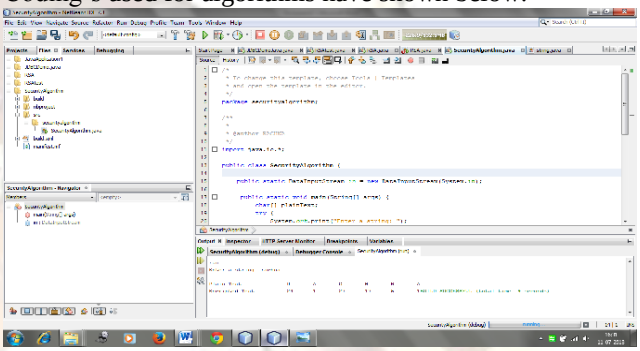
a) Fast- Blowfish encryption rate on 32-bit microprocessors is 26 clock cycles per byte.
b) Compact- Blowfish can execute in less than 5 kb memory.
c) Simple-Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple.
d) Secure- Blowfish 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).

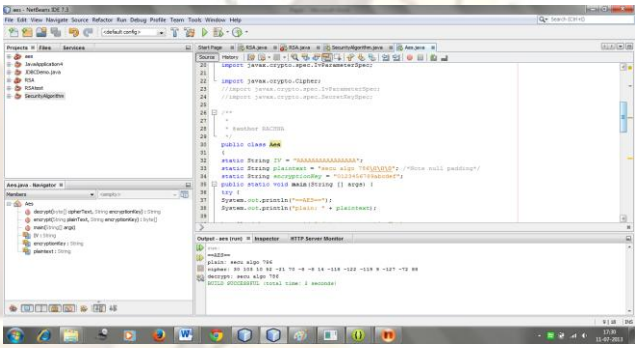
### 5.5 IMPLEMENTATION AND RESULTS

Implementation of algorithms has been done using NetBeans IDE with Java.

Coding's used for algorithms have shown below:



Coding 1 used for making Cloud data secure



Coding 2 used for making Cloud data secure

### 5.6 RESULTS

#### 5.6.1 CHARACTERISTICS AND COMPARISON OF ALGORITHMS

TABLE 1

| Characteristics | AES | RSA | BLOWFISH | DES |
|---|---|---|---|---|
| **Platform** | Cloud Computing | Cloud Computing | Cloud Computing | Cloud Computing |
| **Key Size** | 128,192,256 bits | 1024 bits | 32-448 bits | 56 bits |
| **Key Used** | Same | Public | Same | For |

| | | | | |
|---|---|---|---|---|
| | key is used to encrypt and decrypt the blocks. | key is used for encryption and private key, for decryption | key is used for both encryption and decryption of data. | encryption and decryption same key is used. |
| **Scalability** | Scalable | Not Scalable | Scalable | Scalable |
| **Initial Vector Size** | 128 bits | 1024 bits | 64 bits | 64 bits |
| **Security** | Secure for both provider and user. | Secure for user only | Secure for both providers and user/client side | Security applied to both providers and user |
| **Data Encryption Capacity** | Used for encryption of large amount of data | Used for encryption of small data | Less than AES | Less than AES |
| **Authentication Type** | Best authenticity provider | Robust authentic implementation | Comparable to AES | Less authentic than AES. |
| **Memory Usage** | Low RAM needed | Highest memory usage algorithm | Can execute in less than 5 kb | More than AES |
| **Execution Time** | Faster than others | Requires maximum time | Lesser time to execute | Equals to AES |

## VI. Conclusion and Future Prospects

In this paper encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES, Blowfish and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers.

Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, 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 in IDE tool and JDK 1.7, the desired output for the data on cloud computing has been achieved. In today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, proposed algorithms are helpful for today's requirement. In future several comparisons with different approaches and results to show effectiveness of proposed framework can be provided.

## Acknowledgement

Our Thanks to HCTM, Kaithal for development of this paper.

## References

**Journal Papers:**

[1] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, *International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.*

[2] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), *IEEE Second International Conference 2010, On page(s): 693-702.*

[3] Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. *International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.*

[4] Mohammed, E.M, Ambelkadar, H.S, Enhanced Data Security Model on Cloud Computing, *8th International Conference on IEEE publication 2012, On page(s): cc-12-cc-17*

[5] Sang Ho. Na, Jun-Young Park, Eui- Nam Huh, Personal Cloud Computing Security Framework, *Service Computing Conference (APSSC), Dec 2010 IEEE, On page(s): 671-675.*

[6] Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, *Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.*

[7] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, *January 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.*

[8] Iankoulova, I.; Daneya, M., Cloud computing security requirements: A systematic review, *Research Challenges in Information Science (RCIS), Sixth International Conference on, 2012, On page(s): 1 - 7.*

[9] Cloud Security Alliance, Top Threats to Cloud ComputingV1.0,http://www.cloudsecurityalliance.org/topthreats.

[10] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, Cloud Computing: A Perspective Study, *New Generation Computing-Advances of Distributed Information Processing, Volume 28, Issue 2, April 2010, On page(s): 137-146.*

[11] Puneet Jai Kaur, Sakshi Kaushal, Security Concerns in Cloud Computing, *Communication in Computer and Information Science Volume 169 in 2011, On page(s): 103-112.*

[12] Shui Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, Cloud Computing Research and Development Trend, *Second International Conference on Future Networks (ICFN), IEEE Publications, January 2010, On page(s): 93-97.*

[13] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, *Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference,2010, On page(s): 693-702.*

**Books:**

[14] McGraw Hill, *Cloud Computing, A Practical Approach*, By Toby Velte, Anthony Velte, Robert Elsenpeter.

[15] Furht,B., and Escalante,A. (2010). *Handbook of Cloud Computing. New York: Springer.*

**Chapters in Books:**

[16] Toby Velte, Anthony Velte, and Robert Elsenpeter, *Cloud Computing, A Practical Approach, Chapter 8, Cloud Storage, in 2012, On page(s): 234-253.*

[17] Vamsee Krishna Yarlagadda and Sriram Ramanujam, *Data Security in Cloud Computing, Volume 2 (1) in 2011, On page(s): 15-23.*

**Proceeding Papers:**

[18] W.J. Book, European Network and Information Security Agency (ENISA), 29th IEEE Conference on *Cloud Computing Benefits, Risks and Recommendations*.