Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):15-21
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

USING SECURITY OF ALGORITHMS IN CLOUD COMPUTING AND COMPARE THEM

T.Mshvidobadze
Gori State Teaching University, Gori, Georgia

ABSTRACT : In this paper 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. In general, there are many encryption algorithms that can be used to reduce the real time frauds. These encryption algorithms can be classified into two types. Symmetric encryption algorithms are used earlier for the purpose of providing security such as AES and Blowfish algorithms. In order to provide more security the asymmetric algorithms are used such as RSA algorithm and Elliptic Curve Cryptography (ECC) algorithm. When compared to ECC, RSA algorithms is little slow and uses larger key or message in size. So, now the most efficient ECC algorithm came into the picture in order to provide high security over the existing credit frauds. This proves the efficiency and the less memory usage after the implementation of elliptic curve cryptography.

KEYWORDS: Cloud Computing, Data Security, Symmetric and Asymmetric algorithms, AES, Blowfish, Elliptic Curve Cryptography (ECC).

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 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]. 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 audit ability and public audit ability. Although schemes with private audit ability can achieve higher scheme efficiency, public audit ability allows anyone not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.

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. loud 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.

SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING

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.

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.

RSA ALGORITHM

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. RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption [6]. Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption

$C = P^a \bmod n$

And at decryption side

$P = C^b \bmod n$. *n* is a very large number, created during key generation process[7]. The process is shown in figure 1.

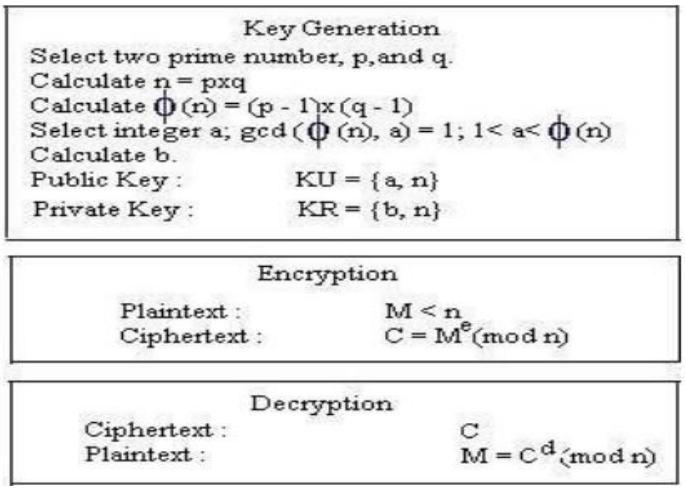


Figure 1. RSA algorithm.

AES ALGORITHM

Advanced Encryption Standard (AES) is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. AES 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[8].

In AES, we have a set of round keys called as derived keys which are applies along with another application which holds one block of data exactly. The steps which are included in the process of performing operations using AES algorithm has involved the following types of operations:

- Sub Bytes
- Shift Rows
- Mix Columns
- XOR Round Key.

BLOWFISH ALGORITHM

Blowfish is a symmetric key cryptographic algorithm. Blowfish encrypts 64 bit blocks with a variable length key of 128-448 bits. Each round consists of a key dependent permutation, and a key- and data-dependent substitution. According to Schneier[9], Blowfish was designed with the followings objectives in mind:

a) Fast- Blowfish encryption rate on 32-bitmicroprocessors 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, but not where the key changes frequently (e.g. Packet Switching).

ELLIPTIC CURVE CRYPTOGRAPHY (ECC):

Elliptic Curve Cryptography (ECC) is a public key cryptography[10]. In Elliptic Curve Cryptography we will be using the curve equation of the form

$$y2 = x3 + ax + b \qquad (1)$$

which is known as Weierstrass equation, where a and b are the constant with

$$4a3 + 27b2 = 0$$

Point addition:

The two point P(1, y1) and Q(x 2, y 2) are distinct. P + Q = R(x 3, y 3) is given by the following calculation.
Figure 1(a) shows graphical representation of Point Addition operation.

$$x\ 3 = \{\lambda 2 - x\ 1 - x\ 2\} \bmod p \qquad (2)$$

$$y3 = \{\lambda(x\ 1 - x\ 3) - y1\} \bmod p \qquad (3)$$

where $$\lambda = \frac{y\ 2 - y\ 1}{x\ 2 - x\ 1} \bmod p$$

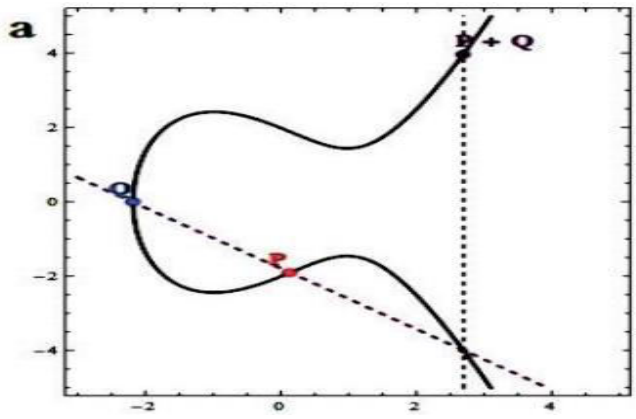
Point Doubling:

The two point P(x 1, y 1) and Q(x 1, y1) overlap. P + Q = R(x 3, y 3) is given by the following calculation.
Figure 1(b) shows graphical representation of Point Doubling operation[11].

$$x\ 3 = \{\lambda 2 - 2\ x\ 1\} \bmod p \qquad (4)$$

$$y3 = \{\lambda(x\ 1 - x\ 3) - y1\} \bmod p \qquad (5)$$

where $$(3\ x\ 21 + a)/\ 2\ y\ 1 \bmod p$$



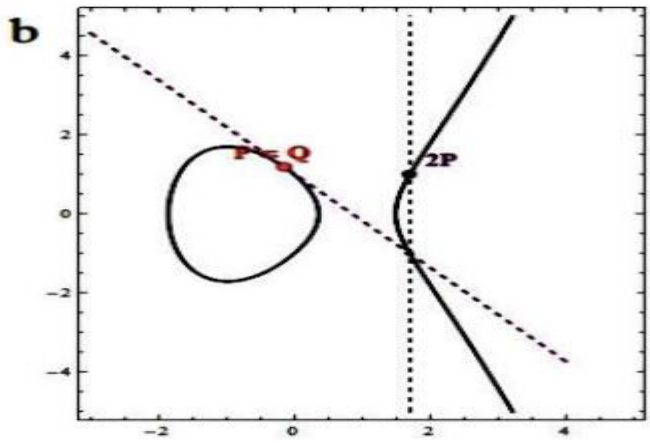


Figure 1.

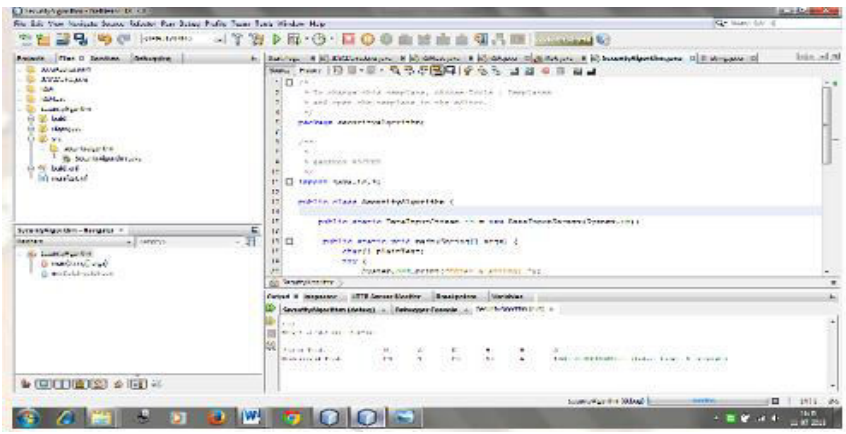
RESULTS:

Comparison between symmetric and asymmetric algorithms such as between AES, RSA and ECC are shown below. This compares the time taken to encrypt using these algorithms. This analysis shows that ECC is comparatively better than AES and RSA.The graph for these values is shown as below:

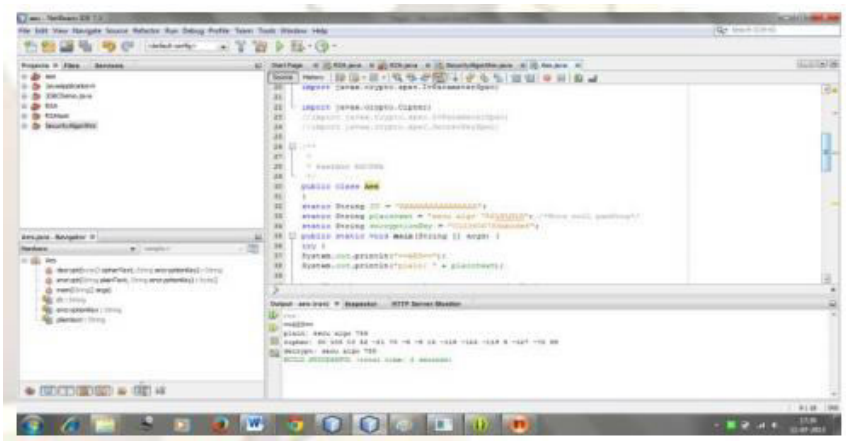
Key size	Time Taken to encrypt in microsec.		
	AES	RSA	ECC
6	100	800	400
25	850	500	250
48	1100	720	300
102	2500	1200	650
128	250	120	70

IMPLEMENTATION AND RESULTS

Implementation of algorithms AES, RSA, BLOWFISH has been done using NetBeans IDE with Java[12]. Coding's used for algorithms have shown below:



Coding 1 used for making Cloud data secure



Coding 2 used for making Cloud data secure

RESULTS
CHARACTERISTICS AND COMPARISON OF ALGORITHMS

Characteristics	AES	RSA	BLOWFISH
Platform	Cloud Computing	Cloud Computing	Cloud Computing
Key Size	128,19 2,256 bits	1024 bits	32-448 bits
Key Used	Same key is used to encrypt and decrypt the blocks	Public key is used for encryption and private key, for decryption	Same key is used for both encryption and decryption of data.
Initial Vector Size	128 bits	1024 bits	64 bits
Security	Secure for both provider and user.	Secure for user only	Secure for both providers and user/client side
Data Encryption Capacity	Used for encryption of large amount of data	Used for encryption of small data	Less than AES
Memory Usage	Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 kb

Table 1.

CONCLUSION

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, 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.

When compared to symmetric algorithms such as AES and Blow fish, asymmetric algorithms such as RSA and ECC are secure as they maintain two keys where one is secret and the oter is shared. They can be used for authentication, confidentiality, key exchange. ECC is better than RSA as this provides equal security at smaller key length. This can be implemented in any applications that requires security such as Image Encryption, banking applications, online exchanges, e-ommerce.

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. 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.

REFERENCES

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. 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.
4.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.
5. 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.
6. Akhil Behl “Emerging Security Challenges in Cloud Computing ”, IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222
7 .Leena Khanna, Prof. Anant Jaiswal “Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them”, International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp. 279-283.
8. Text Book: “Cryptography and network security, Principles and practices”, by William Stalling,
Retrieved on 8 December 2006.
9. Bruce Schneier, "The Blowfish encryption algorithm", Dr. Dobb's Journal of Software Tools,
19(4), p. 38, 40, 98, 99, April 1994 .
10. Neal Koblitz, “Elliptic Curve Cryptosystems”, Mathematics of Computation, Vol 48. Number 177, Jan I987. pp 203-209
11. Victor S. Miller, “Use of Elliptic Curves in Cryptography”, LNCS, Advances in Cryptology —
CRYPTO ’85 Proceeding, Sec V, pp 417-426, 1986, Springer Berlin Heidelberg.
12. Xinmiao Zhang ; Parhi, K.K., “Implementation approaches for the Advanced Encryption Standard algorithm”, Circuits and Systems Magazine, IEEE , Vol 2,Issue: 4 , pp 24