Securing Cloud Data using Cryptography with Alert System

M. Ilaiyaraja
Dept. of CSE
Bharathidasan Institute of Technology
Anna University, Triuchirappalli
Tiruchirappalli
Tamilnadu

P. BalaMurugan
Dept. of CSE
Bharathidasan Institute of Technology
Anna University, Triuchirappalli
Tiruchirappalli
Tamilnadu

R. Jayamala
AP, Dept. of CSE
Bharathidasan Institute of Technology
Anna University, Triuchirappalli
Tiruchirappalli
Tamilnadu

***Abstract*—Cloud computing allows the user to rent the software and storage instead of acquiring with high amount. It provides many benefits in terms of low cost and accessibility of data. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, efficiency and authentication problems are encountered. Data Security, confidentiality and Authentication are the major problems in cloud computing. This paper analyzes the security vulnerabilities of most popular cryptography algorithms such as AES, DES, Triple DES, Blowfish and Hashing algorithms like MD2, MD5, SHA-1, and SHA-2. This paper proposed security architecture going to use Hybrid encryption (Blowfish + RC6) technique and Digital signature to avoid security vulnerabilities without degrading their efficiency. This system also provides an efficient alert system to identify the intruders.**

Keywords— AES, DES, Triple DES, Blowfish, MD2, MD5, SHA-1,SHA-2, Hybrid encryption, Alert System.

I. INTRODUCTION

Cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability [1]. Cloud computing is a technology that uses pay per use concept [2]. It allows consumers and business to use applications without installation and access their personal files at any computer with high speed internet access, it reduce the cost of hardware at the user end. As there is no need to store data at user's end because it can be stored at some other location. So instead of buying the whole infrastructure required to run the processes and save bulk of data at the user's end, the users are just renting the services according to their requirement. The similar idea is behind all cloud networks [3]. Cloud providers maintain the services for the cloud user at the centralized remote server and provide independence of accessing them from any place through a network [3].

A. Cloud computing provides different service models:

- **I**nfrastructure **a**s **a** **S**ervice (IaaS), which provides computing resources to the customers from their large resource pools installed in data centers.
  Ex: Amazon.
- **P**latform **a**s **a** **S**ervice (PaaS), which provides a virtual platform to the cloud customers to run their applications.
  Ex: Google App Engine.
- **S**oftware **a**s **a** **S**ervice (SaaS), which provides applications on the cloud computing platform.
  Ex: Google Pack, Facebook.

B. Deployment model in cloud computing:

- Public cloud also known as External cloud, which allows all the users to access the cloud data.
- Private cloud also known as internal cloud, which provides services only for very restricted set of users.
- Hybrid cloud is a combination of both public cloud and private cloud, which is a private cloud linked to one or more public cloud services, centrally managed by a secure network. It has multiple service providers.

In the scenario of storing and consuming the data's in the cloud, this data needs to be travel in the network. So there may be a chance to the intruder to view and modify the data. To prevent this illegal access the system should implement efficient security architecture. This proposed system analyze the various cryptography algorithm such as AES, DES, Triple DES, Blowfish, Hybrid encryption, Hashing algorithm such as MD2, MD5, SHA-1, SHA-2 and suggests a best security architecture for securing the cloud data. Also this security architecture includes an Alert System to find out intruders. The rest of the paper arranged as follows, Section II states Security vulnerabilities, Section III performance analysis, Section IV Security Alert system, Section V Proposed Architecture and Results, Section VI Conclusion and Future Work.

II. SECURITY VULNERABILITIES

This section includes introduction about various cryptography algorithms with their security vulnerabilities. The most popular cryptography encryption techniques are taken for this research and their possible attacks are listed with some other demerits

A. Cryptography Algorithms

a) AES Algorithm: AES is the Advanced Encryption Standard, Symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits or 192 bits or 256 bits called AES-128, AES-192 and AES-256 respectively [4]. AES-128 uses 10 rounds, AES-192 uses 12 rounds and 256 uses 14 round [5].

Attacks:

The most successful attack on AES is the "Square Attack". The square attack is faster than the Brute force Attack for AES using six rounds or less. For seven rounds or more [6] Brute force attacks are the faster known attacks. Key recovery attack is based on bicliques and is faster than Brute force by a factor of about four. It requires $2^{126.1}$ operations [7] to recover an AES-128 $2^{189.7}$ and $2^{254.4}$ operations are needed to recover an AES-192 and AES-256 respectively. Related key attacks, Distinguishing attacks are other known attacks.

b) DES Algorithm: DES is the Data encryption standard, Symmetric block cipher with block size of 64 bits. Key length can be 56 bits with 16 rounds [8].

Attacks:

The most practical attack to date is Brute force approach due to its very less key length. In Brute force the length of the key determines the number of possible keys [8]. In January, 1999, distributed.net and Electronic frontier foundation collaborated to publicly break a DES key in 22 hours and 15 minutes [8]. Differential cryptanalysis, Linear cryptanalysis, Davies' attack are three known theoretical attacks to break a full 16 rounds of DES.

c) Triple DES Algorithm: Triple Data Encryption Algorithm symmetric key block cipher with block size of 64 bits [9]. Key length can be 56 bits or 112 bits or 168 bits with 48 DES-equivalent rounds.

Attacks:

Two-key triple-DES can be broken with the meet-in-the-middle attack requiring 2^{56} chosen plain text, 2^{56} memory and 2^{56} single DES encryption [9]. Related key slide attack, Differential attack are other known attacks.

d) Blowfish Algorithm: Blowfish is the symmetric key block cipher with block size of 64 bits. Key lengths can be varies from 32 bits to 448 bits [10]. It uses 16 rounds for encryption. It follows random key selection mechanism [10].

Attacks:

Reflection attack is made on weak keys so it is needed to select strong keys [10]. Brute force attack is also possible for less key length.

e) RC6 Algorithm: Rivest cipher 6 is symmetric key block cipher with block size of 128 bits [11]. Key size can be 128 bits or 192 bits or 256 bits with 20 rounds for encryption [11].

Attacks:

Brute force attack, Linear and differential attack. Differential cryptanalysis is a chosen plain text attack on iterative block ciphers [11].

B. *Digital Signature Algorithms*

a) MD2 Algorithm: MD2 message Digest Algorithm is a cryptographic hash function is optimized for 8-bit computers [12]. Its Digest size is 128 bits with 18 rounds.

Attacks:

Preimage attack, Collision attack, Birthday attack, Pseudo Collision attack. Preimage attack [12]has two parts, first part finds many pre images of the compression functions and the second part finds those preimages which conforms with the checksum function.

b) MD5 Algorithm: MD5 Message Digest Algorithm is widely used cryptography hash function producing 128 bit hash value [13]. Its message digest size is 128 bits with 4 rounds.

Attacks:

It also has the Collision and Preimage vulnerability. The collision attack can be performed less than a second on a regular computer [13]. It is not collision resistance so it is not suitable for applications like SSL certificate and Digital signatures.

c) SHA-1 Algorithm: SHA-1 is a cryptographic hash function which producing 160 bits hash value, its message digest size is 160 bits with 80 rounds [14].

Attacks:

SHA-1 algorithm has some theoretical attacks so it may not be secured. Mathematical weakness exists in SHA-1technique [14].

d) SHA-2 Algorithm: SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) [15]. Secured Hashing Algorithm-2 digests size are 224 bits or 256 bits or 384 bits or 512 bits. It has 64 rounds or 80 rounds.SHA-256 and SHA-512 are novel hash functions computed with 32 and 64 bits respectively [15].

Attacks:

This also has preimage attack and collision attack but it is not successfully extended [15].

III. PERFORMANCE ANALYSIS

A. *Output results for Encryption algorithms*

In this study five different cryptography algorithms and four hashing algorithms are chosen. This performance measure of both cryptography and hashing algorithms are based on their encryption speed. For this research various file size such as 10 kb, 20 kb, 50 kb, 100 kb and 500 kb are taken. The evaluations are made on net beans under jdk1.7.0_25 with windows 8 platform.

TABLE I.

Comparative execution times (in milliseconds) for encryption Algorithms with various file size

File Size(in KB)	DES	AES	Triple DES	Blowfish	Hybrid
10	6	76	23	26	20
20	9	119	25	29	24
50	12	264	29	35	31
100	16	622	37	41	39
500	61	7835	108	71	75
Average Time	20.8	1783.2	44.4	40.4	37.8
Throughput(Mb/sec)	6.5	0.07	3.06	3.36	3.59

From the evaluation results it was concluded that, DES is faster and higher throughput than other encryption algorithm. In the other hand, blow fish and hybrid algorithms shows better performance than AES and Triple DES. When comparing blowfish and hybrid, blowfish takes less encryption time but it gives fewer throughputs than hybrid algorithm.

B. Output results for Hashing algorithms

From the study of hashing algorithm it is concluded that, SHA-1 is much faster than other hashing algorithms. SHA-256 gives better performance than other hashing algorithms except SHA-1, MD 2 produces poor results than all other hashing algorithms.

TABLE II
Comparative execution times (in milliseconds) for hashing algorithms with various file size

File Size(in KB)	MD 2	MD 5	SHA-1	SHA-256	SHA-384	SHA-512
10	25	18	17	18	18	19
20	21	19	18	20	19	20
50	30	23	23	22	22	22
100	39	30	23	24	25	26
500	128	35	29	33	48	48
Average Time	48.6	25	22	23.4	26.4	27
Throughput(Mb/sec)	2.79	5.44	6.18	5.81	5.15	5.03

Also average time taking for MD 2 is very high than others, average time taking for SHA-1 and SHA-256 is comparatively less than other hashing algorithms. So that SHA-1 and SHA-256 shows better performance and higher throughput.

IV. SECURITY ALERT SYSTEM

Even though very strong cryptography algorithms available, some unavoidable threats like Brute force attacks are also exist. To protect from these threats some stronger security alert system is needed. This proposed system includes an effective security alert system to protect from these attacks and find out the intruders. This system produces an alert to the cloud service provider and the Data Owner when the intruder tries to decrypt the cloud data with different key values. Content of the alert message contains the information about the intruder with their system configuration.

V. ARCHITECTURE AND RESULTS

From the above study, DES gives better throughput than other encryption algorithms but it is very less secured since it has fewer key lengths (56 bits). At the same time blowfish and hybrid algorithm gives better throughput. But Blowfish algorithm doesn't follow any key construction rules to construct its secret key. So it is easy to find the secret key by brute forcing. On the other hand, the proposed hybrid algorithm encompasses two different cryptography algorithms (Blowfish + RC 6). It also uses two different key values for each encryption process. So it is very hard to find the secret key and cryptanalysis with mathematical functions. From the study of hashing algorithms, SHA-1 and SHA-256 gives better results, but SHA-1 has numerous security vulnerabilities than the SHA-256.

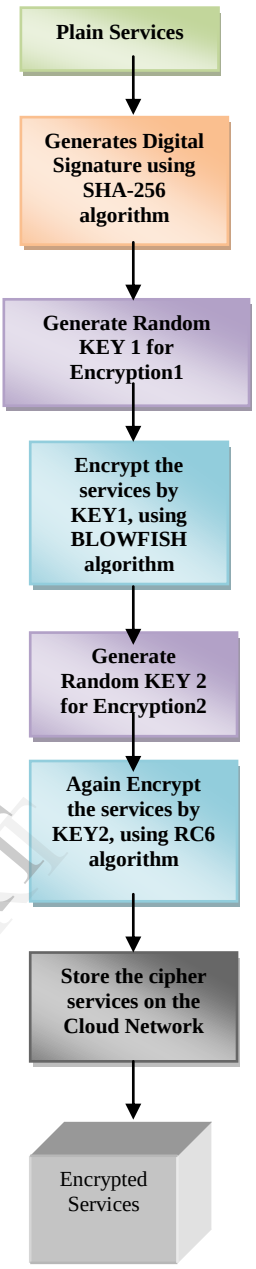

Fig: 1

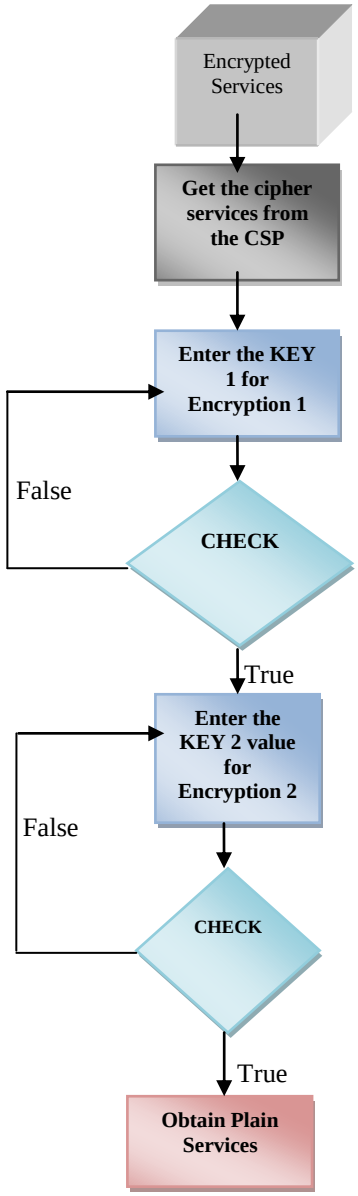

Fig: 2

Fig 1 shows the actions involved in Data Owner side. This encryption process consists of two blocks; the first block takes the original data as input and generates a digital signature. The generated digital signature added to the plain text and encrypted by Blowfish algorithm using key 1. The output of the first block is taken as input to the second block and encrypted by RC6 algorithm using key 2.

Fig 2 shows the actions involved in Cloud user side. Cloud user will get the encrypted services from the cloud service provider, for decrypting the service the cloud user should enter their key 1 value for decryption 1, if the key value is valid then the system asks the user to enter the key 2 value for decryption 2, if it is invalid the system allow the user to reenter the key value 1 again. If the user enters invalid key value more than the threshold value (here threshold value is 3), the security alert system will sends an alert message to the Data owner.

VI. COCNCLUSION AND FUTURE WORK

This paper presents a performance evaluation of selected symmetric encryption algorithms and hashing algorithms. The selected algorithms are DES, AES, Triple DES, Blowfish, Hybrid, MD 2, MD 5, SHA-1 and SHA-2. It was concluded that Hybrid algorithm has better performance than other common encryption algorithms. Even though AES provides better security, it will take more time for encryption process. On the other side, SHA-256 is efficient than other hashing techniques. From the above research it is recommended to use Hybrid algorithm for encryption and SHA-256 for Digital signature and also better to use an Alert system to avoid Brute force attack. In future the work may be extended in the sense of avoiding DOS attack.

REFERENCES

1. Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing, 2010.
2. Ashtosh Kumar Dubay, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", 2011.
3. Mandeep Kaur, Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", 2013.
4. A.G.Nadaph, Amol Dashwant,Dipali Bhivare, Shrikrisn Badade, Pratik Jadhav, "Secure Paper Distribution On Cloud Using Re-encryption",2014.
5. Tugpa Altunalan, Eren Timur, "Data Encryption Standard-Advanced Encryption Standard", 2013.
6. M.Kulkarni,A.S.Bhide,P.Choudhari, "Encryption Algorithm Addressing CSM Security Issues- A Review", 2013.
7. http://csrc.nist.gov/CryptoToolkit/aes/Rijndael.pdf
8. http://en.wikipedia.org/wiki/Data_Encryption_Standard
9. http://en.wikipedia.org/wiki/Triple_DES
10. http://en.wikipedia.org/wiki/Blowfish_(cipher)
11. http://en.wikipedia.org/wiki/RC6
12. http://en.wikipedia.org/wiki/MD2_(cryptography)
13. http://en.wikipedia.org/wiki/MD5
14. http://en.wikipedia.org/wiki/SHA-1
15. http://en.wikipedia.org/wiki/SHA-2
16. Jian Zhang, Xuling Jin, "Encryption System Design Based On DES and SHA-1", 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science", 2012.
17. Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan, "Secure Data Access in Cloud Computing", 2010.
18. Jyun-Yao-Huang, I-En Liao, Chen-Kang Chiang , "Efficient Identity-Based key Management for Configurable Hierarchical Cloud Computing Environment", 2011.
19. http://security.stackexchange.com/questions/16723/how-long-does-it-take-to-brute-force-varying-encryption-standards