Optimization of Cryptography Algorithms in Cloud Computing

Pooja Bindlish
Assistant Professor in CSE Dept. I.G(PG)M.M.V College, Kaithal
Kaithal (Haryana), India

Abstract
Now a day, Security is becoming a main concern to maintain confidentiality and integrity of the data. For this purpose, cryptography techniques are used. Cryptography is used to encrypt the data into non-readable format and decrypt it again into readable format when needed using specific key. Also for business perspective, cloud computing is very useful. Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. It has different meaning to different uses according to their need. According to a business man, it is used to store and access the data to fulfill the memory requirement and consistency. Also secure data transmission feature of cloud computing plays a very important role in business perspective. For using cloud computing, business man has to pay specific amount of money to the cloud service provider. Cloud service provider guaranty either the confidentiality or integrity of the data. This paper proposes and implements the idea of sending already encrypted file through cloud in spite of the original file using RSA and DES algorithm of cryptography. As encrypted file is transmitted, so original file is not available even at the network. So even if any intermediate user sees the data, he will not be able to understand the data. That's why confidentiality and integrity is maintained by this. Hence security of cloud data will be increased. This work can be enhanced using hybrid approach by integrating multiple cryptography algorithms.

Keyword:
Cloud Computing, Cryptography, RSA, DES, Security.

I. Introduction:

As cloud is used to collect the water and rain occurs when cloud collides with any solid thing like that cloud computing is used to store and access data over the internet instead of one's computer hard drive. Cloud computing is gaining momentum because it is highly distributive technology. It has inherited the legacy technology and adding new ideas[1].It provides customers the illusion of infinite computing resources which are available from anywhere, anytime, on demand[2].Computing at such an large scale requires a framework that can support extremely large datasets housed on clusters of commodity hardware. The U.S. National Institute of Standards and Technology (NIST) have put an effort in defining cloud computing, and as NIST‟s publications are generally accepted, their definition of cloud computing will be used in this thesis. The NIST definition of cloud computing is:
"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
It is taken from Greek language which means "hidden or secret". Cryptography techniques like RSA and DES are used to encrypt the data and then encrypted data is send rather than original data. Cryptography is used for constructing and analyzing protocols.

Key Basics:
Key basics of cryptography are that it requires only two components. They are:

1) Algorithm:
Steps for doing encryption and decryption

2) Key:
Any value that is used for encryption/decryption. For example like key of every vehicle is different to insure that no other key can be used to run that vehicle.

Types of Cryptography:
There are two types of cryptography techniques.
1) Symmetric-Key Cryptography
2) Asymmetric-Key Cryptography

1) Symmetric-Key Cryptography:
In a symmetric cryptosystem, the same key is used for encryption and decryption.

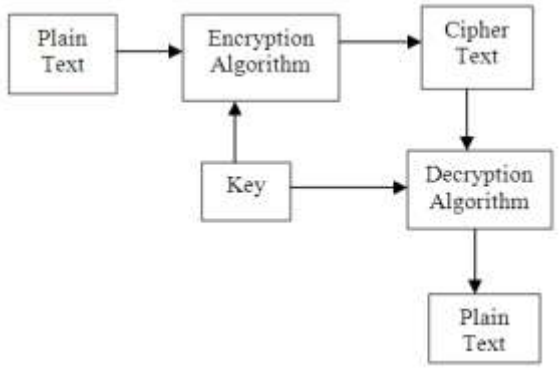

Figure1: Symmetric key Cryptography

DES is symmetric technique. The Data Encryption Standard (DES) was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). DES, as specified in FIPS Publication 46-3, is a block cipher operating on 64-bit data blocks.

2) Asymmetric-Key Cryptography:
In an asymmetric, the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair.

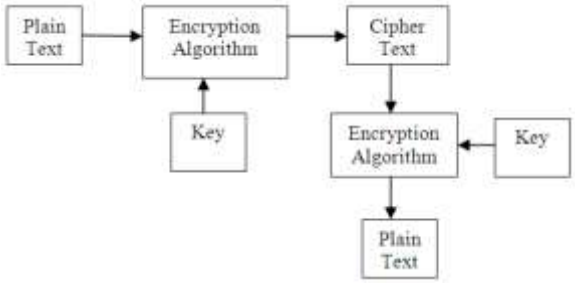

Figure2: Asymmetric key Cryptography

RSA is asymmetric technique. Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA cryptosystem of MIT in 1997.It was described in 1978.It is neither stream cipher nor block cipher.

II. Literature Review:

Dr. Smith Jones [3], proposes and implement a new algorithmic approach for cloud security using key based cryptography. He uses the MD5 SHA-1 cryptography technique to increase the security of cloud.

R.Rivest, A.Shamir and L.Adleman[7] worked on a methodology for digital signatures and RSA cryptosystems. In this research paper which is used RSA cryptosystem for digital signature.It is also increased the efficiency and security.

Ravi shanka dhakar[8] proposes security of RSA cryptosystem depend on the large prime numbers because it is difficult to break the large prime numbers.RSA algorithm provides the security and performance. Every element of the set is greater than all integer numbers .In this paper a RSA algorithm which is provided security against brute force attacks.

Joshi Ashay Mukundrao[18] worked on Cloud computing which is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data security. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two salient features,opposing to its predecessors. Avoiding unauthorized access to user's data by signaling user by sending message to his/her mobile number at the start of transaction. Displaying fake information in case of unsuccessful login for avoiding further login trials by intrusion (Honeypot).

III. Research Methodology and Problem Formulation:

The methodology to be adopted to achieve the objectives would be firstly to select simulation tool. Following this would Implementation Of various Algorithms. After that the validation and analysis will be done. This can be summarized as follows:

1) Selection of simulation tools.
2) Implementation Of various Algorithms
3) Results and analysis.

Problem Definition:
Now a day, Cloud computing has gaining lots of attention. So security in cloud computing is of main concern because of the following reasons:

1) Managing:
The storage, processing and accessing of sensitive data is all done through remote machines (CSP) that are not owned or even managed by data owner themselves.

2) Access of Data:
As there is storage and accessing of data from cloud servers, the concerns about data confidentiality, authentication and integrity are being increased. So, there is also chance of using a part of data or whole by cloud server for their financial gain which results the economic losses to data owner.

3) Third Party:
The main reason behind the above defined issues is that the cloud servers are very likely to be the outside from trusted boundaries of data owner.

4) Unwanted Exposure:
One of the related issues is also the unwanted exposure of data as result of a software malfunction or malicious CSP. When entrusting data to the cloud the data creators i.e. service users need assurances over access to their data. In essence data creators need to regain control over this access i.e. data creators need to become empowered.

Directions for proposed solution:
As privacy of user data is of main concern so that mainly three attributes of security can be attained. They are:
1) Authentication
2) Confidentiality
3) Integrity
Data privacy in cloud can be maintained by using three existing solutions: None of Your Business (NOYB) ; Privacy Manager ; and Content Cloaking (CoClo) . Each of these three solutions each have a different take on how to protect the privacy of data.

1) Encryption:
The CoClo solution dictated that data should be encrypted prior to its insertion into the cloud so that original data would be completely from unauthorized users and even to the CSP.
2) Obfuscation:
With Privacy Manager data was obfuscated. While `obfuscation' does unnecessarily imply the encryption of data, obfuscated data can still nonetheless be operated upon by a CSP with the CSP not learning anything about the underlying data.

3) Contextual Integrity.
The NOYB solution being searched to destroy the link between the data and its creator, as well as hide the data itself.

IV. Proposed Work:

Data privacy in cloud computing is of main concern. In this paper, CoClo solution is used by using encryption of data prior to sending it into cloud. RSA and DES is used for this purpose. It includes following steps:

1) Preparation of Data
2) Encryption
3) Transfer
4) Processing

1) Preparation of Data:
Firstly, the data need to be prepared for encryption process. Data processed by implemented algorithm, can be in file form. File can be of any three type: .txt,.java,.m . In other words data should be in text form not any picture.
2) Encryption:
After preparing the data, file that need to be transfer can be encrypted using any of two algorithms i.e. RSA or DES. Now encrypted file is obtained which is binary format.
3) Transfer:
Disclosure of sensitive data during transfer from one party to the other is a concern that has been addressed quite extensively with the use of encryption. Now encrypted file is transfer or store on cloud. So, even the network has not the copy of original file. Because of this authentication, confidentiality and integrity is maintained. Data privacy of cloud computing is also achieved.
4) Processing:
Processing refers to any use or transformation of Data. There is ongoing research on the possibility of processing data in encrypted form, which is called homomorphic encryption. Homomorphic encryption enables data owners to have their encrypted data processed by another entity, while preventing the processing party to find out what the data is in unencrypted form. This theory is very interesting for the cloud computing paradigm, but the researcher Craig Gentry admits that it may take up to 40 years before the theory becomes practical.

V. Implementation Results:

Any file that is needed to transfer/store on cloud is selected and encrypted using any of the two techniques i.e. RSA or DES. These algorithms are studied and compared with each other on the behalf of the encryption and decryption time. There are following types of times in aspect of cryptography algorithm:

1) Encryption Time:
Time taken by a program to encrypt the data i.e. to convert plain text into cipher text which is not understandable to attacker .

2) Decryption Time:
Time taken by a program to decrypt the data i.e. to convert cipher text into plain text.
3) Total Time in Execution:

Time taken to encrypt and decrypt the data.

Execution Time = Encryption + Decryption Time

The results obtained are as followed:

RSA Result:
The table formed and corresponding graph is as shown below:

Table 1 : RSA Encryption and Decryption time.

File Type	File Size (in Kb)	Public Key	Private Key	Random Number	Encryption Time (in sec.)	Decryption Time (in sec.)	Total Execution Time(in sec.)
.txt	1	2743	19207	29747	0.047	0.062	0.109
.txt	5	23453	14717	29987	2.652	0.14	2.792
.txt	12	13265	15521	24047	10.296	0.141	10.437
.txt	24	9791	2195	37001	35.787	0.234	36.021
.m	2	22643	14507	38191	0.515	0.047	0.562
.m	5	46837	35773	60491	2.855	0.078	2.933
.java	3	20951	25511	29737	1.466	0.063	1.529
.java	8	13309	33877	38021	5.444	0.093	5.537
.java	15	27833	14113	32899	15.163	0.172	15.335
.java	54	17039	4859	40301	151.742	0.39	152.132

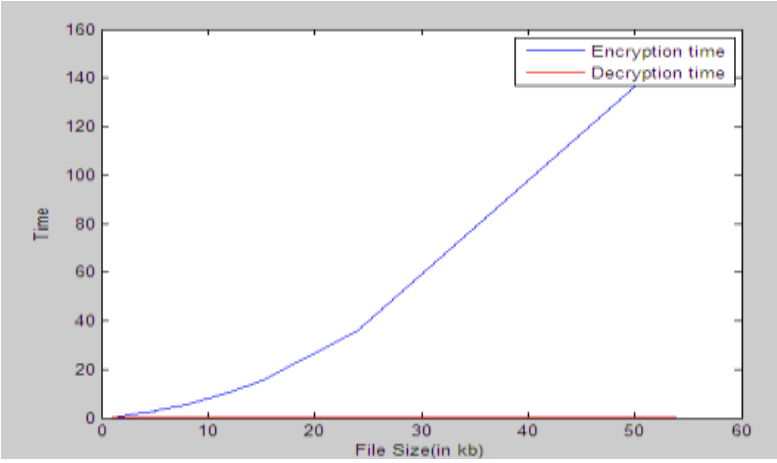

Figure 3: Graph of RSA

DES Results:
The table formed and corresponding graph is as shown below:

Table 2: DES Encryption and Decryption time.

File Type	File Size (in Kb)	Encryption Time (in sec.)	Decryption Time (in sec.)	Total execution Time(in sec.)
txt	1	0.265	0.062	0.327
.txt	5	0.281	0.14	0.421
.txt	12	0.281	0.218	0.499
.txt	24	0.281	0.344	0.625
.m	2	0.265	0.11	0.375
.m	5	0.265	0.219	0.484
.java	3	0.265	0.125	0.39
.java	8	0.266	0.187	0.453
.java	15	0.266	0.327	0.593
.java	54	0.281	0.733	1.014

It can be seen from the table that encryption and decryption time even for the large file is in microseconds. This table is analyzed using the following graph:

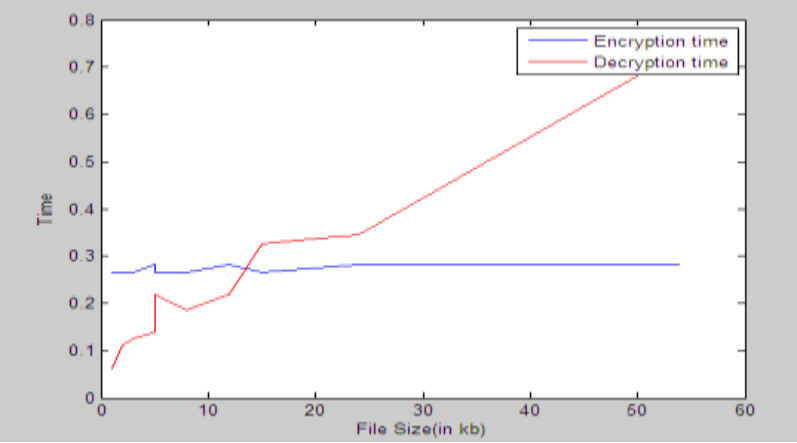

Figure 4: Graph of DES

Comparison of RSA and DES:

Now the comparative study of RSA and DES is done with the help of data obtained. The comparative analysis table and graph is as shown below:

Table 3: Comparative analysis table of RSA and DES

File Type	File Size (in Kb)	RSA (Total execution Time)	DES (Total Execution Time)
.txt	1	0.109	0.327
.txt	5	2.792	0.421
.txt	12	10.437	0.499
.txt	24	36.021	0.625
.m	2	0.562	0.375
.m	5	2.933	0.484
.java	3	1.529	0.39
.java	8	5.537	0.453
.java	15	15.335	0.593
.java	54	152.132	1.014

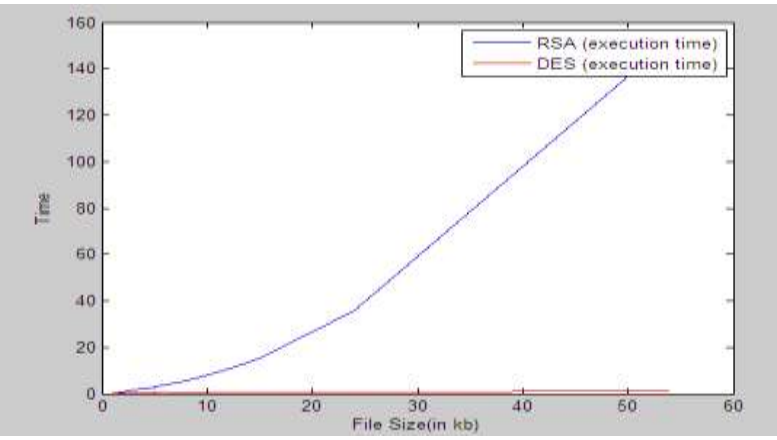

Figure 5: RSA and DES Comparative analysis

VI Conclusion and Future scope:

It can be concluded that DES is much faster than RSA if time is of main concern. But from security point of view, RSA is better than DES.The cryptographic techniques are essential, but not the only one, method to protect private data against partially trustworthy cloud server. Therefore, future work of this research might include:

- Hybrid approach of various cryptographic algorithms can be used.
- The results fetched from RSA and DES can be used in integration.

REFERENCES

[1] Bhaskar Parsad Rimal et al.,"A Taxonomy and Survey of Cloud Computing System",2009 fifth international joint conference on INC,IMS and IDC.

[2] AMIT GOYAL and SARA DADIZADEH," A Survey on Cloud Computing"

[3] Dr.Smith Jones." AN EMPIRICAL CRYPTOGRAPHY ALGORITHM FOR CLOUD SECURITY BASED ON HASH ENCRYPTION", International Journal of Computing and Corporate Research ISSN (Online) : 2249-054X Volume 4 Issue 4 July 2014 International Manuscript ID : 2249054XV4I4072014-43

[4] Borko Furth, Flordia Atlantic, "Cloud computing fundamentals", springer Ist edition, 2010, ISBN 978-1-44 19-6523-3.

[5] Brian Hayes. `Cloud computing'. In: Commun. ACM 51.7 (2008), pp. 9-11. issn: 0001-0782. doi: http://doi.acm.org/10.1145/1364782.1364786.

[6] Charlie Kaufman and Ramanathan Venkatapathy, "Windows Azure™ Security Overview", http://www.windowsazure.com/enus/develop/overview/

[7] A method for obtaining digital signatures and public key cryptosystems, R.Rivest, A.Shamir and L.Adleman "communication of the association for computing machinery " 1978, pp 120-126.

[8] RSA algorithm using modified subset sum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011.

[9] Alok Tripathi, Abhinav Mishra, "cloud computing security consideration", 2011 IEEE International Conference on signal processing, communication and computing, 27 October2011, pp. 1-5.

[10] Joshi Ashay Mukundrao," Enhancing Security in Cloud Computing" Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011.

[11] http://en.wikipedia.org/wiki/Cloud_computing.

[12] Atul Khate,Cryptography and network security,second edition.

[13] CRS BHARDWAJ Modibada, Jabalpur (Mp), India," Modification Of Des Algorithm", IJIRD, Vol 1 Issue 9, November, 2012, , pg.495 – 505.

[14] Cong Wang, Qian Wang, and Kui Ren,Wenjing Lou," Ensuring Data Storage Security in Cloud Computing".

[15] Overview of Cryptography by Alfred J. Menezes

[16] Shraddha Dadhich "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java" in international Journal of Computer Trends and Technology in vol.35 no. 4 in year 2016