Ensuring security on mobile device data with two phase RSA algorithm over cloud storage

Padmavathi Ganapathi
Avinashilingam University

ENSURING SECURITY ON MOBILE DEVICE DATA WITH TWO PHASE RSA ALGORITHM OVER CLOUD STORAGE

[1]SUJITHRA. M, [2]PADMAVATHI. G

[1] Research Scholar, Department Of Computer Science, Avinashilingam Institute For Home Science And Higher Education For Women, Coimbatore, India.

[2] Professor & Head, Department Of Computer Science, Avinashilingam Institute For Home Science And Higher Education For Women, Coimbatore, India.

Email: [1]sujisrinithi@gmail.com

ABSTRACT

Mobile devices are rapidly becoming a key computing platform and an essential part of human life as the most effective and convenient communication tools not bounded by time and place. With the rapid growth of mobile devices and mobile applications, the need for mobile security also has increased dramatically. Due to increasing use of mobile devices the requirement of cloud computing in mobile devices arises, which gave birth to Mobile Cloud Computing. Mobile Cloud Computing refers to an infrastructure where data storage can happen away from mobile device i.e. on a cloud. To ensure the correctness of users' data in the cloud, the framework mainly focuses on the data security over the Cloud Computing Paradigm by purposing new cryptographic technique named as Two Phase RSA Encryption. The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed and compared them to choose the best data encryption algorithm so that it can implement in future work.

Keywords: *Encryption, Decryption, Mobile Device, Cloud Storage, Data Storage*

1. INTRODUCTION

Now a day a mobile device is becoming one of the important data processing devices for mobile users. Portio research estimates that mobile subscribers worldwide will reach 6.9 billion by the end of 2013 and 8 billion by the end of 2016 [1] Ericsson also forecasts that mobile subscriptions will reach 9 billion by 2017. Mobile device is still resource constrained and some applications generally need more resources than a mobile device can pay for. To overcome this problem, a mobile device ought to get resources from an external source known as Cloud Storage. It is not always possible to save all the data and the information on the mobile device itself. So that the mobile agents can utilize the resources from the cloud, it requires the migrations of data and information between the cloud and mobile devices. It consists of front-end users who possess mobile devices and back end cloud servers [2]. Here we have proposed an encryption scheme for protecting the confidentiality and integrity of mobile data while uploading and downloading files to and from cloud respectively. Uploading is the transfer of data from the mobile device to a Cloud Storage, whereas downloading is the transfer of data from the cloud storage to mobile device.

Cryptography is an art of hiding information by encrypting the message. Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) key encryption. In Symmetric key encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys plays an important role [3]. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of the key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. The Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). which is known to the public and private key which is known only to the user.

2. RELATED TERMS OF CRYPTOGRAPHY

- **Plain Text*:*** The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how is you" is a plain text message.

- **Cipher Text:** The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message.Forexample,"Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how is you".

- **Encryption:** A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

- **Decryption:** A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message. The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

- **Key:** A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the

Because users tend to use two keys: public key,

security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "country" then Cipher Text produced will be "Agheuhv"[5].

3. CRYPTOGRAPHY

It is a technique used to avoid unauthorized access of data. The encryption process consists of single or multiple keys to hide the data from the intruders. The original text before the encryption process is known as *Plaintext***.** The text obtain after encoding the data with the help of a key is known as *cipher text*. The encryption process has the power to change/upgrade the key at any time and information of changed or upgraded key has been made known to both the parties. The encryption-decryption process is given in figure.1.

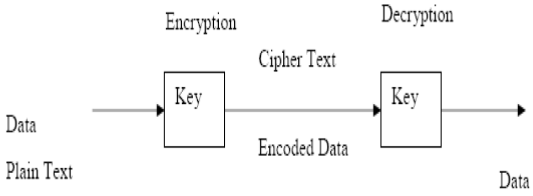


Figure 1: Encryption-Decryption process

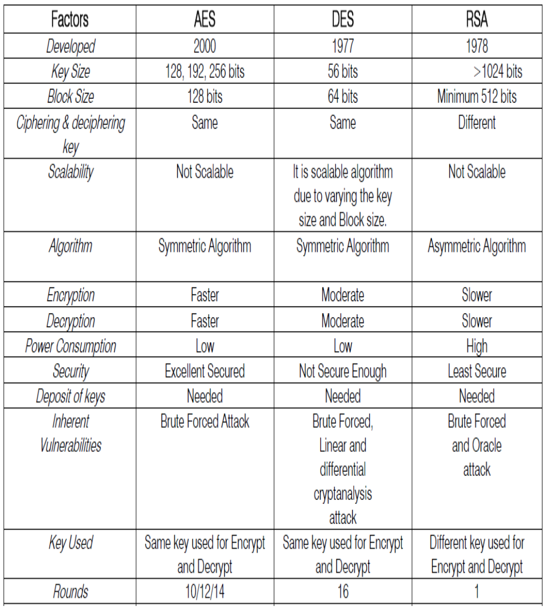
Computers are normally interconnected with each other and are exposed to the other networks and the communication channels therefore encryption is required to keep the data confidential from each other. Secured data communication is also an essential parameter for all the industries/ governments. There is a need of secured data transmission in defence, industries, universities, etc. The basic terminologies used are:

- **Plain text:**
  Original message has to be transferred.
- **Cipher text:**
  Encrypted Message.
- **Cipher:**
  Algorithm which is used to convert the original message to encrypted message.
- **Key:**
  Some critical information used by cipher.
- **For Encryption:**
  Y = EK(X), where Y=cipher text,
  E = encryption, K= key, & X= plain text.

- **For Decryption:**
  X = DK(Y), where X= plain text,
  D = decryption, K= key, Y= cipher text.

In the table below characteristics between AES, DES and RSA is presented in to fourteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds [4].

Table 1: Characteristic features of AES, DES and RSA algorithms.



Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1

4. PROPOSED METHODOLOGY

In the proposed methodology implemented three encryption techniques like AES, DES and RSA algorithms with their combinations namely A-RSA and D-RSA. The DES and AES ideally belong to the category of symmetric key cryptography and RSA belongs to the category of asymmetric key cryptography. The detailed description of the proposed techniques is explained below. Experiments results are given to analyses the effectiveness of each algorithm. There are two main features that specify and differentiate one algorithm from another are the ability to secure and protect the data against attacks and speed of encryption and decryption.

DES: Data Encryption Standard (DES) DES is a block cipher, with a 64-bit block size and a 56- bit key. DES consists of a16-round series of substitution and permutation. DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key is used for encryption and decryption process. In each round, data and key bits are shifted, permutated, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse.

AES: Advanced Encryption Standard (AES) is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages [5].To provide security AES uses types of transformation. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices.

RSA: RSA is a public key system designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. The RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. The problem with choosing long keys is that RSA is very slow compared with a symmetric block cipher such as DES and AES and the longer the key the slower it is. The best solution is to use RSA for bulk data encryption should be done using the comparison of secret key and public key based A-RSA and D-RSA algorithms. RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography [6]. A disadvantage of using public-key cryptography for encryption is speed. Also in RSA algorithm is can only be used to encrypt small data and cannot be used for large data blocks or large files [6]. So symmetric algorithms DES & AES are proposed with RSA. A detailed flow is explained in figure 2 and 3.

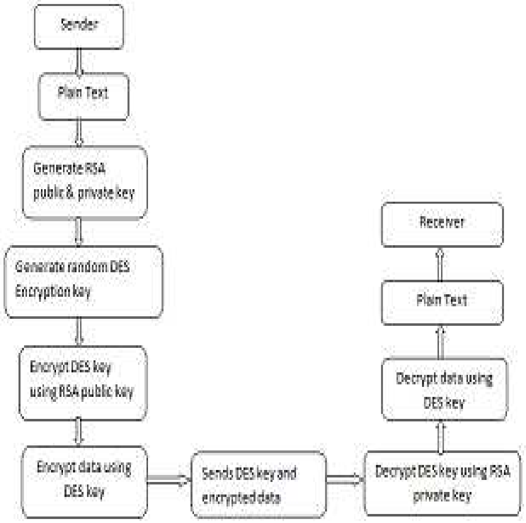

Sender
Plain Text
Generate RSA public & private key
Generate random DES Encryption key
Encrypt DES key using RSA public key
Encrypt data using DES key
Sends DES key and encrypted data
Decrypt DES key using RSA private key
Decrypt data using DES key
Plain Text
Receiver

Figure 2: Proposed Flow Diagram of D-RSA

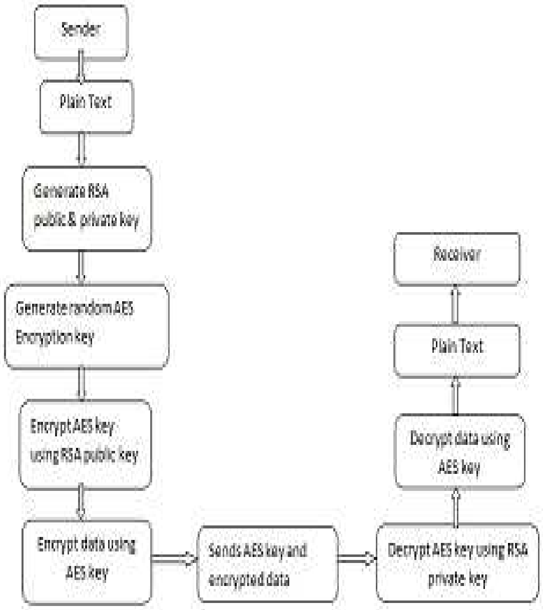

Sender
Plain Text
Generate RSA public & private key
Generate random AES Encryption key
Encrypt AES key using RSA public key
Encrypt data using AES key
Sends AES key and encrypted data
Decrypt AES key using RSA private key
Decrypt data using AES key
Plain Text
Receiver

Figure 3: Proposed Flow Diagram of A-RSA

5. EXPERIMENTATION AND RESULTS

The proposed method is evaluated using various parameters such as input data size, Computation time, Throughput, power consumption and mean processing time. The common measuring criteria for the algorithms are normally expressed as a function of the size of the input n. The six text files of different sizes are used to conduct experiments, where a comparison of the two algorithms A-RSA and D-RSA is performed [7, 8]. The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time.

Input data size: Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

Computation Time: The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is. The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. The decryption time is considered the time that a decryption algorithm takes to reproduces a plain text from a cipher text.

Throughput: Throughput of the encryption algorithms is calculated by dividing the total plain text in Megabytes encrypted on total encryption time for each algorithm. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. The throughput of the encryption scheme is calculated as,

$$\boxed{\textit{Throughput of Encryption} = \frac{\textit{tp (bytes)}}{\textit{et (second)}}}$$

Where,

tp: total plain text (bytes)
et: encryption time (second)

Power Consumption: With the help of these cycles such as CPU clock cycle (the operating voltage count by the CPU) and the average current drawn for each cycle (ampere-cycle) we can easily calculate the energy consumption of cryptographic functions.

$$\boxed{\textit{Power Consumption} = \frac{1}{\textit{Throughput}}}$$

Mean Processing Time: Mean processing time is the difference between the starting time taken to encrypt the data and the ending time. It is the difference between the times taken to encrypt the data. As the size of input increases the time taken to encrypt the data will increase and with the increase in time speed-up ratio decreases.

Mean Processing Time = End time to encrypt – Start time to encrypt

Experimental results of Encryption algorithm for D-RSA & A-RSA is shown in Table 2 and Table 3

Table 2: Metrics of D-RSA Encryption Algorithm.

Input size (kB)	Time to encrypt (ms)	Time to decrypt (ms)	Encryption Throughput (kB/ms)	Decryption Throughput (kB/ms)	*Power Consumption (J)*	*Mean processing time (ms)*
10	31	13	0.32	0.77	3.13	31
20	40	21	0.50	0.95	2.00	40
30	46	32	0.65	0.94	1.54	46
40	54	40	0.74	1.00	1.35	54
50	60	48	0.83	1.04	1.20	60
100	75	65	1.33	1.54	0.75	75
150	100	90	1.50	1.67	0.67	100
200	148	121	1.35	1.65	0.74	148

Table 3: Metrics of A-RSA Encryption Algorithm.

Input size (kB)	Time to encrypt (ms)	Time to decrypt (ms)	Encryption Throughput (kB/ms)	Decryption Throughput (kB/ms)	Power Consumption (J)	Mean processing time (ms)
10	34	11	0.29	0.91	3.45	34
20	50	20	0.4	1	2.5	50
30	55	27	0.55	1.11	1.82	55
40	60	40	0.67	1	1.49	60
50	76	51	0.66	0.98	1.52	76
100	82	65	1.22	1.54	0.82	82
150	95	75	1.58	2	0.63	95
200	124	99	1.54	2.02	0.65	124

Table 2 and 3 provides the comparison of parameters between A-RSA and D-RSA. The given parameters are input data size, Computation time, Throughput, power consumption and mean processing time.

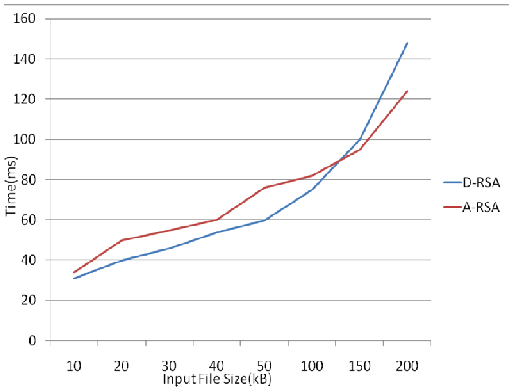


Figure 3: Encryption Time (ms) of Both the Algorithms for Different Input File Sizes

The Figure 3 illustrates the comparison between encryption time and input size for both D-RSA and A-RSA. From figure 3, it can be clearly observed that the A-RSA give better results compared to D-RSA.

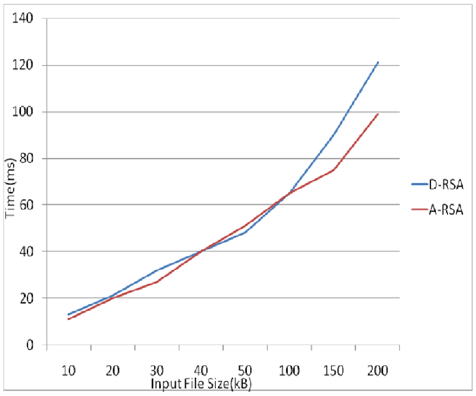


Figure 4: Decryption Time (ms) of Both the Algorithms for Different Input File Sizes

The Figure 4 illustrates the comparison between decryption time and input size for both D-RSA and A-RSA. From figure 4, it can be clearly observed that the A-RSA give better results compared to D-RSA.

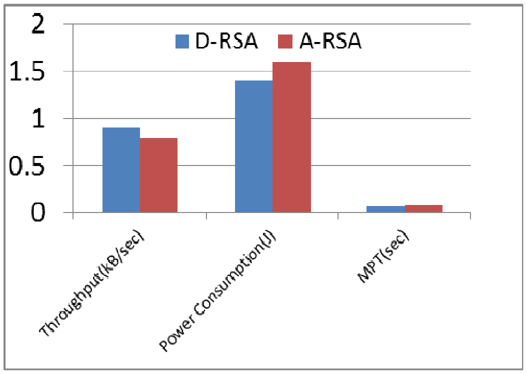


Figure 5: Comparison of Throughput, Power consumption and Mean Processing Time

The above Figure 5 illustrates the comparison between Throughput, Power consumption and Mean Processing Time for A-RSA and D-RSA. From figure 4, it can be clearly observed that the A-RSA give better results compared to D-RSA.

6. CONCLUSION

In this paper, we proposed a Two Phase RSA encryption algorithm for protecting the confidentiality and integrity of uploading files or data in mobile storage cloud. Encryption algorithm play an important role in communication security whereas input data size, Computation time, Throughput, power consumption and mean processing time are the major issue of concern. The selected encryption combinations A-RSA and D-RSA algorithms are used for performance evaluation based on the text files used and the experimental result it was concluded that A-RSA algorithm gives better result in all aspects compared to D-RSA algorithm. We have many more algorithms to be evaluated and their results can be analysed with one another to produce the best implemented security algorithm in cloud environment for future use.

REFERENCES:

[1] Portio Research, "Mobile subscribers worldwide", [online] Available athttp:// www.onbile.comlinfo/mobile-subscribers-worldwide.

[2] Morten V. Pedersen, Member IEEE, and Frank H. P. Fitzek, Senior Member, "Mobile Clouds: The New Content Distribution Platform," Proceedings of the IEEE, Vol. 100, May 13th, 2012.

[3] M.Sujithra, G.Padmavathi, Sathya Narayanan,"Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud", Procedia Computer science, volume 47, pages 480-385, 2015.

[4] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati" A data outsourcing architecture combining cryptography and access control". In Proceedings of the ACM workshop on Computer security architecture, pages 63–69, 2007

[5] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[6] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, Feb 1978.

[7] Wei Ren, Linchen Yu, Ren Gao, Feng Xiong," Light weight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing "Tsinghua Science And Technology, ISSNl1007-0214ll06/09llpp520 528.Volume 16, Number 5, October 2011.

[8] Itani W, Kayassi A, Chehab A "Energy-efficient incremental integrity for securing storage in mobile cloud computing" In: 2010 International Conference on Energy Aware Computing (ICEAC10). Cairo, Egypt, 2010: 1-2.