Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA

Sukhjinder Singh
M. Tech Student,
Department of Information Technology,
Chandigarh Engineering College, Landran, Punjab, India

Mr.Sachin Majithia
Assistant Professor,
Department of Information Technology,
Chandigarh Engineering College, Landran, Punjab, India

Abstract- Cloud computing is an emerging computing paradigm where user can store their data online and access any time and any where according to their requirement.. There are number of requirements to secure the data transmitted over cloud network using different services. To provide the security to the cloud network and data, different encryption methods are used. Encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. The numbers of algorithms are used for encryption and decryption for cloud network. In this paper NTRU algorithm is implemented on cloud network using an android platform. This paper also analyzes the comparison between NTRU public key based algorithms, RSA public key based algorithm, DES secret key based algorithm. There are three main features that specify and differentiate one algorithm from another based on encryption time, decryption time and throughput. This paper compares the performance of three most useful algorithms: NTRU, DES and RSA.

Keywords- Cloud Computing, Android Platform, Encryption, Decryption, NTRU, RSA, DES, throughput.

I. INTRODUCTION

Cloud Computing means "internet computing", internet is seen as collection of clouds and cloud computing enables consumers to access resources online from anywhere any time without worrying about physical/technical issues of resources. But Security of cloud network is main issue. There are various encryption algorithms used for security of data packets send from an android platform on Cloud Network [8]. Android is a software platform and operating system for mobile devices, based on the Linux kernel, and developed by Google and later the Open Handset Alliance. It allows developers to write managed code in the Java language, controlling the device via Google-developed Java libraries. Encryption is a process of converting information in hidden form. So that it is intelligible only to some one who knows how to decrypt it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. In our work, Encryption and Decryption of data over cloud network have been performed by using NTRU encryption algorithm.NTRU and RSA algorithms are public public key cryptography while DES is secret key cryptography.

II. NTRU ALGORITHM

NTRU stands for Number Theory Research Unit. NTRU is actually a parameterized family of cryptosystems; each system is specified by three integer parameters (N, p, q) which represent the maximal degree N-1 for all polynomials in the truncated ring R, a small modulus and a large modulus, respectively, where it is assumed that N is prime, q is always larger than p, and p and q are co prime. The NTRU algorithm involves three steps: key generation, encryption and decryption, throughput [10].

2.1 Key Generation-NTRU involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the NTRU algorithm are generated the following way:

- Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
- Compute $n = pq$.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime.e is released as the public key exponent.e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
- Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
- This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$

- This is often computed using the extended Euclidean algorithm .*d* is kept as the private key exponent.

2.2 Encryption- It is the process to convert data into a form, called ciphertext that cannot be easily understood.

- **Encryption Time-**It is the time taken to perform encryption on user data.

2.3 Decryption- It is the process to convert ciphertext back into the original form.

- **Decryption Time**- It is the time taken to perform decryption on encrypted data.

2.4 Throughput-It is the average rate of successful packets send over a communication channel per unit of time [1].

III. DES ALGORITHM

The standard procedure of blocking the message into blocks of length 64 bits and enciphering each block (using the same key) is known as the electronic codebook mode (ECB).Plaintext is broken into blocks of length 64 bits. Encryption is blockwise.A message block is first gone through an intial permutation IP, and then divided into two parts $L_1||R_1$ where L_1 is left 32 bits. Round i has input $L_{i-1}||R_{i-1}$ and output Li||Ri, where $L_i=R_{i-1}$, $Ri=L_{i-1}$ After Round 16, L16 and R16 are swapped, so that the decryption algorithm has the same structure as the encryption algorithm. Finally, the block is gone through the inverse permutation [3].

IV. RSA ALGORITHM

The RSA algorithm is the most commonly used encryption and authentication algorithm. The algorithm involves multiplying two large prime numbers. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key [6].

V. METHODOLOGY

5.1 Implementation Setup-This section describes the implementation environment and used system components .The implementation of NTRU has been done in Eclipse using Java Language. Cloud has been created using NetBeans IDE 6.5.1.

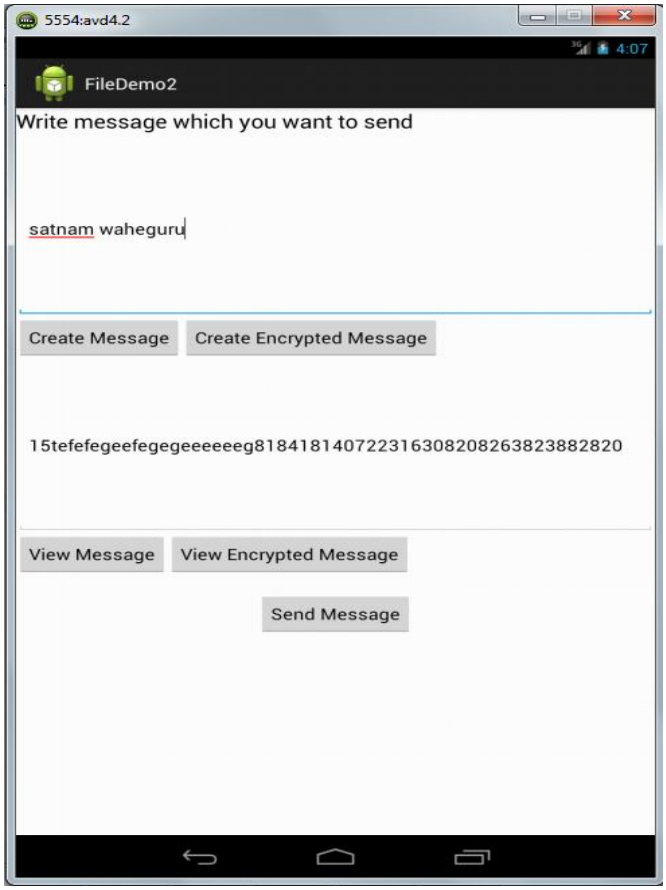

Fig 1: Creating Message in Android console.

5.2 Methodology Used-This section will discuss a methodology and its related parameters, experiment factors.

- **System Parameters-** The experiments are conducted using Intel 32 bit processor with 320 GB RAM. The program is written in Java language.
- **Experiment Factors-**In order to evaluate the performance of NTRU algorithm for android platform on the basis of encryption time, decryption time and throughput.

5.3 Working Steps

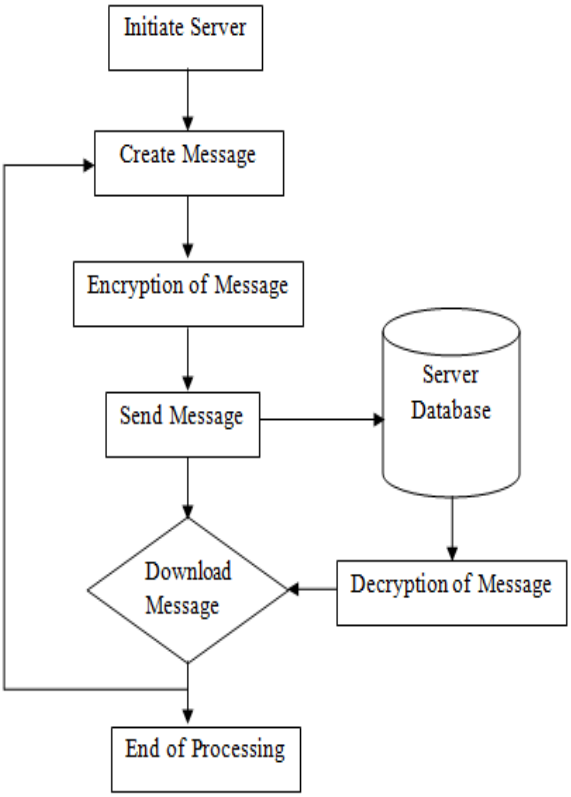

Fig 2: Working Flowchart

VI. SIMULATION RESULT

This Section will show the result obtained from the simulated environment for NTRU, DES and RSA algorithms. Results of the simulation have been shown below in the form of graphs Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased than power consumption decreased. So, as encryption speed of the NTRU is more than the encryption speed of RSA and DES as shown in figure 3 and figure 4. NTRU also consumes small power as comparison to RSA and DES power consumption.

Table 1: Encryption Time for Different Data Input

Data Input	NTRU	RSA	DES
58	12ms	46ms	28ms
78	16ms	65ms	35ms
131	17ms	88ms	40ms
162	35ms	110ms	35ms
322	60ms	157ms	89ms
466	66ms	169ms	131ms
823	125ms	309ms	240ms
1062	147ms	420ms	340ms
Throughput(MB/Sec)	6.33	2.22	3.26

Table 2: Decryption Time for Different Data Input

Data Input	NTRU	RSA	DES
58	15ms	58ms	25ms
78	12ms	62ms	45ms
131	17ms	52ms	50ms
162	56ms	85ms	56ms
322	62ms	148ms	93ms

466	80ms	154ms	98ms
823	136ms	163ms	125ms
1062	172ms	210ms	183ms
Throughput(MB/Sec)	5.50	2.14	5.01

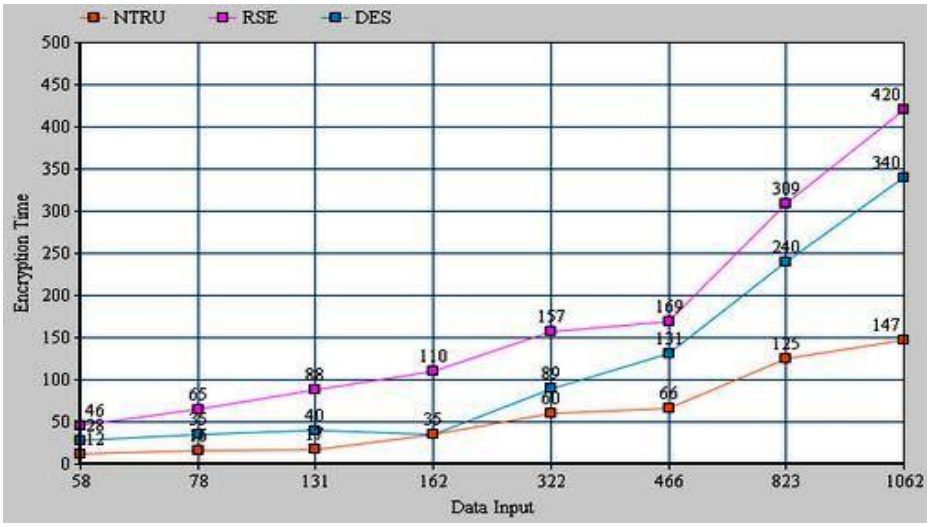

Fig 3: Encryption time of NTRU, RSA, DES algorithms

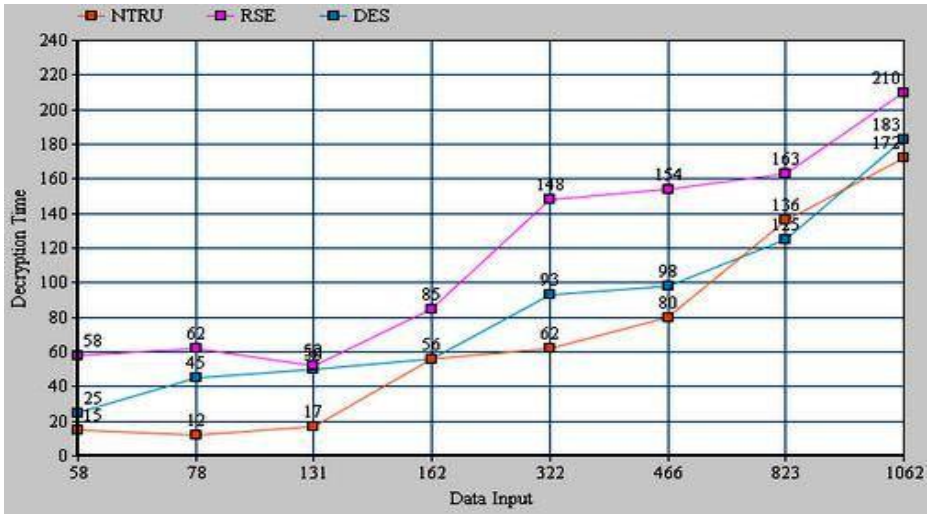

Fig 4: Decryption time of NTRU, RSA, DES algorithms

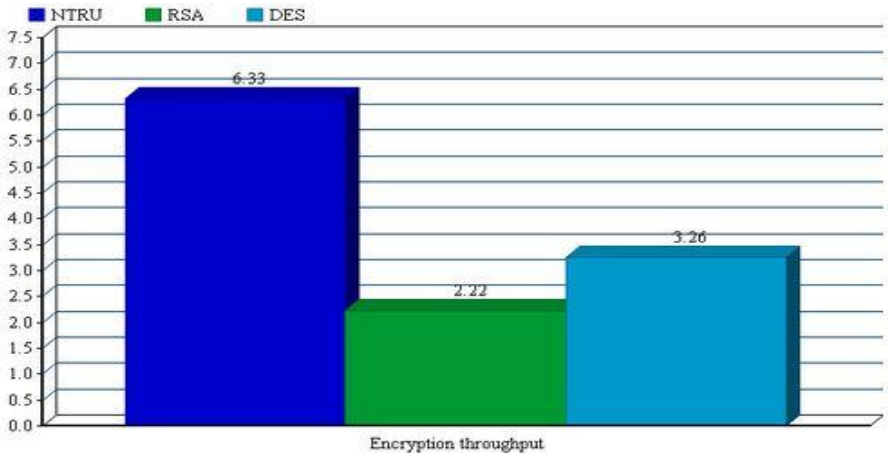

Fig 5: Encryption speed of NTRU, RSA, DES algorithms

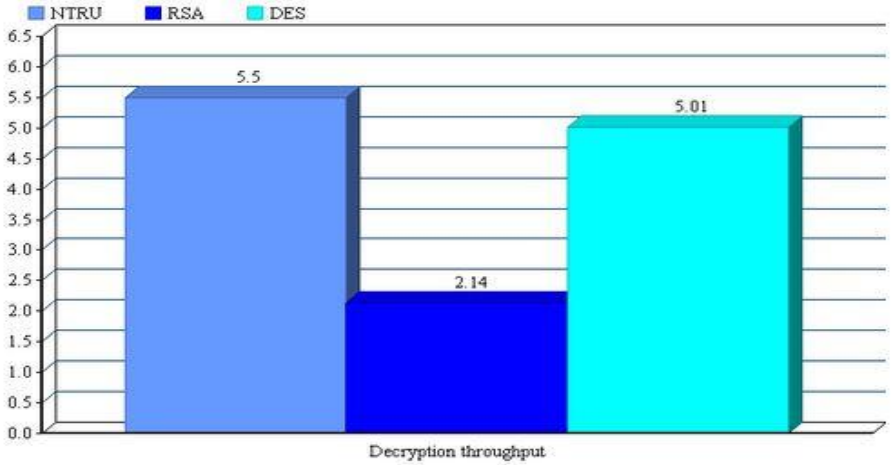

Fig 6: Decryption speed of NTRU, RSA and DES algorithms

VII. COMPARISON

Comparison of NTRU, DES and RSA algorithms has been performed through the results obtained during simulation as given in above figures.

Simulation result shown in Figure 3, 4, 5 and figure 6. The given figures are used to represent the encryption and decryption time and throughput of different algorithms. Thus we find in Encryption and decryption of data that NTRU is better than all other algorithms in throughput and power consumption. Finally, DES and RSA still requires more time than NTRU.

Table 3: Distinction between NTRU, DES and RSA Algorithms.

Features	**NTRU**	**DES**	**RSA**
Approach	A-symmetric	Symmetric	A-symmetric
Encryption Time	Low	Moderate	High
Decryption Time	Low	Moderate	High
Throughput	High	Moderate	Low
Power Consumption	Low	Moderate	High
Confidential	High	Moderate	Low

VIII. CONCLUSIONS

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. Various algorithms are used to secure data send by a mobile phone using an android platform on a Cloud Network. An Android platform is highly used operating system in latest models of mobile phones. From the above mentioned results of tables and figures, concluded that NTRU algorithm is faster and providing stronger security level than other algorithms. NTRU provided better result so it will improve the current security level, speed and provide reliable message at receiver end with respect to key generation, encryption and decryption.

REFERENCES

[1] A.Padmapriya,P.Subhasri "Cloud Computing: Security Challenges & Encryption Practices" International Journal of Advanced Research in Computer Science and Software Engineering, March 2013.

[2] Aderemi A. Atayero, Oluwaseyi Feyisetan "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption ", Journal of Emerging Trends in Computing and Information Sciences October 2011.

[3] Aman Kumar,Dr.Sudesh Jakhar,Mr. Sunil Maakar" Comparative Analysis between DES and RSA Algorithm's" IJARCSSE, vol.2, 2012.

[4] Eman M. Mohamed, Hatem S. Abdul-kader "Modern Encryption Techniques for Cloud Computing by Sherif El-etri", International Journal of Advanced Research in Computer Science and Software Engineering, March 2012.

[5] Ferguson, N.,Schnier, B.and KonhoT.(2010), "Cryptography Engineering: Design principles and Practical applications"

[6] Mandeep Kaur, Manish Mahajan "Implementing Various Encryption Algorithms To Enhance The Data Security Cloud In Cloud Computing " VSRD International Journal of Computer Science & Information Technology, October 2012.

[7] P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[8] Simarjeet Kaur "Cryptography and Encryption in Cloud Computing", VSRD International Journal of CS & IT Vol. 2 Issue 3, 2012, pp. 242-249.

[9] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[10] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.

[11] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.

[12] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

