International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 1 Issue: 11 825 – 829

Performance Evaluation of NTRU Algorithm on Cloud Network on an Android Platform

Sukhjinder Singh
M.Tech Student,
Department of Information Technology,
Chandigarh Engineering College,
Landran, Punjab, India
er.sukhjinder@hotmail.com

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

Abstract— Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to computers on a pay-as-you-use basis. Users can access these services available on the "internet cloud" without having any previous knowledge on managing the resources involved. 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 shows results of parameters like Encryption Time, Decryption Time and throughput when NTRU, a public key encryption algorithm is implemented on cloud network for an android platform.

Keywords:*Cloudcomputing AndroidPlatform Encryption time Decryption Time NTRU 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 algorithm is a public public key cryptography.

II. ENCRYPTION

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. 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. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm, that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

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

III. DECRYPTION

Decryption is the reverse, moving from unintelligible cipher text to the plain text. This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plain text.

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

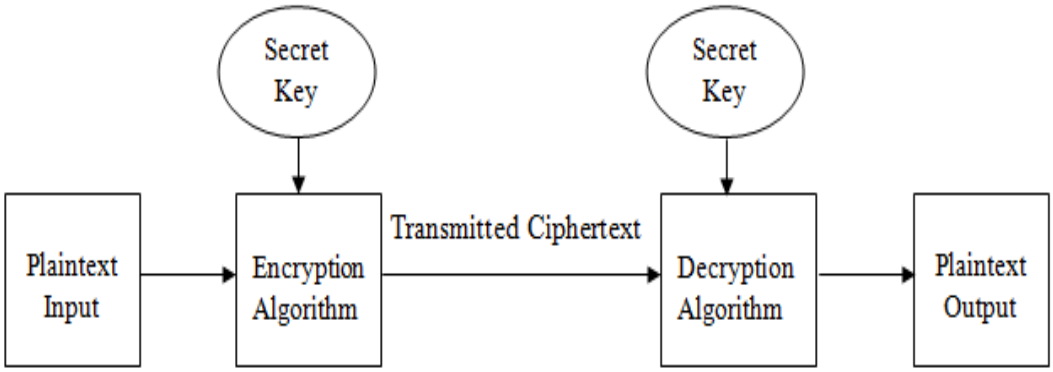

Figure 1: Basic Block Diagram of Encryption and Decryption

IV. 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].

4.1 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 integers 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 $n = pq$.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
- 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.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

4.2 Encryption

- m is plaintext in the form of a polynomial whose coefficients are "small" mod q
- Randomly choose another "small" polynomial r
- r is "blinding value" which is used to obscure the message
- e = r*h +m (modulo q),
- e is encrypted message, m is plaintext, h is public key

4.3 Decryption

- a = f*e (mod q), MUST choose coefficients of a to lie between -q/2 and q/2, e.g. for q=32,
- coefficients must lie in [-15, 16]
- b = a (mod p), MUST choose coefficients of b between -p/2 and p/2, for p=3, the range is [-1,1]
- c = fp*b (mod p), MUST choose coefficients of c between -p/2 and p/2, for p=3, the range is [1,1]

4.4 Throughput

Throughput or network throughput is the average rate of successful message delivery over a communication channel. It is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network.

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.

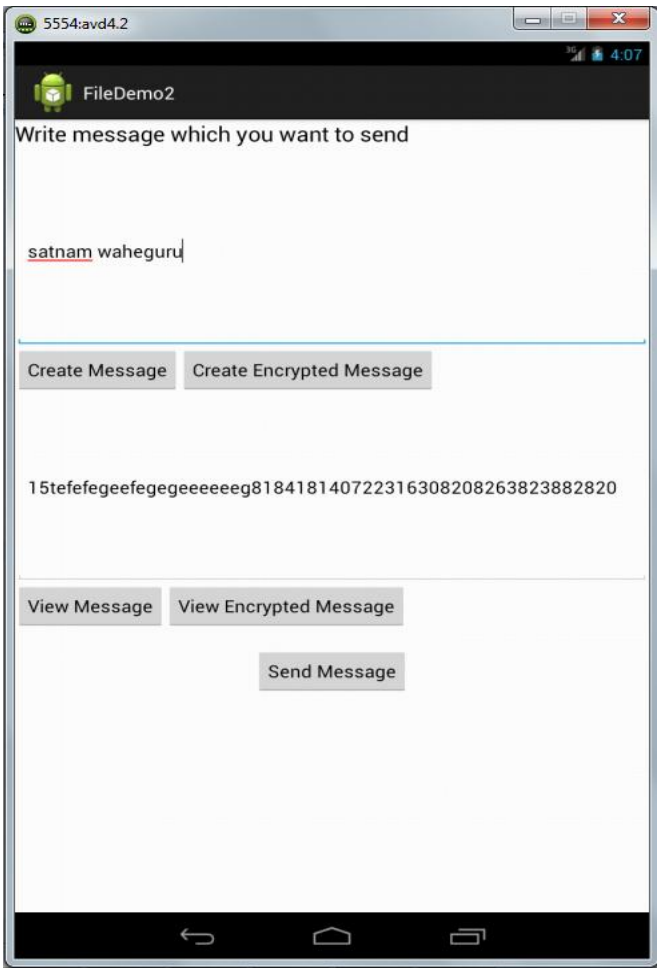

Fig 1: Creating Message in Android console.

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

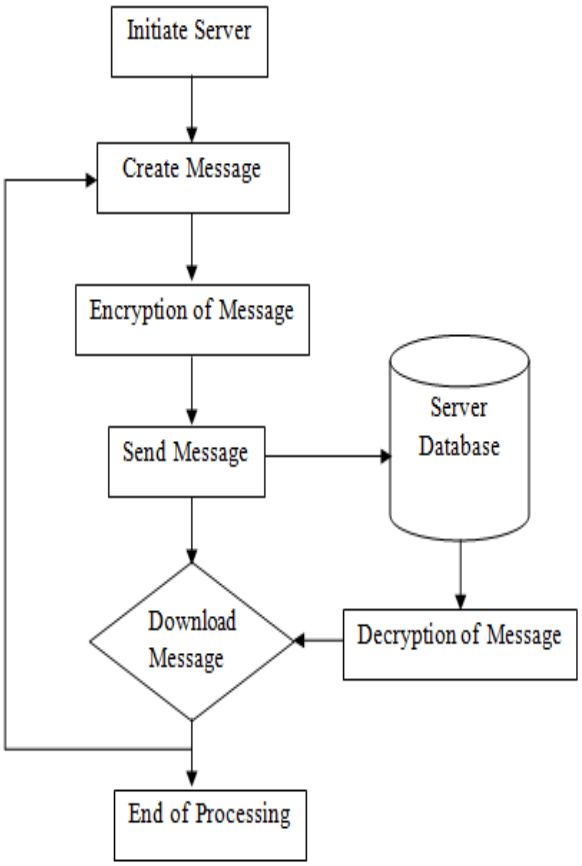

Fig 2: Working Flowchart

VI. SIMULATION RESULT

This Section will show the result obtained from the simulated environment for NTRU algorithm. Results of the simulation have been shown below in the form of graphs Throughput of the encryption algorithm has been calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased than power consumption decreased. Data input is the data or message send by an android user in bytes.

Encryption time has been measured in milliseconds. The whole time taken by NTRU algorithm to encrypt the message or time taken to change plaintext into ciphertext to send over cloud network.

Table 1: Encryption Time for Different Data Input

Data Input	NTRU Encryption Time
58	12ms
78	16ms

131	17ms
162	35ms
322	60ms
466	66ms
823	125ms
1062	147ms
Throughput(MB/Sec)	6.33

Table 2: Decryption Time for Different Data Input

Data Input	NTRU Decryption Time
58	15ms
78	12ms
131	17ms
162	56ms
322	62ms
466	80ms
823	136ms
1062	172ms
Throughput(MB/ Sec)	5.50

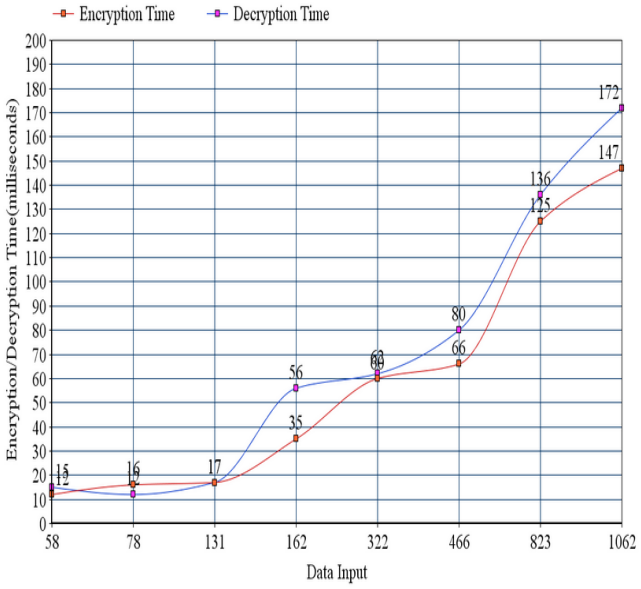

Fig 3: Encryption/Decryption time of NTRU algorithm

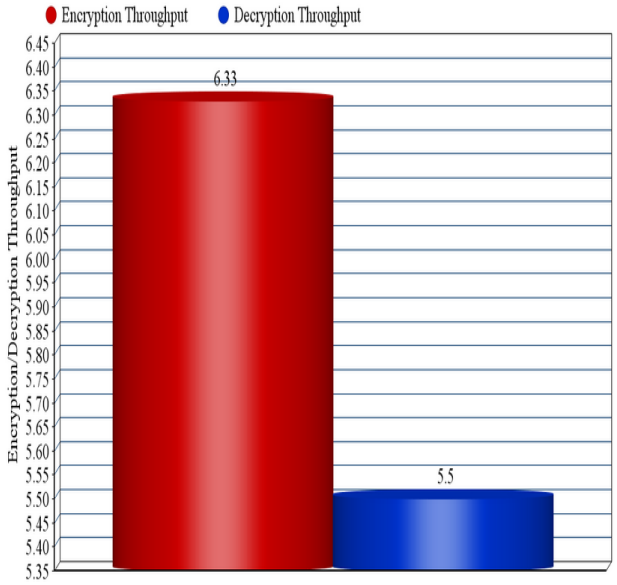

Fig 4: Encryption/Decryption speed of NTRU algorithm

VII. 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, performance NTRU algorithm has been analyzed 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.