JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-3, Issue-6 E-ISSN: 2347-2693

Hybrid Parallel Multithreading Encryption

Deepali[1*] and Namita Kakkar[2]

[1*, 2] *Dept. of Computer Science & Engg, PTU, India,*
deepali.dehar@yahoo.co, namita.kakkar@gmail.com

www.ijcseonline.org

Received: May /29/2015 Revised: June/07/2015 Accepted: June/21/2015 Published: June/30/ 2015

Abstract— First part of this thesis which was needed to be developed before moving onto the next levels is Cloud Computing. The client section was a simple application for user which was made on Socket Programming in Java. Application connection is to be made with Server which is a LAN based server on which data is to be uploaded and downloaded. Since backbone network (client and server) is developed, then it needs to be secured with a particular algorithm or technique. The algorithm studied is known as RSA key oriented algorithm which offers dynamic security on client and server level during communication. The other technique for advancing the level of scalability and improvement along the network layer we used is NTRU encryption. Since this algorithm encrypt data of every type ensures the originality of particular data and adds the advancement in throughput level. These two algorithms are implemented to run on single server on a different core thread thus making the idle cores of sever in use for both the algorithms. It is reflecting that the parallelism encryption done on single content during the data storage on network marginally increase the speed of execution and decryption and encryption timings have been increased. Other part of this thesis also deals with the approaches followed previously which are the part this thesis.

Keywords—RSA, LOSSY, SAAS

I. Introduction

Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge (usually referred to as a "key") that allows them to change the information back to its original, readable form. Encryption is important because it allows you to securely protect data that you don't want anyone else to have entry to. Businesses use it to secure collective secrets, government’s use it to protect classified data, and various individuals use it to secure personal information to guard against things like identity theft. Espionage uses encryption to securely safe folder contents, which consists of emails, ETC. This way, even if your computer is stolen that data is safe. In recent years, with the rapid development of microelectronics technology, the computing capability of many general-purpose processors has gone far beyond CPU. Among them, the Graphics Processing Unit (GPU) is a typical example. The improvement of GPU technology has greatly enhanced the computer graphics processing speed and image quality, and promoted the development of computer graphics-related applications. At the same time, the techniques of streaming processor, parallel computing and programmability of GPU provide a running platform for general-purpose computing beside graphics processing. Therefore, the GPU-based general-purpose computing is a hot topic of research. In this paper, we focus on the application of general-purpose computation on GPU. We propose a new approach of fast RSA parallelizing algorithm according to the architecture of GPU. Our approach can improve the throughput and speed of RSA encryption by optimizing with NTRU [1].

II. Literature Survey

2.1 Parallel AES Algorithm for Fast Data Encryption on GPU (Deguang Le, Jinyi Chang, Xingdou Gou, Ankang Zhang, Conglan Lu)

With the improvement of cryptanalysis, many applications are starting to use Advanced Encryption Standard (AES) instead of Data Encryption Standard (DES) to secure the information. As,current execution of AES algorithm affected from immense CPU resource consumption and less throughput. In this paper, we measured the techniques of GPU parallel computing and its optimized design for cryptography. After that, we proposed another algorithm for AES parallel encryption that has been planned and implemented a fast data encryption system based on GPU. The test proves that our technique can fasten the speed of AES encryption significantly.

2.2 Study on Improved Rijndael Encryption Algorithm Based on Prefix Code (Zhiqiang Xie, Pengfei Gao, Yujing He and Jing Yang2)

Aiming at problem that Rijndael algorithm can be attacked by Square attacks, an improved Rijndael algorithm approach which is built on prefix codes to set forward. Because of the good features in decoding of prefix codes, the approach will modify the sequence of sub-keys through the method of decrypting different plaintext inputted by prefix codes, and build the order relate with the plaintext. With the advancement it has no impact on the efficiency, but it can contact the Square attack radically.

2.3 Comparative Analysis between DES and RSA Algorithm's (Aman Kumar, M.Tech student) BRCM, Dr. Sudesh Jakhar Associate Professor, Mr. Sunil Makkar Assistant Professor)

Internet usage and networking is growing quickly. So there are various needs to protect the data transfer over different networks using distinct services. To supply the protection to the network and data different encryption techniques are used. Encryption is the procedure of converting the plain text in ("readable") form to a cipher text ("non-readable") to provide the security again different attacks. Thus, to provide a protected service to the network there two wide DES and RSA secret and public key cryptography algorithms are used. This paper presents the comparison between DES secret key based algorithm and RSA public key based algorithm. There are two important characteristics that describe and differentiate one algorithm from another are the ability to secure and protect the data against attacks and speed of encryption and decryption. This paper presents the performance of three most useful algorithms: DES, 3DES and RSA. Performance of different algorithms is different according to data loads.

2.4 Comparative Study of DES, 3DES, AES and RSA (Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh (Sunita Lokhande Vishram . N. Bapat)

In today world importance of exchange of data over internet and other media type is eminent; the search for best data protection against security attacks and a method to timely deliver the data without much delay is the matter of discussion among security associated with communities. Cryptography is one of the techniques that provide the security system in timely manner. Cryptography is called as "the study of secret". The two main characteristics that differentiate encryption algorithm from another are their ability to protect the data against attacks and their speed and productiveness in protecting the data. This paper gives a relative study between four such commonly used encryption algorithms i.e. DES, of DES, 3DES, AES and RSA on the base of their ability to protect the data against attacks and rate of encryption and decryption.

2.5 Evaluating Lossless Data Compression Algorithms for Use on Mobile Devices (Literature Synthesis Paul Brittan (BRTPAU008)

In order for this to happen efficiently, the data first needs to be compressed using a data compression application. Data compression is the process of converting an input data stream into a new data stream that has a smaller size. This paper describes four lossless data compression algorithms. Lempel-Ziv 77 (LZ77) and Lempel-Ziv-Welch (LZW) which are based on the dictionary methods, Prediction with Partial Match (PPM) which is based on the statistical methods and Burrows-Wheeler Transform (BWT) which was found to be inadequate since the algorithm does not compression the data only optimizes it for compression. After comparison of the algorithms using benchmark testing, it was found that using LZ77 was the optimal algorithm because of its speed and low memory usage.

III. PAST AND PRESENT SCENERIO

With the improvement of cryptanalysis, many approaches begin to use Rivest, Shamir & Aldeman RSA instead of Data Encryption Standard (DES) to protect their information security. However, current implementations of RSA algorithm suffer from huge CPU resource consumption and minimum throughput. In this paper, we measured the technologies of GPU parallel computing and its optimized design for cryptography. Then, we proposed a new algorithm for RSA with integrating it with NTRU for parallel encryption. NTRU algorithm is a fast encryption algorithm which uses asymmetric key bases approach however we shall not include the key feature of the NTRU the conversion of input text into cipher text shall takes place and designed and implemented a fast data encryption system establish on GPU. The test shows that our technique cans faster the speed of RSA encryption significantly.

IV. PROBLEM FORMALATION

RSA, which is a second good encryption algorithm. What it does, it encrypt the message or can encrypt the data which is been put on network. We can work on the technique by integrating the RSA algorithm NTRU algorithm to speed up the system, moreover there will be a multithreaded server which runs the both algorithm parallel. The hybrid encryption/cryptography technique using this architecture in parallel environment which enhances the performance and speed of Encryption/ Decryption process [2]. That is multiple (two) algorithms will run simultaneously in a single thread. We shall be running two main servers at single system once by using the processor's core thread in short two servers will be running on single system. These two servers will work together to provide a multilevel encryption and generates a secret file from a plain text file.

V. PROBLEM FORMALATION

A. Improving RSA without compromising the security of existing technique to integrate the new technique by introducing the cipher text conversion of NTRU algorithm.

B. Improving the computation time of encryption and decryption by integrating the existing algorithm with NTRU in parallel.

C. To improve the throughput of existing RSA. The benefit of increasing the throughput on decryption and encryption is proposed method will save the energy of server and client devices by using a core CPU threads two at a time.

.

VI. PROBLEM FORMALATION

Cryptographic operations are classified into classes in JCA/JCE. These classes are called as engines. [3]

– JCA engines

– JCE engines

JCA engines are located in java. Security package, JCE engines are located in javax.crypto package.

Example 1: Generate a RSA key and use cipher to encrypt a message.

```
byte[] message = "I am a superman, sshhh don't tell anyone".getBytes();
KeyGeneratorkeygenerator=KeyGenerator.getInstance("DES");
SecretKeydesKey=keygenerator.generateKey();
CipherdesCipher=Cipher.getInstance("DES/ECB/PKCS5Padding");
// Initialize the cipher for encryption
desCipher.init(Cipher.ENCRYPT_MODE, desKey);
// Encrypt message and return
byte[]encryptedMessage=desCipher.doFinal(message);
```

Example 2: Generate random bytes using Secure Random.

```
import java.security.SecureRandom;
public class Main
{
public static void main(String[] argv) throws Exception
{
SecureRandomsecRandom=SecureRandom.getInstance
("SHA1PRNG");
secRandom.setSeed (711);
byte[] bytes = new byte[20];
secRandom.nextBytes(bytes);
}

}
```

VII. CONCLUSION

Through this review this is been analyzed that working on parallel environment will help generate the speed during encryption process and increase the throughput. Since increase in throughput will yield less server overheads which also increases the performance of system (server). Parallel running the two threads will make better utilization of idle threads present in system which will enhance the overall performance ratio of the process.

REFERENCES

[1] Ranjit Ranjan, Dr. A.S Baghel, Sushil Kumar "Improvement of NTRU cryptosystem" International Journal of Advanced Research in Computer Science Vol-2, Issue-9, Page no-**79-84**, September **2012**.

[2] 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, Issue-5, Page no-**1836-1840**, **2011**.

[3] Gurkamal Bhullar and Navneet Kaur "Concurrency and security control with NTRU" International Journal of Innovative Research in Computer Science and Communication Engineering Vol-2, Issue 3, March **2014**.

[4] Dr. C. Sunil Kumar, J. Seetha, S.R Vinotha "Security implications of Distributed parallel cloud database management system models" International Journal of Software Computing and Software Engineering, Vol-2, Issue-11,Page no-**20-28**, **2012**.

[5] Shashi Mehrotra Seth and Rajan Mishra, "Comparative Analysis of Encryption Algorithm for Data Communication", International Journal of Computer Science and Technology Vol-4, Issue-8, Page no-**348-354**, August **2014**.

[6] YashPal Mote and Shekhar Gaikward, "Superioer Security Data Encryption Algorithm", International Journal of Computer Scienece, Vol- 6,Page no-**171-181** , July **2012.**

[7] Parsi Kalpana and Sudha Singaraju, "Data security in cloud computing using RSA algorithm, International Journal of Research in Computer and Communication Technology, Vol-1, Issue-4, Page no-**143-146**, September **2012**.