Improving Battery Life using KUDOS in MCC

Nancy Goel
Pursuing M.Tech (CSE)
Rayat and Bahra Institute of Engg. & Bio-Technology,
Kharar, Punjab State, INDIA.

Atul Bisht
Associate Professor (CSE Department)
Rayat and Bahra Institute of Engg. & Bio-Technology,
Kharar, Punjab State, INDIA.

ABSTRACT

MCC works as a platform where users can perform heavy tasks outside the mobile device i.e. into the cloud. With this concept, a rapid progress in bandwidth, accessibility, security, data processing etc. has made a great effect on human life. .In this paper our main focus is to perform Cloud Computing on Android phones which will help in increasing performance and throughput of mobiles apps in future. There are a number of different cryptography algorithms but here we are introducing a novel methodology which is a Keyless Symmetric technique with bit level security and high speed while performing encryption and decryption tasks on plain text.

Keywords

Cryptography, MCC, RSA, KUDOS, Throughput..

1. INTRODUCTION

In our daily life mobile phones are required to accomplish a number of heavy and complex tasks providing many benefits but while performing such tasks a lot of issues have also been faced by humans. Cloud computing is known to be a promising solution for mobile computing due to mobility, communication, and portability, etc [1]. The cloud can be used to resolve many issues in mobile computing, resulting in many advantages like improving data storage capacity and processing power, improving reliability, etc. There are many applications supported by mobile cloud computing in various areas. Mobile cloud applications are accessed over the wireless connection based on a thin native client or web browser on the mobile devices [8]. MCC also helps in reducing the running cost for compute-intensive applications that take long time and large amount of energy when performed on the limited-resource devices.

Cloud computing can efficiently support various tasks for data warehousing, managing and synchronizing multiple documents online [4]. So when we implement security technique that is cryptography in MCC using an optimal Keyless Symmetric algorithm, then it will results in more safe transmission of data with high authentication [3]. More beneficially, less time will be consumed, more throughput, fast data transmission over network, etc.

The paper is organized as follows: section 2 gives brief introduction about related work, section 3 explains about the methodology followed and section 4 the experimental result of the study. Finally conclusions of the research are presented in section 5.

2. RELATED WORK

There are many techniques which are helpful in providing security, integrity on the data transmission through various different channels, very popular one of them is cryptography. In addition, we also require redundancy, authentication and speed. Here are some papers studied related to various techniques as following:-

- **Gupta et al.** has discussed about background and features of CC and an overview of MCC by defining that MCC integrates cloud computing into the mobile environment and overcomes obstacles related to performance (e.g. battery life, storage, and bandwidth), environment (e.g. heterogeneity, scalability, and availability) and security (e.g. reliability and privacy). This paper has explained two categories of MCC i.e. General Purpose MCC (GPMCC) and Application Specific MCC (ASMCC) [6].
- **Thambiraja et al**. focuses mainly on the different kinds of encryption techniques that are existing with an experimental study of implementations of various available encryption techniques and also focuses on image encryption techniques, information encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. To sum up, all the techniques are useful for real-time encryption [5].
- **Ivy et al.** has used a modified RSA cryptosystem algorithm to handle ‘n’ prime numbers and provides security over the networks. The ‘n’ prime numbers play very necessary role in RSA cryptosystem. To develop the RSA algorithm for ‘n’ prime numbers and also used four prime numbers. It is involved encryption, decryption, and key generation [7].
- **Dimple et al.** In this review paper different asymmetric cryptography techniques, such as RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm) are analyzed. Also in this paper, a survey on existing work which is used different techniques for image encryption is done and a general introduction about cryptography is also given. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications [9].
- **Kumar et al.** explains about RSA algorithm which is the most popular and asymmetric key cryptographic algorithm. It may used to provide both secrecy and digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key [4].
- **Kaushik et al.** explains KUDOS encryption, which is a keyless security algorithm to provide best security. It is based on the concept of user customization. The algorithm doesn’t use the traditional approach of using an encryption key; but defines a series of sequence-counters for encoding. The cryptosystem gives extra power to the user i.e. to choose the sequence-counters. Thus it is up to the user to maintain a balance between speed and security provided by the algorithm. The

cryptographic algorithm is based partially on both stream and block encryption, hence the output of same input block over same input sequence-counter is dissimilar and provides enhanced security. Moreover, for security enhancement, the encryption is done at three levels: block level, character level and bit level [2].

- **Lakshmi et al.** has discussed that Key-oriented algorithms are very efficient but they were very bulky to manage as key handling must be done. Due to the great overhead, keyless algorithms seem an attractive option. There can be various techniques that can be used to attain secure transfer of data like firewalls, proxy servers, and steganography, data security plans against worms, viruses or denial-of-service attacks. So, The KUDOS cryptographic algorithm basically falls under the symmetric encryption i.e. the same key is used at both ends to encrypt and decrypt the data. However, KUDOS actually depends on the sequence counter instead of the encryption key. The major benefit of using KUDOS over other encryption algorithms is its power of customization. In this proposed algorithm both stream cipher and block cipher have used to enhance the security by using advantages of both i.e. high diffusion and bit level security [10].

3. METHODOLOGY

We have introduced an optimal keyless algorithm KUDOS that provides better security and improved efficiency (throughput) on data as compared to other existing key-oriented algorithm RSA. There are two types of cryptographic algorithms used which have been explained as follows:

3.1 Algorithm RSA

It given by three MIT's namely Rivets, Shamir & Adelman [5] and is an asymmetric key algorithm based on two keys.

3.1.1 Significance of RSA

- In this technique we do 'n' prime number factorization.
- It provides efficiency, reliability and security over the networks.
- Security of RSA cryptosystem depends on the large prime numbers, encryption key and decryption key.
- It becomes hard for the eavesdropper to detect the prime numbers from the factorization. Hence it is hard to break this algorithm.
- The real challenge in the case of RSA is the selection and generation of the public and private keys.
- RSA can be used in Mobile nodes; because they are vulnerable to many attacks due to their broadcast nature.

3.1.2 Disadvantages of RSA

- RSA is not suitable for Wireless Sensor Network (WSN) because of high time complexity and consumption demand.
- Another disadvantage of using public-key cryptography for encryption is speed.
- RSA consumes large amount of time to perform encryption and decryption operation resulting low throughput.

3.2 Algorithm KUDOS

This cryptographic algorithm basically falls under the symmetric encryption. It depends on the sequence counter instead of any key. The main benefit is of power of customization. Sequence counter can be manipulated by user according to its own needs [7].

3.2.1 Significance of KUDOS

- In the proposed algorithm we have used both stream cipher and block cipher to enhance the security by using advantages of both i.e. high diffusion and bit level security.
- This algorithm is based on the idea of maintaining a balance between security and speed of an algorithm.
- Three levels of encoding- Block level, Character level, Binary level will make it harder to crack even using brute-force attack.
- Due to absence to keys time required for encryption and decryption of data will be less.
- In our work we mainly deal with MCC and the cloud database. The techniques will be implemented on LAN which is a real world example and will test it on network. Here the web socket programming in java will be used to implement this protocol. On client end that is mobile device, an application is being made from where a user can upload and download its contents to network which is a cloud based server. The user uploads the confidential documents to server to retain its data. The data is being uploaded into server and secured through both algorithms that are RSA and KUDOS. For maximal protection we have added a technique of mac address verification which benefits the user in terms of authenticity. To do implementation, we have to follow the given methodology:
- Cloud Server will be made from where the communication can take place.
- Use Android platform to implement algorithm.
- SDK tool is used for mobile applications which are built in java programming.
- Connection of established cloud server with application is made android SDK.

Figure1 is showing a flowchart of proposed scheme where we will evaluate and compare keyless algorithm (KUDOS) with a key-oriented algorithm (RSA) based on parameters such as : Throughput, Encryption Execution Time (EET) and Decryption Execution Time (DET).

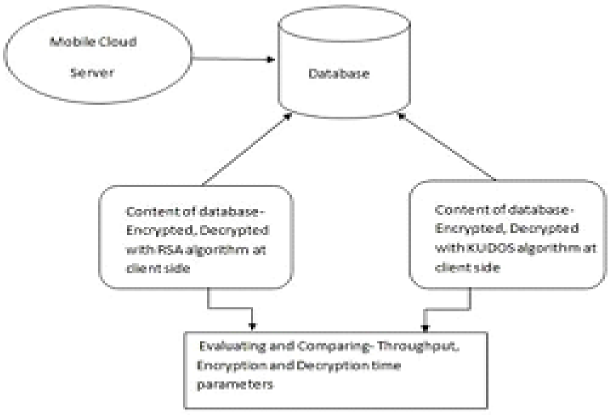
Mobile Cloud Server
Database
Content of database-Encrypted, Decrypted with RSA algorithm at client side
Content of database-Encrypted, Decrypted with KUDOS algorithm at client side
Evaluating and Comparing- Throughput, Encryption and Decryption time parameters

Figure 1: Flowchart of proposed scheme

4. EXPERIMENTAL RESULTS

The Table 1 represents the experimental results with six different sizes of files and corresponding encryption execution time taken by KUDOS and RSA algorithms in seconds. By analyzing the Table 1, we conclude that the encryption time taken by KUDOS is very small as compared to RSA. The encryption time taken by KUDOS and RSA and six different size input files are also shown in figure 2.

Table 1. Encryption Execution time (seconds)

Input file size (MB)	Encryption Execution time (seconds)	
	RSA	KUDOS
5	31.600	30.588
10	72.839	64.649
15	100.201	90.180
20	136.978	125.382
25	162.795	154.465
30	190.847	178.471

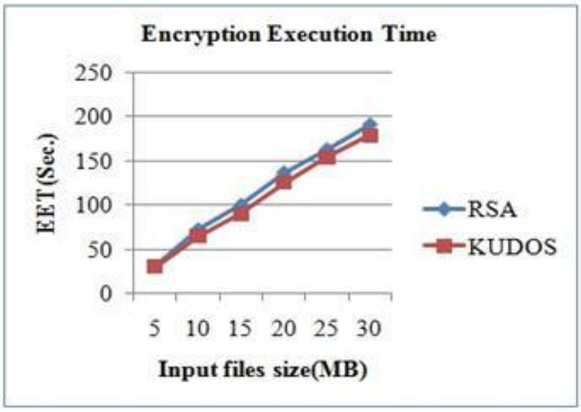

Figure 2: EET among RSA and KUDOS

The Table 2 represents the six different sizes of files and corresponding decryption execution time taken by KUDOS and RSA algorithms in seconds. By analyzing the Table 2, we come to know that experimentally time taken by KUDOS is very small as compare to RSA. The decryption time taken by KUDOS and RSA and six different size input files are also shown in figure 3.

Table 2. Decryption Execution time (seconds)

Input file size (MB)	Decryption Execution time (seconds)	
	RSA	KUDOS
5	33.135	31.871
10	69.353	60.489
15	94.794	87.506
20	126.381	111.735
25	154.715	148.656
30	191.437	188.754

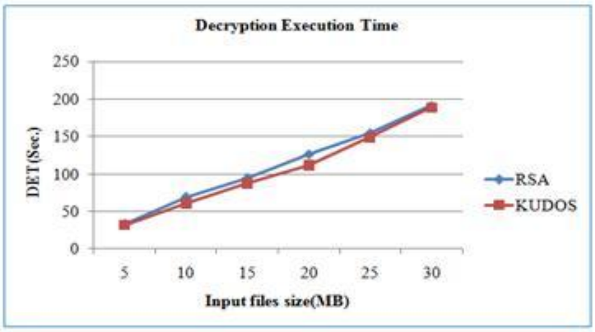

Figure 3: DET among RSA and KUDOS

The Table 3 also represents the results with the six different sizes of files and corresponding throughput execution time taken by KUDOS and RSA algorithms in MB/seconds. By analyzing the Table 3, we conclude that the throughput value resulted by KUDOS is large as compare to RSA. The throughput time taken by KUDOS and RSA with respect to six different size input files is also shown in figure 4. This shows that KUDOS has overlapped RSA.

Table 3. Throughput Execution time (MB/seconds)

Input file size (MB)	Throughput Execution time (MB/seconds)	
	RSA	KUDOS
5	3.7130	3.7134
10	7.4185	7.4401
15	1.1110	1.1132
20	1.4836	1.4858
25	1.8528	1.8550
30	2.2220	2.2242

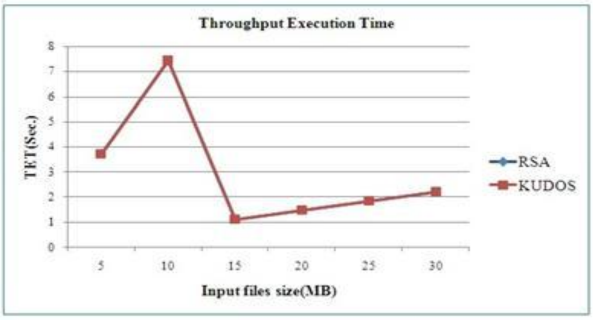

Figure 4: TET among RSA and zUDOS

5. CONCLUSIONS

In this research paper we have presented the implementation of keyless symmetric encryption - cryptography algorithm that is KUDOS which has given the increased throughput value and take less time to perform various encryption, decryption tasks to text files using android phones.

By comparing KUDOS with RSA algorithm which is key-based, we come to the conclusion that security of data will also be enhanced by bit level security using a unique number which is known to user only. Further, if no keys are involved then we overall concluded that it saves the resources of smart phones by reducing battery drainage issue as lot of energy is consumed while using keys. Moreover, if we execute large tasks remotely with efficient ways of transferring data, it may also lead to greater reduction in battery consumption. In future research, the work can be carried out on power consumption factors which included non-suspicious behavior of applications such as a malware in an android environment. Further, several research works can be carried out on issues such as task division, network access management, low bandwidth, etc. Our deemed future working area is to find better strategies and algorithms to offload computation task from mobile devices to cloud.

6. REFERENCES

[1] Dinh, H.T.; Lee, C.; Niyato, D.; and Wang, P. (2011), “A survey of Mobile Cloud Computing: Architecture, Applications, and Approaches”, Wireless Communication and Mobile Computing, Vol.13, October 2011, pp 1587- 1611.

[2] Kaushik, A., Satvika., Barnela, M., and Kumar, A., (2012), “Keyless Use Defined Optimal Security Encryption”, International Journal of Compute and Electrical Engineering, Vol.4, 2, April 2012, pp. 99-103.

[3] Min, Y.G.; Shin, H.J. and Bang, Y.H. (2012), “Cloud Computing Security Issues and Access Control Solutions”, Journal of Security Engineering, Vol.9, 2, April 2012, pp. 135-141.

[4] Kumar, A., Jakhar, S., and Makkar, S. (2012), “Comparative Analysis between DES and RSA Algorithms”, IJARCSE, Vol. 2, July 2012, pp. 386-390.

[5] Thambiraja, E., Ramesh, G., and Umarani, R. (2012) “A Survey on Various Most Common Encryption Techniques”, IJARCSSE, Vol. 2, July 2012, pp. 226-233.

[6] Gupta, P. and Gupta, S. (2012), “Mobile Cloud Computing: The Future of Cloud”, IJAREEIE, Vol. 1, September 2012, pp. 134-145.

[7] Ivy, B.P.U., Mandiwa, P., and Kumar, M. (2012), “A modified RSA Cryptosystem based on ‘n’ prime numbers”, International Journal of Engineering and Computer Science, Vol.1, November 2012, pp. 63-66.

[8] Prasad, M.R.; Gyani, J. and Murti, P.R.K. (2012), “Mobile Cloud Computing: Implications and Challenges”, Journal of Information Engineering and Applications, Vol. 2, 7, 2012, pp 7-15.

[9] Dimple (2013), “Encryption Using Different Techniques: A Review”, SSIJMAR, Vol. 2, 1, January 2013.

[10] Lakshmi, M. and Kavitha, S. (2013), “Keyless User Defined Optimal Security Encryption”, IJECS, Vol. 2, June 2013, pp. 788-793.