A Review: Modified keyless user defined encryption system for Mobile Cloud Computing environment

[1] Khushpreet Kaur, [2]Rajbhupinder Kaur

[1]Department of Computer Engineering, Yadvindra college of Engineering, Talwandi Sabo, Punjab, India
[1]Khushisingh.sidhu706@gmail.com, [2]er.rajbhupinder@gmail.com

***Abstract*— Cryptography and encryption is emerging field of network security. As it is known fact that security of data is very important aspect and has become the first priority for the organization. So it is very much important that the security methods should not only be strong, but should also be easy to execute and implement. The cryptographic algorithms are categorized into key-oriented and keyless encryption algorithms. The main goal of an encryption algorithm is to provide security against unauthorized attacks. Key—oriented algorithms are very efficient but they are hard to manage as key handling need to be done. Because of the great overhead, keyless algorithms seem to be an attractive option. Security in keyless algorithm is achieved by KUDOS encryption which is a keyless algorithm and provide security one level above key-oriented algorithm. Now, we are going to study the optimal security in KUDOS encryption by adding unique number which saves the resource of smart phones as lot of energy and battery is consumed while generating private and public key.**

***Keywords* - Cryptography, encryption, decryption, key-oriented algorithm, keyless algorithm, sequence counter, user defined.**

I. INTRODUCTION

Security issues play a crucial role in computer and communication systems and must be addressed before hand to guard against illicit attacks. In the global communal world, security of confidential data during transfer from one place to another place is a major concern. There are a number of approaches that can be applied inside the organization to keep the data safe and sound. But when this confidential data or information comes outside, it becomes susceptible to the unauthorized attacks by hackers or opponent companies. There can be various techniques that can be used to achieve secure transfer of data like firewalls, proxy servers, data security plans against worms, viruses or denial-of-service attacks. But cryptography proves itself as a central tool for achieving data and software protection. Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel.

The strength of this cryptographic technique comes from the fact that no one can read the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. Due to this advantage, it has grasped a great deal of attention and huge amount of research is being carried out on it. During the course of time, various encryption algorithms have been developed to achieve the ultimate aim of safe environment for information transmission. However, the principal objective guiding the design of an encryption algorithm must be security against all possible unauthorized attacks. However for all practical applications, performance and the cost of implementation are also important concerns. The best cryptographic algorithm is the one that strikes a good balance between security and performance.

Most of the cryptographic algorithms fall into either of these two categories, but the algorithm proposed here uses a combination of stream and block ciphers. The proposed algorithm is known as Keyless User Defined Optimal Security (KUDOS). As the name suggests, KUDOS algorithm is keyless because there is no key involved in the encryption process. Only sequence counters are used. The sequence counters have a definite start point and a particular increment value. The sequences are merged with the actual data at a particular level (described later) and encrypted data then replaces original data. As the KUDOS is user defined, the user can select the starting of the sequence. There are sequence counters on each and every level with different type of increment value. User can define his/ her own counter number from which the counter will start, and then this information will be packed in a packet and appended to the encrypted data. If user does not define anything about the start point of sequence counter, then default values will be taken and there will be no need to append anything to the encrypted data. That's why it is called user defined algorithm.

II. PROBLEM DEFINITION

Data security has become more important as the methods which are used to ensure security not only need to be strong and efficient but should also be easy to implement and execute.

- Key oriented algorithms are very efficient but they are bulky to manage because key handling needs to be done.
- During encryption key generation, lot of energy is dissipated in generating a public and private key which results in low throughput and effects the battery consumption.
- The proposed Keyless algorithm removes all the limitations by adding a unique number which is known to user only. User can upload and download the content by adding unique number. This method also saves the resources of smart phones as lot of energy and battery is consumed while generating private and public key.

III. OBJECTIVES

The objectives are as follows:

- The main objective of the research work is to increase the security in mobile computing environment for mobile users by making the use of keyless algorithm.
- To modify a proposed keyless algorithm KUDOS (Keyless User Defined Optimal Security) by adding unique number which provides ultimate security at one level above of key oriented.
- Proposed algorithm KUDOS uses the advantages of both block ciphers and stream ciphers.

IV. WORKING METHODOLOGY

- The methodology of the work will require the implementation of KUDOS algorithm which is modified by adding unique number to provide security for uploading, downloading document and then this algorithm will perform their encryption and decryption of text document.
- Use Android platform to implement algorithm.
- Calculated and analyzed these parameters which are described as follows:
  1. Encryption Time.
  2. Decryption Time.

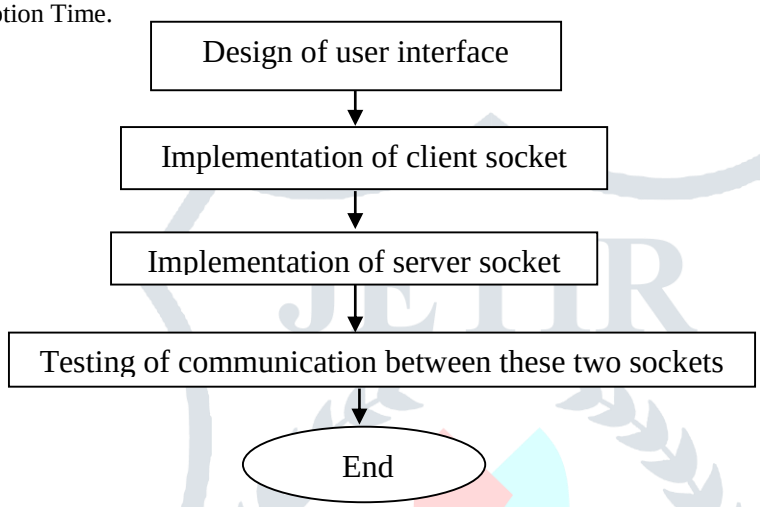


Figure 1 Flow chart of proposed work

V. PROPOSED SYMMETRIC KEY ALGORITHM

The KUDOS cryptographic algorithm falls under the symmetric encryption. However, KUDOS 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 his own needs.

The KUDOS cryptographic algorithm falls under the symmetric encryption. However, KUDOS 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 his own needs.

Sequence counter- It is a new concept which is used to provide dynamic behavior when characters are converted from one form to another. It is imposed as temporary key which alters the characters and bits in original data. It is applied to chosen number of data bits and sequence numbers changes according to an algorithm. This number does not need to save.

Suppose, ASCII sequence of characters

12, 14, 16, 20

And add an even no. sequence of characters

2, 4, 6, 8

Now suppose add operation is used, so solution will be

14, 18, 22, 28

Data is completely changed and it is more powerful but we only need to know the first character of sequence. In the proposed algorithm, it is used at following levels:

Block level- it is the uppermost level where blocks characters of a single block or line are transposed according to the sequence counter.

Character level- Every character have an equivalent ASCII value, which can be merged with the sequence counter. The above example is same.

Binary level – It is lowest level. The calculations are done in form of 0 and 1. It provides more security because effects are visible. 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.

VI. ENCRYPTION PROCESS OF KUDOS

This algorithm is based on the idea of maintaining a balance between security and speed of an algorithm. In this algorithm, two stacks are taken. First stack holds the information about sequence counter and other stack maintains record for the data on which encryption has to be performed. Following are the steps of encryption.

Steps in encryption process:

1. Reading plain text from file line by line.
2. Character transposition is performed using sequence counter and user chooses the sequence counter according to his choice.

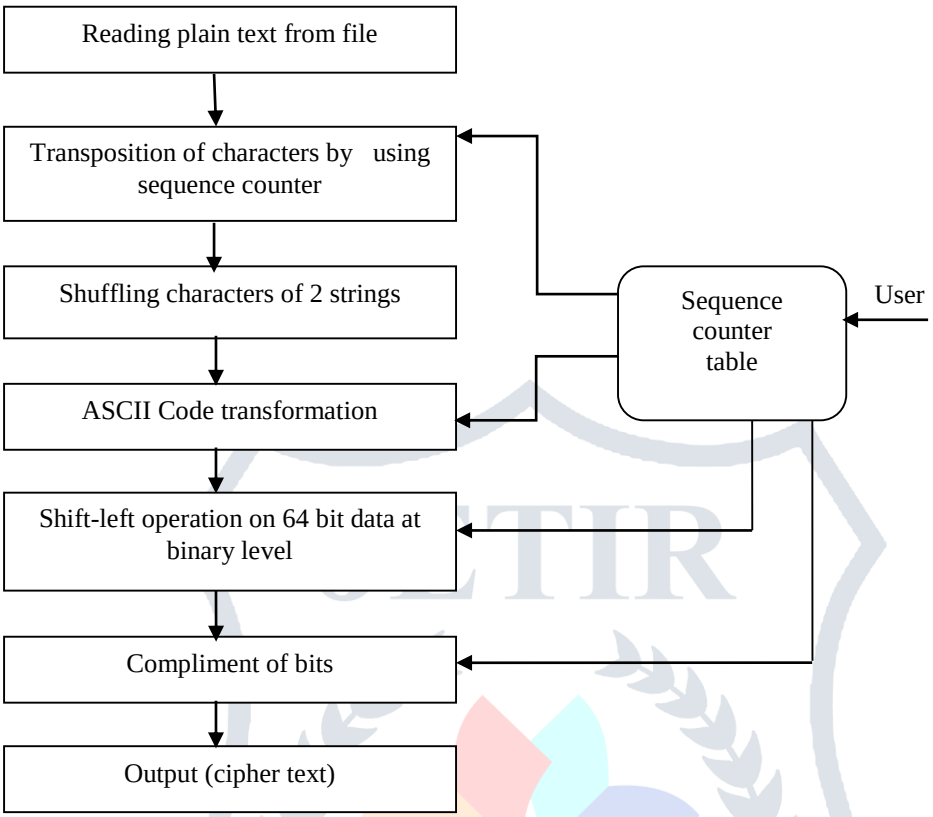


Figure 2.KUDOS encryption procedure

3. Two strings are chosen from file and both are shuffled by placing one character of first string followed by first character of second string. This encryption is user independent.
4. Output from step 2 is taken as input and characters are transformed to ASCII code.
5. Shift-left Operation is performed on 64-bit data at binary level.
6. Encryption process is performed on the base of compliment. Sequence of bits is complimented and next sequence of same number of bits remains unchanged.
7. All the steps are repeated till plaintext is changed into cipher text.

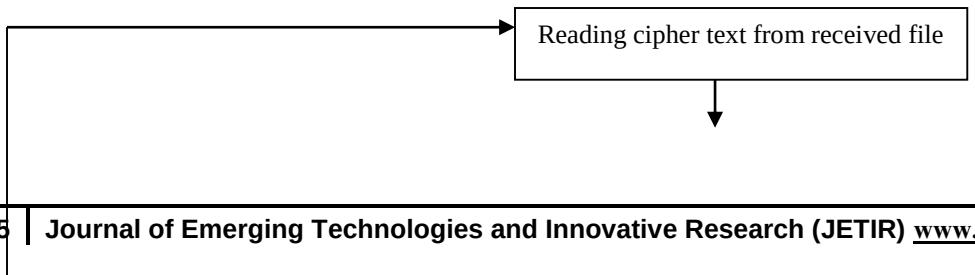
The system does not have any encryption key as sequence counter is used. Sequence counter is of 4 bytes, one byte for each encryption step. Encoding key is the combination of 4 sequence counters. If user chooses the sequence counter, then combined key is sent along with data for encryption at other end otherwise default sequence is used for encryption.

VII. DECRYPTION PROCESS FOR KUDOS

Decryption process is exactly the reverse of encryption process. The proper Sequence counters are identified from the sequence counter table for decryption procedure.

Steps in decryption process:

1. Reading cipher text from received file.
2. Reading sequence counter from central database server and compliment is performed at binary level.
3. Shift-right Operation is performed on modified cipher text.
4. ASCII codes are transformed to characters.
5. Reverse shuffling is performed to get intermediate cipher text.
6. Re-transposition of characters of a single line takes place.
7. All the steps are repeated till cipher text is converted into plain text.



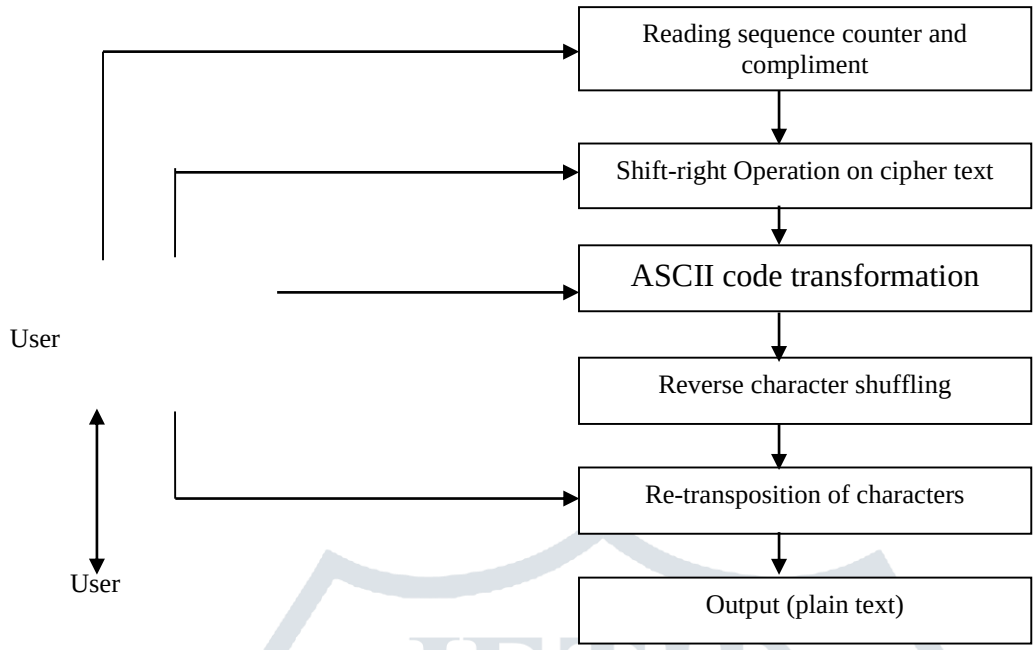


Figure 3.KUDOS decryption procedure

VIII. MODIFIED KUDOS ALGORITHM

Things to remember:

1. It is noted that mobile internet connection and computer internet connection should be same as their platform of connecting through internet should be same otherwise it would not work.
2. User should have android phone with full specification like memory card etc.
3. All the files which are processed will be saved in memory card in different folders.
4. Encryption time and Decryption time will be displayed after each file is processed.
5. Loop optimization is done as loop consumes more time to execute.

IX. IMPLEMENTATION LANGUAGES FOR MODIFIED KUDOS

KUDOS algorithm which is modified by adding unique key will be implemented in java. It can be implemented in any language which supports Unicode system. An Android platform is used for mobile applications such as SDK tools which are built in java programming.

X. BENEFITS OF MODIFED KUDOS ALGORITHM

1. It reduces power consumption as private and public key generation in systems takes lot of resources.
2. This method saves the resources of smart phones as lot of energy and battery is consumed while generating public and private key.
3. Good throughput results of proposed system which increases efficiency and prevents overhead on server as well as smart phone devices.

REFERENCES

[1]. A. C. Donald, S. A. Oli and L. Arockiam, (2013), "Mobile Cloud Security Issues and Challenges: A Perspective," *International Journal of Engineering and Innovative Technology*, Vol. 3, Issue 1.

[2]. V. Chandel and N. Sood, (2013), "Implementation of image and audio data using kudos and compression techniques," *International journals of computing and corporate research*, Vol. 3, Issue 3.

[3]. P. Gupta and S. Gupta, (2012), "Mobile Cloud Computing: The Future of Cloud," *International Journal of Advanced Research in Electrical, Electronics, Instrumentation Engineering*, ISSN 2278-8875, Vol. 1, Issue 3.

[4]. S. Singh, R. Bagga, D. Singh, and T. Jangwal, (2012), "Architecture Of Mobile Application, Security Issues And Services Involved In Mobile Cloud Computing Environment," *International Journal Of Computer and Electronic Research, Volume 1, Issue 2, ISSN:2778-5795*.

[5]. A. Patrascu, D. Maimut and E. Simion, (2012), "New Directions in Cloud Computing. A Security Perspective," IEEE

[6]. R. D. Caytiles and S. Lee, (2012), "Security Considerations for Public Mobile Cloud Computing," *International Journal of Advanced Science and Technology*, Vol. 44.

[7]. V.L.Divya, (2012), "Mobile Application With Cloud Computing," *International Journal of Scientific and Research Publications, Volume 2, Issue 4, ISSN 2250-3153.*

[8]. A. Kaushik, M. Barnela, A. Kumar and Satvika, (2012), "Keyless User Defined Optimal Security Encryption," *International Journal of Computer and Electrical Engineering*, Vol.4, No.2.

[9]. W.Xu-dong and L. Xin, (2012), "Protect Cloud Computing's Data Using Fully Homomorphic Encryption," *National Conference on Information Technology and Computer Science*.
[10]. J. Li, D. Song, S. Chen and X. Lu, (2012), "A Simple Fully Homomorphic Encryption Scheme Available In Cloud Computing" *in the Proceedings of IEEE CCIS*.