Improvisation of Network Security using Encryption Technique for Big Data Technology

Geeta Yadav
M .Tech Scholar
Department of Computer Science & Application
M.D. University, Rohtak , Haryana

Sandeep Dalal, PhD
Professor
Department of Computer Science & Application
M.D. University, Rohtak , Haryana

ABSTRACT
An era has come where technology plays a very dominant role in every one's life. Communication is one such aspect which is crucial for any business to flourish on day to day basis. An upcoming trend changer in terms of technology is Big Data technology which makes the organizations achieve competitive edge over others through big data which helps in exploiting values from available data. All organizations prefer networking system for communicating with their consumers or clients at a faster rate compared to earlier years and achieve success in dynamic environment.

This requires an infrastructure that can manage exploding volumes of unstructured and structured data in rest as well as in motion and protect data privacy and security. Most critical aspect of big data technology lies in security. Leak of security can prove to be dangerous for any business success considering data confidentiality.

In recent years, many scientists and researchers have work towards strengthening of big data's security aspect. Transferring rate of big data depends on its volume, velocity and variety. This research paper show design of a new algorithm which improve security aspect of big data technology and makes application of big data technology safer to operate by organizations.

Keywords
Cryptography, RSA, CAESAR, Big Data, Networking

1. INTRODUCTION
A process for sending information in secret way is known as cryptography [1]. This technique is widely used for protection of information or data. Stenography is an art of that technique in which information hides on the way of communication between two nodes. Cryptography converts messages in cipher text form so that it is not possible for un-authorized person to understand it. Hence, information hidden by stenography technique cannot be seen by any other person that is not authorized for it. In this paper, a new algorithm is being designed by using both processes of stenography and cryptography. This new system will help I enhancing security and confidently of the required data. It

RSA technique which is one of the cryptography technique is very secure and safe technique for transferring the confidential data. New algorithm makes use of RSA technique as a first step for encrypting the data which is followed by second step in which custom neural technique is applied to make data further secured. It is also possible to apply these techniques individually but any hacker can decode them in that condition as retrieve the original confidential data. Hence, integration of these two techniques make the new algorithm even much more secure. An attempt has also been made in this research paper for encrypting images by using techniques of cryptography and stenography.

Benefits of using this technique are:

- The data sent in encrypted form is always more secure and safe.
- Key benefit of hidden data is that attention of intruder cannot notice it.
- By chance if data is extracted then it will be in encrypted form.

With this technique, it will become very difficult to break the encrypted data. The features of this technique is as follows:

- In place of hiding complete text in image, it is first segmented according to 32*32 segmentation plan.
- To merge ASCII encoded bits into the base image, public or private keys are used.
- Original message is accessible to that who knows about this with the help of keys that are used for encryption. Reverse process is applied to get original message.

This technique is more secure and if anyone tries to access it from steno image [2] then it will became waste for that intruder.

2. LITRETURE SURVEY
A study was done by D.S.Abdul. Elminaam et.al, (2009) in which he had evaluated effects of cryptography algorithms on power consumption by wireless devices. He presented a performance estimation of selected symmetric encryption algorithm on power consumption by these devices. Several outputs were generated from the experiment. In the first case, when the packet size was changed with and without transmission of data using different architectures and different WLANs protocols, the result had shown that blowfish had better performance than other common encryption algorithms followed by RC6.

In the second case, results showed that when data type such as audio and video files when used then the result obtained was same as that of text and document type data. In the case of image instead of text, it was found that RC2, RC6 and

Blowfish has disadvantage over other algorithms in terms of time consumption. He found that 3DES still has low performance compared to algorithm DES. In the third case [3] when the transmission of data was considered then there was insignificant difference in performance of different symmetric key schemes (most of the resources were consumed for data transmission rather than computation).

In adhoc wireless LAN connection with excellent signals, there was insignificant difference between open key authentications and shared key authentication. In case of poor signal it was found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod. Finally during the case of changing key size, it can be observed that higher key size leads to obvious change in the battery and time consumption.

Mr. Simar Preet Singh and Mr. Raman Maini has done comparison on data encryption algorithms. The simulation results showed that blowfish has shown better performance than other commonly used algorithms. During examination it was revealed that AES algorithm showed poor performance compared to other algorithms since it requires more processing power. The first sets of experiments were conducted using ECB Mode. The results revealed that superiority of Blowfish algorithm over other algorithms in terms of processing time. It also showed that AES consumes more resources when data block size is relatively large. Another point was observed that 3DES requires always more time than DES because of its triple phase encryption characteristic. Blowfish, which has a long key (448 bit), outperformed other encryption algorithms. DES and 3DES are known to have worm holes in their security mechanism; Blowfish and AES do not have any so far [4].

Analysis found that, CBC requires more processing time than ECB because of its key-chaining nature. The results specify that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection.

3. RSA ALGORITHM

RSA is based on a public key system that was made by Mr.Ron Rivest, Mr.Adi Shamir, and Mr.Leonard Adleman in 1978 [5]. Three basic steps are required to complete the process of RSA operations which are; key generation, encryption and decryption. First, messages are converted into numbers (integers), and then the numbers are manipulated according to the prescribed encryption scheme. Here is the description of the RSA cryptosystem. For the implementation of RSA, following steps are followed [6]:

Step 1 First select two prime number p and q.
Step 2 Then compute value of n= p x q.
Step 3 Chooses e with $(e, (p-1)(q-1)) = 1$ and computes d with $de \equiv 1 (\mathrm{mod}(p-1)(q-1))$.
Step 4 Makes n and e public and keeps p, q, and d secret.
Step 5 Sender encrypts m as $c \equiv me \pmod n$ and sends c to Receiver
Step 6 Bob decrypts by computing $m \equiv cd \pmod n$.

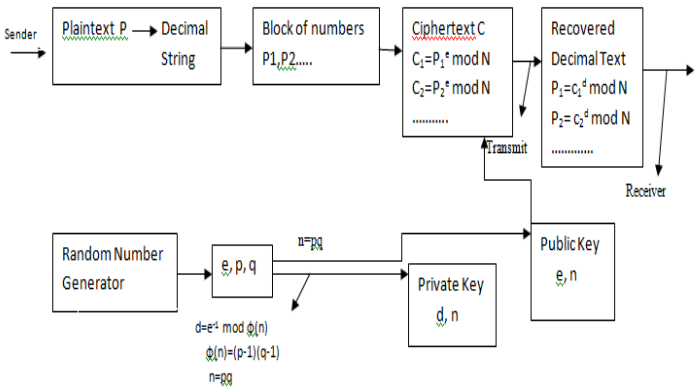

Fig 1: RSA Algorithm

4. CAESAR CIPHER

An example of conventional cryptography can be taken as substitution cipher. A substitution cipher substitutes one piece of information or data for another. It is most commonly performed by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring and Julius Caesar's cipher. In both cases, the algorithm indicates offset the alphabet and the key represents the number of characters to offset it.

For example, if word "SECRET" is encoded using Caesar's key value of 3. Then alphabet will be offset first so that the 3rd letter down (D) begins the alphabet.

So, starting with

ABCDEFGHIJKLMNOPQRSTUVWXYZ

And sliding everything up by 3, result obtained is

DEFGHIJKLMNOPQRSTUVWXYZABC

Where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, "SECRET" gets encrypted as "VHFUHW." For decoding the data, key 3 will required to read the cipher – text.

This is simple example which illustrates that how conventional cryptography works.

5. COMPARATIVE GRAPH OF EXISTING SECURITY ALGORITHMS

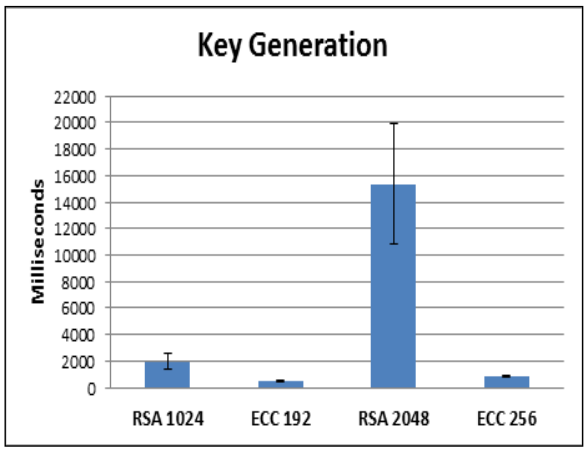

Fig 2: Key generation time

5.1 Asymmetric performance testing

Execution time: When the tests were performed, results show that there is a major difference in the execution time between RSA and ECC. It was discovered that for key generation, due to the smaller key size ECC is extensively faster than RSA. However for both key exchange and the digital signature performance tasks, RSA is significantly faster than ECC. Below graph shows that the execution time for the key generation performance tasks.

5.2 Symmetric performance testing

Execution time: Below graph represents the average execution times for encryption across all 5 algorithms when tested using the sample medical records. From the graph, it can be seen that XTEA and two fish are the most efficient in this instance.

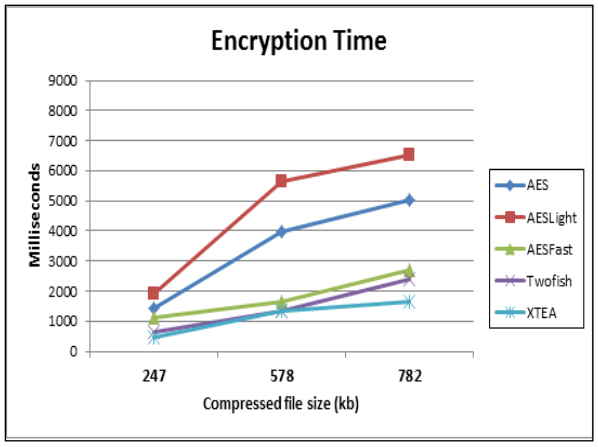

Fig 3: Encryption time for encryption algorithm

Since there exist both symmetric and asymmetric algorithms that can be implemented efficiently on a mobile phone for the purposes of securing the record during both transmission and in storage within the limited resources, it can be concluded that it is feasible [6]. This result can widen the RSA algorithm for better performance for data protection.

6. PROBLEM STATEMENT

Main motive of the research paper is providing protected communication between sender and receiver. Access any important information by unauthorized user is main problem in communication through networking. So this type of attack is avoided by using some encryption algorithm. RSA is most popular technique used by sender for encryption of data. But as time passes new algorithms replace old algorithms due to some best features. So modification in Caesar will replace RSA in case of time consumption in encryption/decryption.

7. OBJECTIVE OF RESEARCH WORK

Step 1: It is necessary to study the concept of cryptography in Big Data. How a big data challenge security and how this challenge can be dealt?

Step 2: Encryption process is applied on a file. For this two files can be taken whose volumes varies but variety and velocity remain constant.

Step 3: RSA algorithm is applied on those files one by one and time consumption in both cases is compared. This comparison finds out effect of volume variation on encryption process.

Step 4: Caesar cipher is then modified and applied on those files one by one and time consumption in both cases is compared. This comparison finds out effect of volume variation on encryption process.

Step 5: A table generated in which comparison for RSA and Caesar cipher is shown for both files.

8. FLOWCHART FOR PROPOSED METHOD

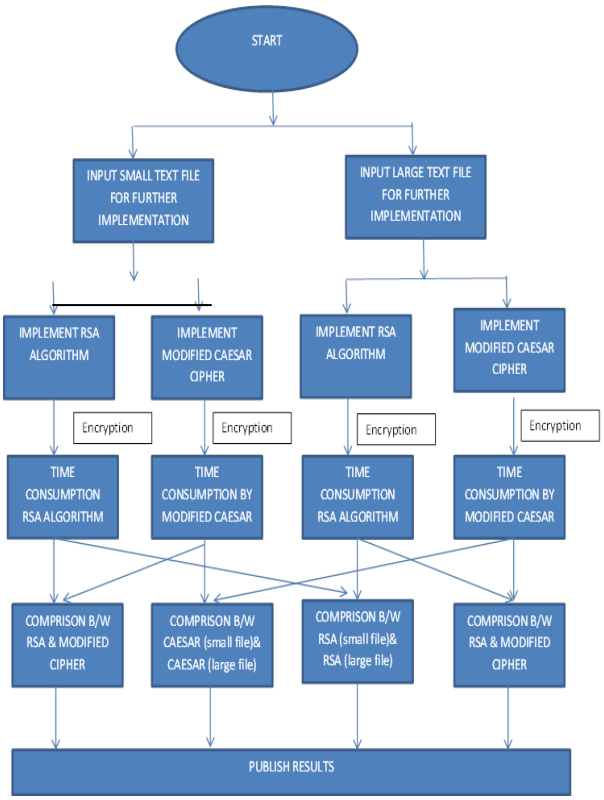

Fig 4: Step follow to achieve proposed result

9. RESULTS

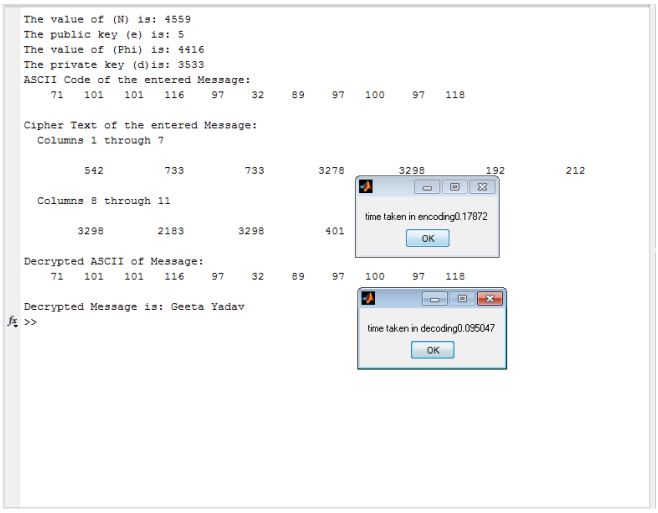

Fig 5: Apply RSA on small txt file

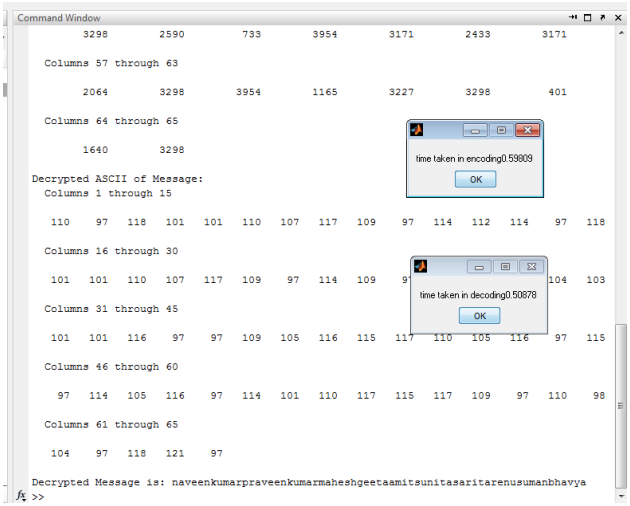

Fig 6: Apply RSA on large txt file

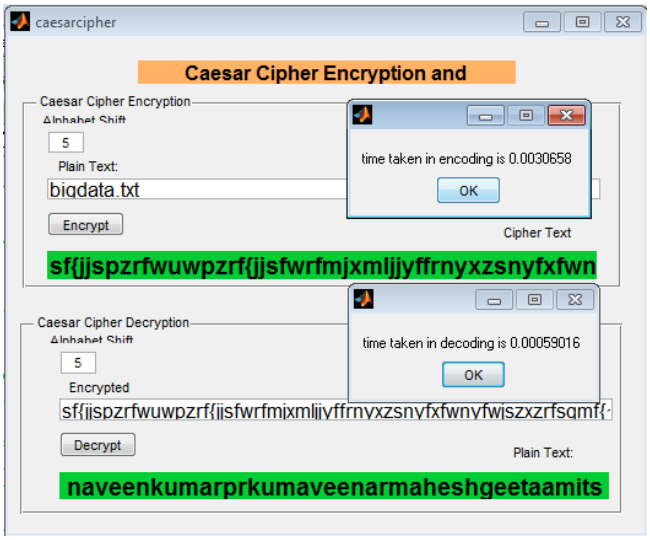

Fig 7: Apply Modified Caesar Cipher on small txt file

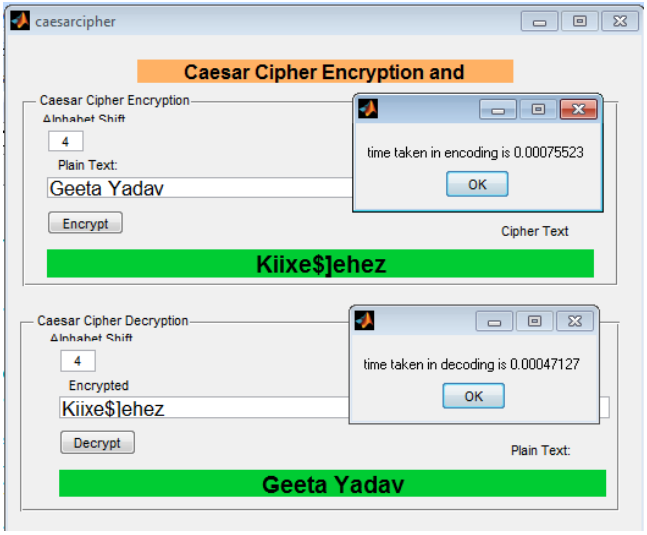

Fig 8: Apply Modified Caesar Cipher on large txt file

10. CONCLUSION & FUTURE SCOPE

This research paper shows successful achievement of the encryption and decryption of the given text files for all the algorithms. It also showed cryptanalysis for the two algorithms of modified Caesar Cipher & RSA encryption techniques. These encryption techniques make data more secure. Comparisons were performed by these algorithms on various data types. It was observed that size of text file varies to count the effect of volume due to big data in comparative results. In future the proposed algorithm can be applied on audio and video files. The variety and velocity of big data is constant in this work. In future, these issues can be taken up and varied for getting desired output.

11. REFERENCES

[1] Michael Cooper & Peter Mell, "Tackling Big Data" NIST Information Technology Laboratory, Computer Security Division, Dept. of commerce, US.

[2] Information Commissioner's Office, "Big Data and Data Protection", Version: 1.0, 1998.

[3] Domenico Daniele Bloisi, Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127-134.

[4] Professor Paul Cheung, "Big Data, Official Statistics and Social Science Research: Emerging Data Challenges" United Nations Statistics Division, 2012.

[5] Kharrazi, M., Sencar, H. T., and Memon, N. Image Steganography: Concepts and practice. In WSPC Lecture Notes Series (2004).

[6] Dave Clemente, "Cyber Security and Global Interdependence: What Is Critical?" The Royal Institute of International Affairs, 2013.

[7] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept

[8] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[9] C. Kaufman, R. Perlman, M. Speciner, Network Security, Private Communication in a Public World, Prentice Hall, 1995.

[10] Kudakwashe Zvarevashe, Mainford Mutandavari, Trust Gotora, "A Survey of the Security Use Cases in Big Data" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2014

[11] Jung-Wen Lo, Min-Shiang Hwang, Chia-Hsin Liu, "An Efficient Key Assignment Scheme for Access Control in a Large Leaf Class Hierarchy" Information Sciences Vol. 181, 2011 pp. 917–925.

[12] Paul Brittan, Shelley Petzer, "Mobile Medical Records", Link: people.cs.uct.ac.za/spetzer/mobileMedRecords/results_shelley.html