A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA

[1]Dr. M. Veeresha, [2]CH Srilakshmi Prasanna
[1]Associate Professor, [2]Assistant Professor
Department Of CSE
Dr. K. V. Subba Reddy Institute Of Technology, Kurnool.

ABSTRACT

During the last decades, information security has become a major issue. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Cryptography plays major roles to fulfilment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others. But most of the proposed algorithms encountered some problems such as lack of robustness and significant amount of time added to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security goals were enhanced via "A New Approach for Complex Encrypting and Decrypting Data" which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

I. INTRODUCTION

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis.

During the last decades, information security has become a major issue. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Cryptography plays major roles to fulfilment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others. But most of the proposed algorithms encountered some problems such as lack of robustness and

significant amount of time added to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security goals were enhanced via "A New Approach for Complex Encrypting and Decrypting Data" which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

Cryptography is blend of information security and mathematics. The main purpose of encryption is that only the authorized person can decode the message with the help of decryption scheme. It involves processing a message sent by a user by using a cipher to create an output which seems vague to the third party. It was Zimmerman [1] who explained the importance of encryption for hiding messages and data from unwanted third parties. Sukhraliya et al.[3] described the method of using ASCII values for encryption and decryption. Kumar et al. [4] further devised a complex way of using ASCII value. Moreover, an effective method of encrypting data is by formation of a dynamic algorithm. Its effectiveness lies in the fact that the same message will have a different encrypted data each hour thus making it difficult to decrypt without the decryption scheme. Chandrasekaran et al. [2] devised the method of encrypting data using dice and binary conversions in 2015. In this paper, we have proposed a method of encrypting the message using ASCII table and decimal to quaternary conversion.

II. SYSTEM ANALYSIS AND DESIGN EXISTING SYSTEM

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can make use of multiple-core processor to achieve higher speed with higher level of security.

1) Encryption:

In term of encryption process, the algorithm consists of combination of public key infrastructure for hybrid system and RC6 algorithm for confusion and diffusion operations as shown.

2) **Decryption:**

The decryption process involves converting the encrypted data back to its original form for the receiver’s understanding. The same process is performed at the beginning of the encryption and decryption process (connection established) as described in the encryption part at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text.

Disadvantages of Existing System:

- Heavy algorithms to be used to in analysing the data.
- Critical programming techniques to be used.
- No logical packages for encrypting and decrypting the text.
- Libraries are not efficient in analysis user data is never considered in the enhancement of the product.

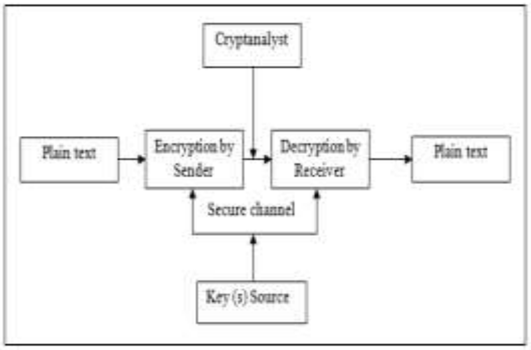
We are using Python programming to analyse the data files. The Python program has many in built methods and libraries to work Programming are easy.

Advantages:

- Python has huge packages which are more efficient to work on files and any kind of unstructured data.

- User friendly programming language.
- Has a Python Library.
- It has package as inbuilt libraries are used at most to analysis.

SYSTEM ARCHITECTURE



III. IMPLEMENTATION

Modules Description

Encryption:

In term of encryption process, the algorithm consists of combination of public key infrastructure for hybrid system and RC6 algorithm for confusion and diffusion operations as shown. The proposed encryption algorithm consists of the following processes Public position is Hexadecimal numbers arranged in 8*8 matrix announced to all. In this step RC6 algorithm play major roles to generate a private position based to the secrete value from public key infrastructure. Plain-text 1024- bits size divided to 2 blocks. One of these blocks used as key after performed confusion and diffusion operations using RC6 algorithm. The last step is Insert the key inside the Cipher data based on the private position.

Encryption, which encodes and disguises the message's content material, is carried out by using the message sender. Decryption, which is the system of deciphering an obscured message, is executed by using the message receiver. The safety furnished with the aid of encryption is immediately tied to the type of cipher used to encrypt the facts -- the power of the decryption keys required to go back ciphertext to plaintext.

Decryption:

The decryption process involves converting the encrypted data back to its original form for the receiver’s understanding. The same process is performed at the beginning of the encryption and decryption process (connection established) as described in the encryption part at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text.

Although there had been many researchers at the cryptography, but maximum of the prevailing algorithms have numerous weaknesses both due to low security level or boom the put off time due the layout of the set of rules itself. The proposed algorithm had been examined towards unique recognized attacks and proved to be cozy against them. Therefore, it is able to be consider as a very good alternative to some applications because of the high stage of security and common time needed to encrypt and decrypt a record the usage of a proposed algorithm is an awful lot smaller than AES algorithm

Objectives Of The Project

There is quite a number of encryption algorithms used for keeping information secured. Their complexity and ability to resist attack varies from one algorithm to another. The main component of encryption process is the algorithms that serve basic purpose in different ways. Popularly used algorithms include DES, TripleDES, RC2, RC4, Blowfish, Twofish and Rijndael (AES) as we mentioned in the abstract.

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can make use of multiple-core processor to achieve higher speed with higher level of security

IV. CONCLUSION

In this project we have proposed a dynamic approach of encrypting a message for safer transmission. The ASCII values of the characters are multiplied with the current hour. The decimal product is then converted to base 4 number. The hour of encryption are sent as first two places of the message which will be required at the time of decryption. The following encryption technique makes the message appear as complex set of numbers ranging from 0-3. Each character of message is converted into set of 6 digit number. Thus making the message long and appear vague to the third party. Since the approach is dynamic and the same message will have different encryption after every hour, it becomes very difficult for the third party to decrypt it.

FUTURE ENHANCEMENT

The proposed algorithm have been tested against different known attacks and proved to be secure against them. Therefore, it can be consider as a good alternative to some applications because of the high level of security and average time needed to encrypt and decrypt a data using a proposed algorithm is much smaller than AES algorithm.

REFERENCES

[1] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

[2] C. Shannon, “Communication Theory of Secrecy Systems”, Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.

[3] I. Nichols, K. Randall (1999), ICSA Guide to Cryptography, McGraw-Hill, Companies Inc, New York.

[4] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.

[5] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.

[6] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

[7] M. Wali and M. Rehan, “Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)”, in the Proceedings of the Engineering Sciences and Technology Conference, vol. 7, pp. 1-7, Karachi, 2005.

[8] C. Jie, “Design Alternatives and Implementation of PKI Functionality for VoIP”, Master of Science dissertation, Telecommunication Systems Laboratory, Royal Institute of Technology (KTH), Stockholm, 2006.

[9] R. Hunt, “PKI and Digital Certification Infrastructure”, in the Proceedings Ninth IEEE International Conference on Networks, vol. 4, pp. 234 – 239, Bangkok, Thailand, 2001.

[10] S. Xenitellis, The Open–Source PKI Book: A Guide to PKIs and Open-Source Implementations, Open CA Team, 2000.