ISSN 2395-1621

Hybrid Encryption Technique For Heterogeneous Data With Distance Learning System

[#1]Suraj Mahale, [#2]Abhijit Kamble, [#3]Sagar Waykule, [#4]Pravin Kothavale

[1]thesurajmahale@gmail.com
[2]abhijit1491@gmail.com
[3]sagarwaykule41@gmail.com
[4]pravinkothavale14@gmail.com

[#1234]Student of Dept. Of Computer Engineering

Indira College of Engineering and Management, Tal. Maval, Maharashtra

ABSTRACT

Various encryption algorithms have been developed for processing text doc-uments, images, video, etc. After collaborate the advantages of the different ex-isting encryption methods, then a new hybrid encryption method can be developed which offers better security and protection. So, in order to accomplish the Hybrid encryption technique, data encryption techniques using a standard Symmetric and Asymmetric two algorithm to achieve better security and high performance i.e.RC6 algorithm, AES algorithm are studied from 'Hybrid Encryption Technique For Het erogeneous Data With Distance Learning System' reference paper, analyzed and their performance is compared. In propose system the message is divided into three parts and these two techniques are applied to these parts and the performance is again analyzed. The application of these two methods to different parts of the same mes-sage along with two keys, namely, segmenting key and encrypting key to provide further authentication and validation is the basis of paper.

ARTICLE INFO

Article History

Received: 10th December 2017

Received in revised form :

10th December 2017

Accepted:14th December 2017

Published online :

14th December 2017

Keywords: Encryption, Decryption, RC6, AES, Hybrid Technique

I. INTRODUCTION

The cloud computing security has become the most important problems in its growth. It has a huge interactions number of data between the platform of cloud computing and user [1]. In the process of data transmission, the data which transfer between the users and cloud computing could possibly be intercepted, it may lead in to leaked of secret data for the enterprise. Data leakage or loss will have a destructive impact on the enterprise. It is not impact on the reputation of enterprise only, but it is cause the customers and partners to lose trust and confidence on the enterprise. Actually the security in cloud have two major aspects: First, the user's data are not going to be leaked to prevent unnecessary losses.

Second, it make sure that the user can get his data accurately whenever he required. Therefore, we must focus on data in storage and in transmission. When the users are willing to transfer their sensitive data to the cloud, the first step is to encrypted the data, so even if the data interceptors steal the data, then they cannot retrieve the data content as it is encrypted. That is why it make sure that the security of user data during transmission in cloud computing.

There are three aspects threats for the data. 1) Security threats, the privacy information could possibly be intercepted by attackers; 2) Integrity threats, data could possibly be altered by attackers; 3) the authenticity of message, to help the cloud to detect whether the message have sent from attacker or authenticated user. In view of such type of threats, we have proposed a strategy to secure the users' data during transmission. It use a technology of double encryption, and combines with the technology

of hash-based message authentication code (HMAC) to ensure the data of users are transfer effective safely. The client generates a value of HMAC and attach it behind the encrypted message by AES algorithm. It ensures the integrity and message authentication of user data. Then the proposed work will use the RC6 algorithm to encrypt the secret key of AES to make sure that the secret key of AES is sent safely.

II. LITERATURE SURVEY

[1] An ASCII value based text data encryption system Year:-2013, in this System having an algorithm to encrypt and decrypt the data base on symmetric key encryption technique. The proposed system is generating very good results. In future,: the system can be further improved by using variable length key. System can be made to encrypt the data on the basis of Unicode values. It also can be improved for to decrypt the sentence form of data. so that it can be accepted globally
Advantages:- it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in infor-mation security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer sci-ence, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.
Limitations:-It also can be improved for to decrypt the sentence form of data.
Technology Used:-ASCII, Symmetric Encryption

[2] An Enhancement of code and energy optimization in PN SEQUENCE Generation Year:-2013, An intermediate approach which is software based generation of PN sequence but acts/operates very closely to hardware. C is a language capable of accessing the systems memory in bitwise manner and it can per-form bitwise operations as well.The approach shows that the memory used for implementation of LFSR is just 2 bytes and 8 bytes for short and long PN sequence respectively.Lesser amount memory means lesser number of memory fetches and lesser number of instruction execution .The calculations shows nearly 70%of reduction in instruction on execution, which intern im-plies nearly 50% of less energy consumption for generating PN sequence.
Advantages:- PN sequences widely uses in CDMA communication system. It can acquire in the presence of channel error, false detection can be minimized without reducing the frame efficiency by using a long sequence multiplexed with the data. PN sequence uses in Spread spectrum modulation to spread the RF bandwidth of the signal, reducing the power spectral density. PN sequence also use for scrambling the data at the same rate to obtain spectral energy dis-tribution within the signal band.
Limitations:-Generator polynomial used for generation of PN sequence is having less number of feedback stages resulting better energy efficiency.
Technology Used:-PN-Sequence

[3] Secured Crypto-Stegano Communication through Unicode and Triple DES Year:-2013, These system usage of how message from sender is encrypted using triple DES through Unicode and hide the encrypted image into an stego image.. On the receiver end, extraction algorithm is designed in such a way that the process separates the message and image into two different entities; then reads the extracted message which is in the encrypted form and trans-forms it from the Unicode symbols to a readable form. The method is defined as undetectable, strong and secured communication of data related to the mul-timedia image. Thus any confidential message can be send to any target with-out the knowledge of others through an unsecured communication channel. This encoding and decoding scheme of the proposed new method is signifi-cantly different as compared to traditional schemes.
Advantages:- The method is defined as undetectable, strong and secured com-munication of data related to the multimedia image. Thus any confidential message can be send to any target without the knowledge of others through an unsecured communication channel
Limitations:- Secret message detectable without secret knowledge.
Technology Used:-Cryptanalysis

[4] An application of data encryption technique using random number gen-erator Year:-2012, these paper having an innovative technique for data encryption is proposed based on the random sequence generation. The new algorithm provides data encryption at two levels and hence security against crypto anal-ysis is achieved at relatively low computational overhead.the system has pow-erful key management and, even more importantly, public-key cryptography has the ability to implement digital signatures in an efficient way. However, symmetric-key is a form of cryptography in which two parties that want to communicate can share a common and secret key. Advantages:-Provides data encryption at two levels and hence security against crypto analysis is achieved at relatively low computational overhead.
Limitations:- Decryption technique not used.
Technology Used:-Cryptanalysis

[5] Secured Communication through Fibonacci Numbers and Unicode Symbols Year:-2012, these paper is a process that scrambles information by rearrangement and substitution of content making it un-readable to anyone except the person capable of unscrambling it. Security key is provided in converting plain text to cipher text, and another key is used to convert the cipher text to Un-icode symbols. Security key in each level is an added advan-tage to the method. It is difficult to decode the Unicode sym-bol from the text file which makes the system complicated in retrieval of the message for an unknown person. Moreover, information stored in a text file in the form of symbols increas-es the amount of information to be conveyed in secret.

Advantages:- Converting plain text to cipher text andconverting cipher text to Unicode symbols. In each level, security key is used to encode the original message which provides two levels of security from intruders. On the other end, the extraction algorithm is designed in such a way that the process con-verts the Unicode symbols into cipher text and then cipher text to plain text.

Limitations:- Unicode System

Technology Used:-Cipher text, Fibonacci Number

III. PROPOSED SYSTEM

We are using following encryption techniques to encrypt and decrypt the document:-

1. RC6 Algorithm.
2. AES Algorithm

RC6 Algorithm.

- RC6 is a symmetric key block cipher derived from RC5.
- Block size of 128 bits. Flexibility of key size.
- No key separation. Operators involved are simple in function favorably.
- High speed with minimal code memory.
- Provides a solid well-tuned margin for security against well-known differential & linear attacks.
- Max potential for parallelism when multiple streams are processed.

RC6 algorithm basic operations:

- a + b: integer addition modulo 2w.
- a - b: integer subtraction modulo 2w
- Aˆb: bitwise exclusive-or of w-bit words.
- An x b: integer multiplication modulo 2w.
- a ¡¡¡ b: rotate the w-bit word a to the left by the amount given by the least significant law bits of b.
- a ¿¿¿ b: rotate the w-bit word a to the right by the amount given by the least significant law bits of b.

AES Algorithm

- AES is a symmetric block cipher that it uses the same key for both encryption and decryption.
- The AES standard states that the algorithm can only accept a block size of 128 bit.
- The entire data block is processed in parallel during each round using substitutions and permutations.
- The input is a single 128 bit block both for decryption and encryption and is known as the in matrix.

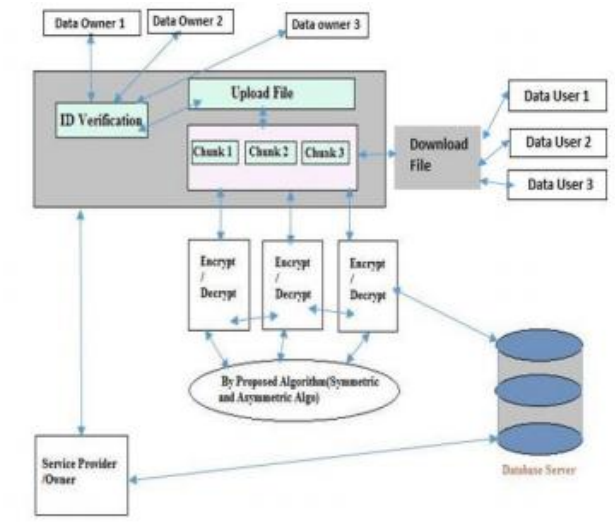

Figure 1: Architecture diagram

IV. CONCLUSION

In this paper, a hybrid encryption system has been constructed. The problems about designing an efficient technique for real time secure audio, video are solved. It is well known that a good encryption technique must withstand any kind of at-tack and should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible. In addition, the high speed of the proposed cryptosystem is sufficient for a real-time encryption. All in all, our hybrid cryptosystem obtains significant computational efficiency and robustness. Thus, it will be well suited for realtime encryption which makes it suitable in multimedia communications.

REFERENCES

[1] Efficient Hybrid Encryption System Based on Block Cipher and Chaos Genera-tor IEEE international Conference On Computer And Information Technology

2016.

[2] Udepal Singh and Upasna Garg, An ASCII value based text data encryption System, in International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013, ISSN 2250-3153.

[3] Rina Choudhary, An enhancement of code and energy optimization in PN Se-quence generation, in International Journal of Engineering and Management Sciences, I.J.E.M.S., VOL.4 (4) Sep2013: 426-429, ISSN 2229-600X.

[4] Sharad Kumar Verma and D.B. Ojha , An application of data encryption tech-nique using random number generator, in International Journal of Research Studies in Computing, Volume 1, Number 1, 35-42, April 2012.

[5] A. Joseph Raphael and V. Sundaram , Secured Communication through Fi-bonacci Numbers and Unicode Symbols, in International Journal of Scientific & Engineering Research, Volume 3, Issue 4, April-2012, ISSN 2229-5518.

[6] Sudha Rani, T. C. Sarma and K. Satya, Text File Encryption Using FFT Tech-nique in Lab View 8.6, in IJRET: international Journal of Research in Engineering and Technology ISSN: 2319-1163, Volume: 01, Issue 01, April-2012.

[7] D. Saran Kumar, CH. Sabetha and A.Chandrasekhar, A Block Cipher Using Rotation and Logical XOR Operations, in IJCSI International Journal of Com-puter Science Issues, Vol. 8, Issue 6, No 1, November 2011, ISSN (Online): 1694-0814.

[8] Himanshu Gupta and Vinod Kumar Sharma, Role of multiple encryption in secure electronic transaction, in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[9] V. Sundaram and A. Joseph Raphael, Secured CryptoStegano Communication Through Unicode, in World of Computer Science and Information Technology Journal(WCSIT) ISSN: 2221-0741 Vol. 1, No. 4,138-143, Aug2011.

[10] Alberto Apostolico and Aviezri S. Fraenkel, Robust Transmission of Un-bounded Strings Using Fibonacci Representations, in Report Number : 85-545, 1985 Jun-2010.

