International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 5 238 - 242

Privacy Preserving of Data Files & Audio / Video Encryption –Decryption Using AES Algorithm

Ms. Aamrapali Murlidhar Tamgadge
R.T.M. Nagpur University
Email: aamrapali1@gmail.com

Prof. Vikram Raut
WCEM Nagpur University
Email: vikramrautcse@gmail.com

Abstract : Recently in many areas like facebook , watsapp and many more social networking site many users upload their personal data, video ,voice recording. This paper proposed and idea of encryption – decryption of any file which user s going to upload on site. The specific site which are providing such kind of functionality needs to adopts this method to secure user data for privacy preserving.So that any hackers or indruder can not directly hike your data. If in exceptional cases someone even hacks the data they will not get the actual file they will only get the encrypted file withoud having a decrypt key for the data. So they never see an original file.This will improve the data security over internet uses. The proposed system wiil used a special Advanced Encryption Standard, also known by its original name Rijndael for secure encryption decryption of audio ,video as well as data files.

Keywords *:Rijndael Algorithm , Infrastructure, Internet , DES , AES , Encryption , Decryption.*

*****

I. INTRODUCTION

Now a days, the Security of data over a network traffic is the most important and challenging aspect in web application. With the passage of each day, increasing number of users share their personal data, voice recording ,video fileas in different fields, such as legal, medical, financial, social networking, bank transaction with internetworking and information transfer which are meant to be confidential. These information transfer should be secure and needed a special treatment. Cryptography is the best means for secure transmission. Cryptography is the study of Secret means (crypto) and Writing means (graphy). There is cryptographic processes of encryption and decryption of data these processes are done with the help of cryptographic symmetric and asymmetric keys. In the symmetric keys, client and server both use the same key for encryption and decryption. And in the asymmetric keys, both client and server use the different keys for their encryption and decryption of processes. Now a days, due to network traffic to maintain the security of the data most of the companies are shifting towards the AES (Advanced Encryption Standard) based encryption security of data. There are basically 3 types of encryption keys in AES that is 128 bit encryption, 192 bit encryption and 256 bit encryption which uses the 10, 12 and 14 rounds. The data which is stored in the remote servershould be encrypted by before storing it on the server. As with the growth of

Internet technologies almost all sizes of are already using the remote server.Now a days number of users store and share their personal data ,photos,videos, audio clips on the remote server. In the proposed scheme the end user is encrypted by using the AES 128, 192 and 256 bit encryption algorithm which is secure as compared to other encryption techniques and shows the time which is taken by the technique for the encryption and decryption of data. And authorized user can share their data to other authorized user. A comparative study based on analysis of simulation time for encryption and decryption of data is done and found that AES algorithm is better than DES and all other encryption algos.

II. LITERATURE REVIEW

[1] Narender Tyagi in 2014, proposed a theoretical study on cryptography to provide secure transmission again malicious people who were trying to harm and gain some information. In paper comparison of algorithm DES, 3DES, AES, Blowfish have been made and also show how these algorithm consume computer resources like memory, battery, CPU time. The parameters for comparison are block size, speed, key size. The author concluded that blowfish is the most secure and provide superior performance as compared to other algorithm. 3DES have least performance.

[2] Anjula gupta in 2014, proposed that cryptography is a greek word and combined of two words crypto-—secret‖ and graphy-—writing‖. In the paper cryptography is defined and comparison had been done between various symmetric algorithms DES, AES, 3DES, IDEA, blowfish and asymmetric algorithm RSA. This paper is mainly for beginners and concluded that RSA is the securest and RSA can be combined with other algorithms like DES&RSA, AES&RSA, blowfish&RSA, Diffie Hellman&RSA to improve security.

[3] Ashwini.R.Tonde in 2014, proposed that how much cryptography is important and applied to security measure and discussed the AES algorithm. The author's AES design is coded with very high speed integrated circuit hardware descriptive language. The design use loop approach and key size is 128-bit. The AES design have low latency and high throughput. The author concluded that AES is not so much costly and perform high speed secure transmission.

[4] Obaida in 2013, proposed that most of the algorithms

encounter some problems like lack of robustness and time added to packet delay to maintain security. The author show how security goals were enhanced with a new approach of encrypting and decrypting data that maintain security on channel of communication which makes it difficult for malicious user to know the pattern and increases the speed of encryption and decryption. This is a new approach as it is complex for encryption and decryption. This algorithm was tested against different attacks and resulted in secure cipher. Hence it is a good approach as alternative to existing algorithms and application because it has high level of security and small time for encryption and decryption.

[5] Mohammad Soltani in 2013,proposed a new robust cryptography algorithm to enhance security in the Symmetrickey producing algorithm. The features of cryptography algorithm defined as the ability to encode the secret file in successive loops, changing the physical structure of the secret file, the number of keys have no limitation, Creating five keys at each stage of cryptography, secret file is stored at one of the keys at each loop of cryptography,all keys are independent in all loops of encrypting and decrypting, for making the keys dependent on each other and to encrypt the secret file by each of them, there are 2 independent algorithms of type of algorithm needed to make the keys inter dependent by the user, big changes in the physical structure of the encrypted file In the case of false decryption and to make the resulting keys and encryption file unique after the cryptography.

[6] Amritpal Singh in 2013,proposed the main characteristics that differentiate and identify encryption algorithm from another are their ability to secure the protected data against attacks and the speed and effectiveness of securing the data. This review paper provides study of comparison between four widely used encryption algorithms DES, 3DES, AES and RSA on the basis of their ability to protect and secure data against attacks and speed of encryption/decryption.

[7] Pranab garg in 2012, proposed the cryptographic algorithm that fulfil condition of message authentication, digital signature and integrity. This system can be for block / stream format but the largest constraint is key length. When all these algorithms are taken at once , the performance and security level can be increased. In this scheme to generate private key CDMA approach can be used. Every user will be provided an unique number called PN Number, which is generated randomly at receiver and that PN Number is not known to unknown and any other user. This same PN number is sometimes used to decode the cipher text.

[8] Navraj Khatri in 2012, have proposed secure electronic data structure & the difference between AES and other algorithms by increasing key size by 200 bits. The performance of the algorithms is measured by the power consumption of size of data in encryption and decryption.The paper finally conclude the idea that measure the level of security by having larger block with 200 bits than 128 bits and block is made of 5*5 matrix unlike 4*4 matrix in AES, it require more multiplication and transformation of the matrix. In this research paper the CPU cycle to encrypt is 30 percent less than other algorithms and the CPU cycle to decrypt are more than 20 percentof the other algorithms. Therefore this model is more secure and used when high data rate communication is required.

[9] Shivangi Goyal in 2012, proposed a idea of cryptography, to where it is applied and its uses. It proposed an advanced user authentication,confidentiality, integrity and electronic signatures of data. This algorithms in cryptography use mathematics for encryption and decryption to secure data.

[10] Akhil kaushik in 2010, have proposed a new algorithm BEST(block encryption standard for transfer of data) which is developed the computer technologies C++ and JAVA .Resulting algorithm is compared with Advance Encryption Standard and Data Encryption Standard and shows that it can easily protect from Replay attacks and Brute force attacks and, also it can change the key format when send it from one sender to reciever.

III.PROPOSED SYSTEM

In this, we are using AES encryption process using encrypted keys are very complex combinations. The purpose of applying AES technique is to completely secure the records and abstain from the utilization of single secret code. The randomly created secret keys are exceptionally unpredictable combination along these lines client won't retain it exactly. In this system user first register in to the system then if he/ she is an authorized user and having an encrypted key then only he can upload a file to a system these files are stored in an encrypted format, our system proposed a advance types of file including Text,word,pdf,audio and video files. User can able to download the files if is having decrypted key, for this user have to send the request for the access key to the administrator who upload that file , we are providing the actual data to the authorised users only.This provides security to the person to protect their information from others. If user needs to download any file they need to request that particular file, then this request will pass to auditor then automatically user get an secret key to their mail and during download verification will be required. The secret code sent to their mail will be given in the verification part, then the file will downloaded. Advantages: The passkeys are very complex thus user will not be able to fully memorize them.

IV. CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms are basically called as encryption algorithms,contains mathematical procedures for encryption

data.there are numerous encryption algorithms techniques having different strengths. Mainly strength of algorithm depend on computer system used for generation of keys. Secret information is made with the help of hash functions, digital signature and key management. Various algorithmic techniques are:

A. DES (Data Encryption standard):IBM(International Business Machines)Corporation in late 60's found DES,which was result of cipher called LUCIFER and next version of LUCIFER was proposed as new encryption algorithm by NBS(National Bureau of standard) and finally in 1977, it is adopted as data encryption standard(DES). DES is symmetric block encryption algorithm and uses 64-bit key,in which 56-bit make independent key and remaining 8bit are for detection of errors. Operation included in DES are permutation and substitution. Permutation are used in expansion of key part. Decryption in DES is just similar to encryption part but in reverse order and resulted output is a block of 64 bits.

B. 3DES(Triple DES):It is also called TDEA(Triple Data Encyption Algorithm),works by applying DES three times, which increases encryption performamnce as well as enhance security. Key length is 192-bit. The procedure is same as data encryption standards, data is encrypted with first key, by second key the data gets decrypted and by third key again the data gets encrypted.

C. AES: The Advanced Encryption Standard (AES) is the United State Government standard for symmetric encryption. AES is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (cipher text), or decrypts a 128-bit block (cipher text) to a 128-bit block (plaintext).AES uses a cipher key of length either 128or 192, or 256 bits. Hereafter encryption/decryption with a key of 128, 192, or 256 bits in cipher is denoted AES128, AES192, AES256.The notation AES128, AES192, AES256 process the data block in 10,12,14 iterations respectively of a pre-defined sequence of transformations, which are also called ―rounds‖ (AES rounds) for short. The rounds are identical except the last one, which slightly differs from the others (by skipping one of the transformations). The rounds operate on two 128-bit inputs: State and Round key. Each round from 1 to either 10or12or14 uses a different round keys. Eithe10or12or14 round keys are redeemed from the cipher key by the algorithm called ―Key Expansion‖ .AES algorithm is not dependent of processed data, and can be easily carried out without depending on any encryption or decryption phase

D. Blowfish :Blowfish is a public domain encryption algorithm, designed by Bruce Schneider in 1993 as an alternative to already existed algorithm. It's key length vary from 32-bit to 448-bit. Any attack is not successful on blowfish.

E. IDEA(International Data Encryption Standard Algorithm):It is also a block symmetric algorithm and operate on 64bit text block and key size is 128-bit.IDEA contains algebraic operations like XOR,addition modulo216 and multiplication modulo 216+1. This algorithm efficiently work on 16-bit processor. It is based on substitution & permutation but not include S-Boxes.

F. RSA: The full form of RSA is named on mathematicians who discovered it, Ron Rivest, Adi Shamir and leonard Adleman in 1997. Variable size key and encryption block is used to make public and private key. RSA is the most secure and convenient.

How safe is AES 256 bit encryption?

AES-256 is used among other places in SSL/TLS across an Internet. It's is among the top encryptions schemes. In theory it's not crack able since the combinations of keys are massive. Although NSA has categorized this in Suite B, they have also recommended to use higher than 128-bit key encryption scheme. AES encryption algorithm is an iterative rather than Feistel cipher scheme for encryption and decryption. It is based on the substitution of the permutation network. It also comprises of a series of linked operations, some of them involve replacing of inputs by some scpecific number of outputs and others have involve shuffling of the bits around the permutations. AES performs its operations based on the bytes rather than the bits. Hence, AES algorithm treats the 128 bits plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing a matrix − Unlike DES, number of rounds in AES is variable in size and depends on the length of key which are using. AES algorithm uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Algorithm

Step 1: Authentication Process

a. Authentication of user and grant access rights to the user for new user.
b. User send request to administrator to provide a key for data accessing purpose,
c. Administrator will send the key to the user.

Step 2: Uploading file

a. Data owner can upload number of files (f1, f2….fn) to the server.
b. Internally system will encrypt the files and send to the cloud server.
c. f and f' will be encrypted.
d. Upload encrypted f and f' to server.

Step 3: File Retrieval

a) User can search the data uploaded on server.
b) To retrive the specific file user have to enter a valid key provided to them.
c) f' will be decrypted to f.
d) Download encrypted f'to f to the local machine.

An AES algorithm to provide efficient multi-keyword ranked search .

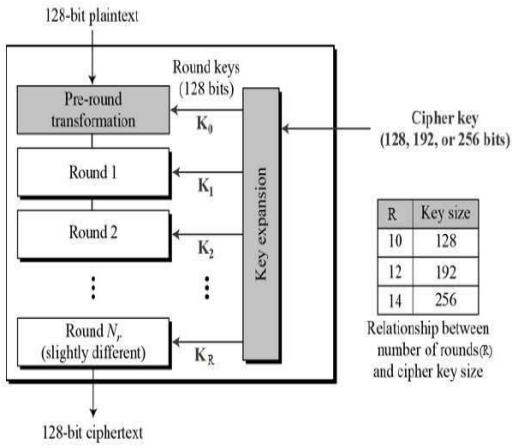
The secure **Rijndael algorithm** is utilized to encrypt the index and query vectors.
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher

128-bit data,

- 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details



Why AES Encryption Algorithm?
A difference has been made between the various key sizes of AES and DES algorithm on different key sizes and finds out that AES performs better and which variation of AES performs better in all file size is shown in table 2.

Table 2 Comparison of AES & its variations with DES

Table 2 Comparison of AES & its variations with DES

File Type	File Size	AES 128	AES 192	AES 256	DES
.txt	1 KB	1685	1450	1216	1794
.jpg	61 KB	1894	1779	1669	1990
.jpg	3.15 MB	4958	4820	4103	5463
.pdf	11MB	10982	9991	8384	11481
.pdf	57.6 MB	24507	19095	18735	37034
.mp4	1.15 GB	1015168	976930	816156	1173966

From the above table as given from the Comparison, (AES) performs better than (DES) and also the variation of AES that is AES 256 performs the encryption and decryption in less time as compared to its other variation and other algorithm.

V. PROPOSED METHODOLOGIES

Techniques/tool required

Hardware Requirements:

- System : Pentium IV 3.5 GHz.
- Hard Disk : 40 GB.
- Monitor : 14’ Colour Monitor.
- Ram : 2 GB.

Software Requirements:

- Operating system : Windows 7 Ultimate.
- Coding Language : ASP.Net with C#
- Front-End : Visual Studio 2013 and advance vesrions of visual studio.
- Database : Sql Server 2012
- Other Advance Technologies : Ajax , Javascript ,CSS

Module

1. Data Users
2. Cipher text Module

Data users:
Data user is the user of the system and are having file/data that ,he wants to outsource to the server .
In first step user need to register in to the system after successful registration ,user request will go to administrator to provide the access to the user,once admin will grant(send authentication mail to user email id) an access to user can able to upload/ fetch encrypted documents from server. Then, the data user can decrypt the documents with the shared secret key.

Cipher-text Module:
In this model, we have perform the encryption decryption of the files , in our system cloud server only accept the encrypted data with the authorised user can decrypt the file Encryption decryption performed using AES Rijndael algorithm.

VII. CONCLUSION AND FUTURE SCOPE

Sensitive information of privacy preservingof data will be present in the forms of analysis information similar to Social Networking , Medicine - hospital cost analysis, prediction hospital cost analysis, drug side effects, and automotive diagnostic expert systems genetic sequence analysis. Finance - credit assessment, fraud detection stock market prediction, Marketing/sales - sales prediction, product analysis, target mailing, identifying unusual behavior, buying patterns, Scientific discovery, Knowledge Acquisition. In addition to that, privacy preserving data

mining by implicit function theorem kind of approach will also be used in distributed data mining to protect information of privacy and applied for business

VIII. REFERENCES

[1]. K. Ren, C.Wang, Q.Wang et al.,"Security challenges for the public cloud," IEEE Internet Computing, Vol. 16, No. 1, pp. 69–73, 2012.

[2]. S. Kamara, K. Lauter,"Cryptographic cloud storage," In Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[3]. C. Gentry,"A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4]. D. X. Song, D. Wagner, A. Perrig,"Practical techniques for searches on encrypted data," In Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[5]. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," In Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006

[6]. Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[7]. Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.

[8]. For AES Cryprographyfrom https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[9]. Larry A. Dunning, Member, IEEE, and Ray Kerman "Privacy Preserving Data Sharing With Anonymous ID Assignment" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013

[10]. Anita Rajendra Zope, Amarsinh Vidhate, and Naresh Harale "Data Mining Approach in Security Information and Event Management" International Journal of Future Computer and Communication, Vol. 2, No. 2, April 2013

[11]. S. Subramaniam, T. Palpanas, D. Papadopoulos,V. Kalogeraki, and D. Gunopulos, "Online outlier detection in sensor data using non-parametric models, in VLDB", 2006

[12]. Lu-An Tang, Jiawei Han, and Guofei Jiang, "Mining Sensor Data in Cyber-Physical Systems" TSINGHUA SCIENCE AND TECHNOLOGY ISSNll10070214ll01/11llpp225-234 Volume 19, Number 3, June 2014

[13]. Social Networking Secure Against Malicious Users", 2011 Ninth Annual International Conference on Privacy, Security and Trust.

[14]. Chris Clifton, Murat Kantarcioglu,Jaideep Vaidya, Xiaodong Lin, Michael Y. Zhu, "Tools for Privacy Preserving Distributed Data Mining"