Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 3, March-2017

Mobile Data Encryption and Decryption Application Based On Cloud

Chirayu M. Shinde[1], Shubham Singh[2], Himanshu Vanmali[3]

[1]*B.E COMPUTERS, THEEM COE*
[2]*B.E COMPUTERS, THEEM COE*
[3]*B.E COMPUTERS, THEEM COE*

Abstract— In recent years, fast evaluation of digital data exchange occurs. Because of this protection of information is very vital in data storage and transmission process. Protection of internet banking account passwords, email accounts password etc. needs text protection in digital media. During industrial and research processes, image transmission and storage needs image security in the same way. The National Institute of Standards and Technology (NIST) have taken steps for a process to develop Federal information Processing Standard (FIPS) which should be most flexible, secure, fast and which can replace Data Encryption standard(DES). This new standard is known by name Advanced Encryption Standard (AES). Characteristics of data are depends on its types. Thus same security technique cannot be used for all data types. Similar techniques cannot be used to secure images as well as text from unauthorized access as images have huge data sizes and also has real time constrain problems. However with few changes in method, AES can be used to give security to image as well as text. In this project we have implemented encryption and decryption for text, image, audio and also video using AES.

Keywords— Advanced Encryption Standard (AES), Encryption, Decryption, Cloud, FIPS, NIST, Rijndael

I. INTRODUCTION

Now a day security of digital information is most important issue due to increasing use of computers. Intruder is an unauthorized person who reads and makes modifications in the information while transmission is occurring. This activity of unauthorized person is called intrusion attack. To overcome such attack data may be encrypted to some formats that is unreadable by an unauthorized person. AES is mainly advance version of data a encryption standard (DES).

From January 1997 efforts towards developing Advanced Encryption Standard were started. AES is a symmetric key encryption algorithm. AES to be better than DES, NIST made a worldwide public call. At initial stage 15 algorithms were selected. MARS, RC6, Rijndael, Serpent and Two fish were the only 5 algorithms selected after doing an detailed analysis. The all 5 final algorithms were then determined and tested to be qualified as the algorithm for AES [3]. Rijndael was selected as the algorithm for AES after the detailed test and analysis. Features of Rijndael are: It provides high security, mathematical soundness, resistance to all known attacks, high encryption speed, worldwide royalty free use, suitability across wide range of hardware and software.

II. INTRODUCTION TO AES

The Advanced Encryption Standard (AES) is a symmetric key cryptographic algorithm also known as Rijndael which is a specification for the encryption of electronic data which is established in 2001 by the NIST. The AES is a successor algorithm for Data Encryption Standard (DES).The DES became vulnerable to brute force attacks, and due to this NIST announced the starting development of AES which will overcome the drawbacks of DES in the year 1997.The AES was established by the U.S government in the year 2001 and now is used worldwide. For AES, the NIST selected 3 members each of block size 128 bits but with different key lengths: 128,192 and 256 bits. The AES algorithm is a symmetric key algorithm that is it uses the same key for both encryption and decryption process. After the approval by the Secretary of Commerce on May 26, 2002 AES became more effective as a Federal government standard. AES is available in many different encryption packages. It is also included in ISO/IEC 18033-3 standard. AES is the first and only publicly accessible cipher which is approved by the National Security Agency (NSA). AES allows the data length or plain text size of 128, 192 and 256 bits. AES consists of multiple rounds for processing different key bits like 10 rounds for processing 128-bit keys, 12 rounds for processing 192-bit keys and 14 rounds for processing 256-bit keys.

All Rights Reserved, @IJAREST-2017

III. SYSTEM RELATED WORK

Text encryption and decryption by AES:

The number of rounds are 10, for the case when the encryption key is 128 bit long(as mentioned earlier, 12 rounds for processing 192-bit keys and 14 rounds for processing 256-bit keys). The given plaintext is divided into 128 bit block as consisting of a4*4 matrix of bytes . Thus, the first four bytes of a 128 bit input block gets situated in the first column in the 4*4 matrix of bytes. The next four bytes gets situated in the second column, and so on. AES operates on a 4*4 column- major matrix of bytes; called as state array. AES has also notion of a word. A word consists of four bytes that is 32 bits .

Table1.Key block round combinations

Algorithm	Block size(Nb words)	Key Length (Nk words)	Number of rounds(Nr)
AES 128	4	4	10
AES 192	4	6	12
AES 256	4	8	14

Before any round-based processing for encryption can begin each byte of the state (plaintext) is combined with the round key using bitwise XOR operation. Nr stands for number of rounds. AES divide plaintext into 16 byte (128 bit) blocks, and treats each block as a 4*4 State arrays. It then performs four operation in each round consists of several processing steps like substitution step, and the addition of the round key. Except for the last round in each case, all other rounds are identical. Final round doesn't have (MixColumns) it includes of only SubBytes, ShiftRows and AddRoundKey. The process of transforming the cipher text back into original plaintext using same encryption key is called decryption process of AES, during decryption process rounds are reversed.

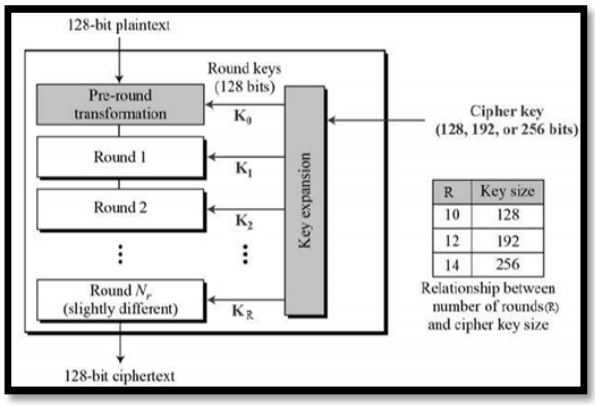

Fig No 01: AES Encryption Algorithm for text

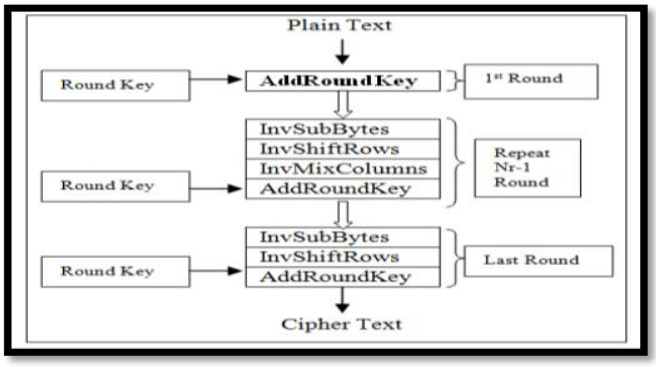

Fig No 02: AES Decryption Algorithm for text

Decryption occurs through the function AddRoundKey (), plus the inverse AES functions InvShiftRows (), InvMixColumns () and AddRoundKey () does not require an inverse function, as it simply XORs the state with the subkey.

All Rights Reserved, @IJAREST-2017

- **Image Encryption and Decryption:**

The Image encryption and decryption is based on AES key expansion techniques. The steps involved in the AES key expansion technique are as follows:

Key Selection: The users who want to encrypt and decrypt the image file agrees upon a 128 bit key. For encryption and decryption this key will be used.They must share the key in very secure way as it is symmetric key encryption method. The key is shown as blocks k[0],k[1]...k[15]. Here each block is 8 bits long (8*16=128 bits).

Generation of Multiple keys: The users can now independently generate the keys required for the process using the Modified AES Key Expansion technique. This is a one- time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

Encryption: Encryption of image file is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte oriented transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round Key.

Decryption: The decryption process is similar as encryption, but we use Inverse Sub Byte Transformation. The whole AES structure is sketched in Fig below.

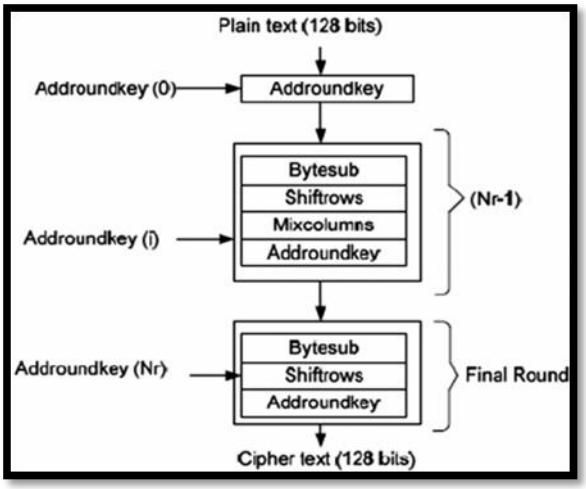

Fig: Structure of AES algorithm

IV .CONCLUSION

In the older techniques these cryptographic algorithms are implemented in the Single system environment. Now due to availability of high performance computing techniques, similar test has been conducted in the single system environment i.e. local environment and also in the Cloud environment. From the observed results, and based on the considered parameters, storing the mobile data in cloud increases the efficiency. Also the results reveal that AES algorithm qualifies better than other algorithms in Mean processing time and combination of MD5+ECC+AES algorithm qualifies better than others in Speed-Up ratio. Considering only these parameters, other performance measures like Turn-around time, Throughput are planned to be included in the future work.

A cloud storage web application which is based on AES algorithm and a new variant of the RSA encryption algorithm has successfully been implemented. The concept provides a high level of security; encryption and decryption are both performed on the client's side. The decryption key is neither stored on the user's machine, nor has the key to be typed in manually. Though, there are some limitations of this implementation, especially that only text files can be saved on the server. For a widespread use of the application, a user should be able to save all types of files. This could be realized by creating a standalone program instead of using the browser, since a JavaScript file executed in a browser is currently not able to save to the file system. This is necessary, because the data received by the server has to be processed on the client for decryption.

All Rights Reserved, @IJAREST-2017

V. REFERENCE

[1]. Kumar, K., Lu, Y-H.: Yung-Hsiang Lu: Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? Computer 43(4), 51– 56 (2010)
[2] Simoens, P., De Turck, F., Dhoedt, B., Demeester, Remote Display Solutions for Mobile Cloud Computing. Computer 44(8), 46–53 (2011)
[3] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review," Journal of Emerging Trends in Computing and Information Sciences, 2012.
[4]. Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication," IJCST Vol. 2, Issue 2 June 2011.
[5]. Shahryar Shafique Qureshi1, Toufeeq Ahmad1, Khalid Rafique2, Shuja-ul-islam3 "Mobile cloud computing as future for mobile applications– implementatio methods and challenging issues"-2011.
[6]. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD
[7]. 29. Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18
[8]. Pearson, S., Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing", in Proceedings of the 1st International Conference on cloud computing. 2009, Springer-Verlag: Beijing, China. p. 90-106.
[9]. Wang, Q., et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", in Computer Security –ESORICS 2009, M. Backes and P. Ning, Editors. 2009 springer Berlin / Heidelberg. p. 355-370.
[10]. Hoang T.Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A Survey of Mobile Cloud Computing: Architecture Applications, and Approaches .In Wireless Communications and Mobile Computing 2011.
[11]. Wei Ren, Linchen Yu, Ren Gao,Feng Xiong.Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing. Tsinghua Science And Technology, ISSNl1007-0214ll06/09llpp520 528.Volume 16, Number 5, October 2011.
[12]. Liu Q, Wang G, Wu J. Efficient sharing of secure cloud storage services. In: 2010 IEEE 10th International Conference on Computer and Information Technology (CIT10). Bradford, West Yorkshire, UK, 2010: 922-929.

All Rights Reserved, @IJAREST-2017