International Journal on Recent Researches
In Science, Engineering & Technology
(Division of Computer Science Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.
It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper Available
online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 5, Issue 4,
April 2017

JIR IF : 2.54
DIIF IF :1.46
SJIF IF: 1.329

AN AGGREGATED AES ALGORITHM FORPREVENTING KEYLEAKAGE PROBLEM IN CLOUD COMPUTING

P.Gowthami[1],M.Nishanthi[2], B.Indhumathi[3], M.Navaneethakrishnan[4]

[1,2,3] Department of Computer Science and Engineering, St. Joseph College of Engineering, Chennai, India.blessybless1995@gmail.com

[3] Professor & HOD, Department of Computer Science and Engineering, St. Joseph College of Engineering, Chennai, India.

mnksjce@gmail.com

Abstract: Advanced Encryption Standards (AES) algorithmwhich is used to provide security, But it has challenges about Key Leakage problem along with sidechannel attacks.AES Algorithm which is used to provide more securityalso used toprevent attacks.Security is amajor problem inrecent Years. Several researchers for doing their research in information security domain to improve their security through their information sharing.The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data to be encrypted. This array we call the state array.The block to be encrypted isjust a sequenceof128 bits. AES workswith byte quantities so we first convertthe 128 bits into 16 bytes. We say "convert," but, in reality, itisalmost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensionalbyte array of four rows and four columns. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. The problem of secure many to many communications in large-scale network files systems that support parallel access to multiple storage devices. That is, we consider a communication model where there are a large number of clients (potentially hundreds or thousands) accessing multiple remote and distributed storage devices (which also may scale up to hundreds or thousands) in parallel.

Keywords: Encryption, Decryption, AESAlgorithm, Cloud Computing.

I.INTRODUCTION

The companies that may have files that require access by multiple employees daily. The problemof secure many to many communications in large-scale network files systems that support parallel access to multiple storage devices. That is, communication model where there are a large number of clients (potentially hundreds or thousands) accessing multiple remote and distributed storage devices (which also may scale up to hundreds or thousands) inparallel. Particularly, we focus on how to exchange key materials and establish parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS) the current Internet standard in an efficient and scalable manner. The development of pNFS is driven by Panasas, Netapp, Sun, EMC, IBM, and UMich/CITI, and thus it shares many common features and is compatible with many existing commercial/proprietary network file systems. Networking is the practice oflinking multiple computing devices together in order to share resources. These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Without theability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely usefulcapability. Perhapseven more valuable is the ability to access the same data files from variouscomputers throughout a building. This is incredibly useful for companies that may have files that require access by multiple employees daily. Before applyingthe algorithm to the data, the block and key sizes must be determined. AES allows for block sizes of 128, 168, 192, 224, and 256 bits. AES allows key sizes of 128, 192, and 256 bits . The standard encryption uses AES-128 where both the block and key size are 128 bits. The important features confidentiality, authentication,integrity andnon –repudation. The cryptography is arts or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.In this we are usingencryption and decryption .Decrption isthe process of converting information or data into a code, especially to prevent unauthorizedaccess**.**Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

II.REVIEW AT RELATED WORKS

Komal Kate et al [1] presented a usefull of Cloud storage can provide good accessibility and reliability, strong protection and low cost. In data privacy , there is no traditional technique of authentication because unexpected previlages will expose all data. As a result, the deligation can always get an aggregate key of constant size. It is a storage online in cloud which is accessible frommultiple and connect resources.

BharatiMishra et al [2] presented a usefull of file encrypting tools like Veracrypt, AxCrypt, Boxcrypt, are place to encrypt files. But theyhave implemented AES and RSA encryption algorithm. Files are stored in cloud storage systems in plain text format.Again multiple copies of the files are maintained in multiple locations for faster access and availability.

Charles Bouillaguet et al [3] presented a usefull of to demonstrate the strengh of the tools, we allow toautomatically discover new attacks on round-reduced AES with very low data complexity, and to find improved attacks on the AES.The tools can be used in the context of fault attacks.The system is vulnerable to various types of Network Attacks.Versatile and powerful algorithms for searching guess-and determine and meet-in-the-middle attacks on some byte-oriented symmetric primitives .Algorithms exploit the algebraically simple byte-oriented structure of the AES.

MichelAbdalla et al[4] presented a process of password-based encrypted key exchange are protocols that are designed to provide pair of users communicating over an unreliable channel with a secure session key even when the secret key or password shared between two users is drawn from a small set of keys. In proposed scheme, two simple passwords based encrypted key exchange protocol based on that of Bellovin and Merritt.

Sai Kumar et al [5] presented a process of Passwords are one of the most common causes of system crashes, because the low entropy of passwords makes systems vulnerable to brute force guessing attacks. Due to new technology passwords can be hacked easily. Automated Turing Tests continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users.

III.BASIC CONCEPT OF AES

Advanced Encryption Standard(AES) is a symmetric key block cipher published by the NIST in December 2001. The Advanced EncryptionStandard (AES), also known by its original name Rijndael isa specification for the encryptionof electronic data .

AES is based on a design principle known as a substitution permutation network, a combination of both substitutionand permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Fiestal network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, theRijndael specification per specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 coloumn major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a particular finite field.The key size used for an AES cipher specifies the number of repetitions oftransformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself.A setof reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

A. Evaluation Criteria For AES

Evaluation criteria forAES are Security,Cost,Algorithm and implementation characteristics.The securityrefers to the effort required cryptanalyse an algorithm.Following parameters are also consider for evaluation The actual security compared to other submitted algorithms. Randomness is extent to which the algorithm output is indistinguishable from a random permutation on the input block. The soundness of the mathematical basis for the algorithm's security. Other security factors raised by the public during the evaluation process.

B. AES OPERATIONS:

a. AddRound Key

Many blockciphers are defined by specifying a round and then running that specification multiple times. For example, in AES, a round consists of the operations.That is one round and, to get AES, you run that multiple times (plus some setup and some post-processing).

Thus a round is defined by each cipher and typically consists of a number of building blocks that are composed together to create a function that is run multiple times.

b. Mix Coloumns

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns functiontakes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. The multiplication operation is defined as a multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x1B should be performed if the shifted value is larger than 0xFF.

c. Shift Rows

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged.Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state.

d.Sub Bytes

This Sub Bytes transformation is a simple table lookup. Only one S-Box for the whole cipher, a 16x16 matrix of byte values, that contains a permutation of all possible 256 8-bit values. Each individual byte of state is mapped into a new byte in this way. Leftmost 4 bits of the byte are used as a row value; rightmost 4-bits used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output values.

e. Key Leakage Problem

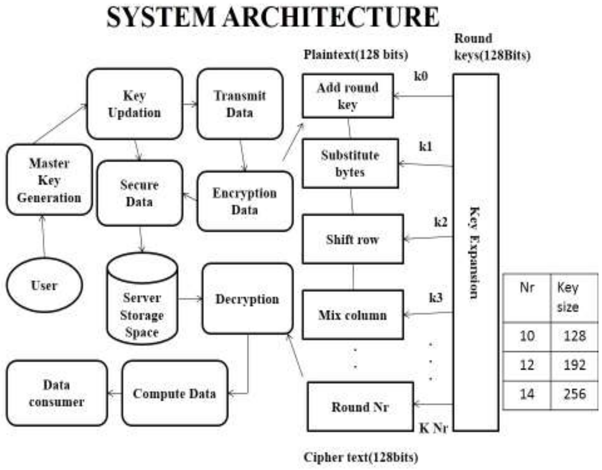
Key leakageproblem happens whenever a system that is designed to be closed to an eavesdropper reveals some information to unauthorized parties nonetheless. For example, when designing an encrypted instant messaging network, a network engineer without the capacity to crack encryption codes could see when messages are transmitted, even if he could not read them.

f. Proposed System

It uses AES algorithm , which is used as Key size as32- 448 bits.It provides more security along with reduce attacks. In this it improves the security and to reduce the key leakage problem.

IV.SYSTEM ARCHITECTURE

Architecture diagram shows the relationship between different components of the system.This diagram is very important to understand the overall concept of the system.They are heavily used in the engineering world in hardware design, electronicdesign, software design and process flow diagram.



The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data to be encrypted. This array we call the state array.

You take the following aes steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array
4. Add the initial round key to the starting state array.
5. Add the initial round key to the starting state array.
6. Add the initial round key to the starting state array.
7. Add the initial round key to the starting state array.

Steps InAES Algorithm Process

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D0 .

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- SubBytes
- ShiftRows
- MixColumns
- XorRoundKey

The details of these operations are described shortly, but first we need to look in more detail at the generation of the Round Keys, so called because there is a different one for each round in the process. In the first nine rounds of the process, the four operations are performed in the order listed. In the last (tenth) round, the MixColumns operation is not performed and only the SubBytes, ShiftRows, and XorRoundKey operations are done.

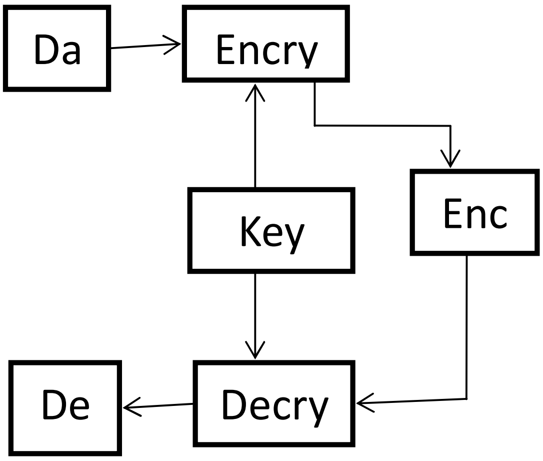
V. MODULES DESCRIPTION

A.Key Generation Module:

1) Key generation is the process of generating keys for cryptography. The key is used to encrypt and decrypt data whatever the data is being encrypted or decrypted.

Related algorithms – Symmetric Key algorithm

2) Symmetric-key algorithms use a single shared key keeping data secret requires keeping this key secret. Public-key algorithms use public key and a private key.



B.Stateless KeyUpdation Module:

1) Key-up dating assumes that the two communicating parties share only the secret key and a public variable (nonce).

2) There is no shared secret state between them. This updating mechanism is required whenever there is no synchronization between the two communicating parties during initialization of a secret channel.

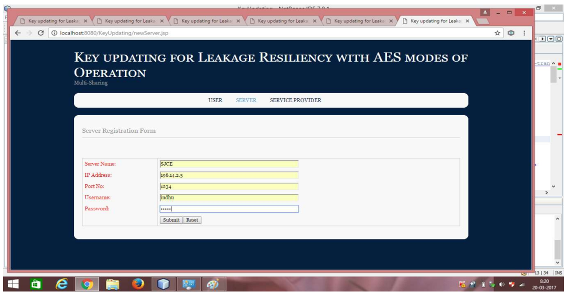
C.Statefull KeyUpdation Module:

Stateful key-updating assumes that the two communicating partiesshare a common secret state (other than the key).

They both can update the secret key into a new key without requiring any external variables.

VI .Performance and Results

A.Registration Module:



localhost:8080/KeyUpdating/newServer.jsp

KEY UPDATING FOR LEAKAGE RESILIENCY WITH AES MODES OF OPERATION

Multi-Sharing

Server Registration Form

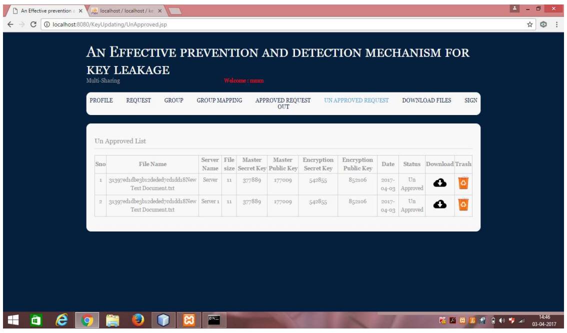
Server Name:	SJCE
IP Address:	196.14.2.5
Port No:	1234
Username:	indhu
Password:	•••••

8:20
20-03-2017

Fig 6.1

B.USER UNAPPROVED LIST

In these the user only decide to whom to view the data, because the user send the master secret key ,to unapproved the list.



localhost:8080/KeyUpdating/UnApproved.jsp

AN EFFECTIVE PREVENTION AND DETECTION MECHANISM FOR KEY LEAKAGE

Multi-Sharing

Welcome : mmm

Un Approved List

Sno	File Name	Server Name	File size	Master Secret Key	Master Public Key	Encryption Secret Key	Encryption Public Key	Date	Status	Download	Trash
1	31397ed1dbe3b12deded7cd1dd18New Text Document.txt	Server	11	377889	177009	542855	852106	2017-04-03	Un Approved	⬇	🗑
2	31397ed1dbe3b12deded7cd1dd18New Text Document.txt	Server 1	11	377889	177009	542855	852106	2017-04-03	Un Approved	⬇	🗑

14:46
03-04-2017

Fig 6.2

The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codes the platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed.

VII. CONCLUSION

Two communication parties can share their secret key over public channel. Enough security is achieved in the key leakage problem using an AES algorithm process. In these we canprevent from Side channel analysis attack.By modelling the side-channel analysis problem adequately, SASCA bring themissing link between standard DC distinguishers and analytical strategies forkey recoveries. As a result and for the time, we are able to anciently exploitthe probabilistic information of all the leaking operations in a software implementation. Our resulting attacks are optimal in data complexity and ancient intime and memory. Yet, we note that the tools exploited in this instantiationof SASCA can certainly be improved. For example, the BP algorithm performstoo many computations for our needs. Indeed, it propagates every distributionthroughout the factor graph whereas in practice, we are mostly interested inthe key. Hence, further works could exploit the propagation of messages onlytowards the schedule

VII. REFERENCES

[1] K. Tiri et al., "Prototype IC with WDDL and differential routing—DPA resistance assessment," in Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2005, pp. 354–365.

[2] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 69–88.

[3] F.-X. Standaert, O. Pereira, Y. Yu, J.-J. Quisquater, M. Yung, and E. Oswald, "Leakage resilient cryptography in practice," in Towards Hardware-Intrinsic Security. Berlin, Germany: Springer-Verlag, 2010, pp. 99–134.

[4] Y. Dodis and K. Pietrzak, "Leakage-resilient pseudorandom functions and side-channel attacks on Feistel networks," in Proc. 30th CRYPTO, 2010, pp. 21–40.

[5] S. Faust, K. Pietrzak, and J. Schipper, "Practical leakage-resilient symmetric cryptography," in Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2012, pp. 213–232.