IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Enhancing Distributed Data Storage Security for Cloud Computing using AES algorithm

Vasant S. Kakade[1], Akshay Kirve[2], Ankush Bhoir[3], Sagar Kadam[4]

Computer Engg Dept., Dr. DYPCE Ambi, Pune, India [1,2,3,4]

Abstract: Now an afternoon's cloud computing is used in lots of areas like industry, military schools etc to storing large amount of statistics. We are able to retrieve facts from cloud on request of person. To shop records on cloud we should face many troubles .To offer the answer to those troubles there are n wide variety of ways .Cryptography and steganography techniques are more popular now a day's for facts safety. Use of a unmarried algorithm isn't effective for high degree safety to data in cloud computing. On this paper we have introduced new security mechanism the usage of symmetric key cryptography set of rules and steganography .in this proposed gadget AES set of rules are used to offer block sensible safety to records. This set of rules key length is 128 bit.. LSB steganography method is introduced for key information security. Key statistics includes which part of file is encrypted the usage of by which set of rules and key .file is splited into 8 parts. Each and each a part of record is encrypted using extraordinary set of rules. All parts of file are encrypted concurrently with the assist of multithreading technique. Records encryption Keys are inserted into cowl photo the use of LSB approach. Stego picture is ship to valid receiver the use of e-mail .For record decryption reason opposite manner of encryption is applied.

Keywords: Privacy Preserving, AES Algorithm, Hash Code, Encryption, Cloud Computing, Integrity.

I. INTRODUCTION

Cloud computing model is extremely exciting model especially for business peoples. Several business peoples have gotten attracted towards cloud computing model attributable to the options simple to manage, device freelance, location freelance. however this cloud models comes with several securityissues[1]. A business person keeps crucial data on cloud, therefore security of information is crucial issue as chance of hacking and unauthorised access is there. Conjointly handiness could be a major concern on cloud.

This paper, discusses the file distribution and AES technique. Once file is distributed then information is additionallysegregated into several servers[3]. Therefore here the necessity of information security arises. Each block of file contains its own hash code, victimization hash code whichcan enhance user authentication process; solely approved person can access the info[4].

Here, the info is encrypted victimization advanced cryptography commonplace, so data issuccessfully and firmly keep on cloud. Third party auditor is employed for public auditing[2]. This paper discusses the handling of some security problems like quick error localization, information integrity, information security. The projected style permits users to audit the info with light-weight communication and computation value. Analysis shows that projected system is extremely economical against malicious information modification attack and server colluding attack[4]. Performance and intensive security analysis shows that projected systems area unit incontrovertibly secure and extremely economical.

II. MOTIVATION

There exist many communicative ABE (Attribute Base cryptography)schemes wherever the decoding formula solely needs a continuing range of pairing computations. Recently, green et al. Planned a remedy to the current downside by introducing the notion of ABE with outsourced decoding, that mostly eliminates the decoding overhead for users[8]. Supported the prevailing ABE schemes, green et al. Conjointly bestowed concrete ABE schemes with outsourced decoding[1].

In these existing schemes, a user provides AN untrusted server, say a proxy operated by a cloud service supplier, with a metamorphosis key TK that enables the latter to translate any ABE cipher text CT happy by that user's attributes or access policy into an easy cipher text CT', and it solely incurs atiny low overhead for the user to recover the plaintext from the remodeled cipher text CT'. The protection property of the ABE theme with outsourced decoding guarantees that AN human (including the malicious cloud server) be ineffectual to be told something concerning the encrypted message; but, the theme provides no guarantee on the correctness of the transformation done by the cloud server[5]. Within the cloud computing setting, cloud service suppliers could have sturdy money incentives to come back incorrect answers, if such answers need less work and square measure unlikely to be detected by users.

III. LITERATURE SURVEY

1."Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage:"Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou,:

DOI10.17148/IJARCCE.2017.63178

In this paper, we have a tendency to show a way to firmly, with efficiency, and flexibly share knowledge with others in cloud storage. We have a tendency to describe new public-key cryptosystems that turn out constant-size ciphertexts such economical delegation of decipherment rights for any set of ciphertexts area unit attainable. In different words, the key key holder will unleash a constant-size combination key for versatile decisions of ciphertext set in cloud storage, however the opposite encrypted files outside the set stay confidential. This compact combination key will be handily sent to others or be keep during a} charge account credit with very restricted secure storage. We offer formal security analysis of our schemes within the customary model.

2. "A review of scalable data sharing techniques for secure cloud storage:"AditiTripathiMayank Deep KhareDr. Pradeep Kumar Singh
In cloud storage data sharing is an important functionality. Data transfer should be done securely and efficiently with others in cloud computing. In this paper we review different scalable data sharing techniques in cloud storage. To minimize the expenseof managing and storing secret keys for general cryptographic use is aim of cryptographic key assignment schemes. For supporting flexible hierarchy in decryption power delegation, a encryption scheme is represented which is basically proposed for concisely transmitting large number of decryption keys in broadcast scenario. To protect data privacyis a central question for cloud storage. We illustrate new public-key encryption scheme, which produces constant-size cipher texts such as efficient delegation decryption rights for any set of cipher texts are possible.

3. "**Efficient public key cryptosystem for scalable data sharing in Cloud storage:"**Ms. PramilaGharjale,Mr. Prakash Mohod
The Cloud storage means that the storing the information on-line within the variety of cloud. Knowledge sharing is one amongst the necessary practicality in cloud.

This approach describe one amongst the public-key cryptosystems as Key mixture Cryptosystem. This cryptosystem turn out constant-size cipher texts, here decipherment is additional powerful since any set of cipher text is decrypted at only 1 time by victimisation mixture key. Which can show however one can communicate or share the information from cloud firmly, with efficiency and flexibly. The construct of this cryptosystem is that one will mixture or gather any set of secret keys and from that gathering keys create single key that is compact. That means, the user WHO hold the key key will send a constant-size mixture key for set of cipher text in cloud, however the opposite encrypted files that is gift outside the set can stay confidential. During this approach MES-2 that's fashionable cryptography Standard-2 rule are used for cryptography and PKI (Public Key Infrastructure) is employed for key generation.MES-2 used vernam cipher construct to cypher the information.

4."Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage :" Baojiang Cui, Zheli Liu_ and Lingyu Wang
In this paper, we tend to address this sensible drawback, that is basically neglected within the literature, by proposing the novel construct of key-aggregate searchable encoding and instantiating the construct through a concrete KASE theme, during which an information owner solely has to distributeone key to a user for sharing an oversized variety of documents, and also the user solely has to submit one trapdoor to the cloud for querying the shared documents. The safety analysis and performance analysis each make sure that our projected schemes ar incontrovertibly secure and much economical.

5. "Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm:"Punam V. ArunaVerma
This paper, discusses the file distribution and SHA-1 technique. Once file is distributed then information is additionally lily-white into several servers. Therefore here the requirement of knowledge security arises. Each block of file contains its own hash code, victimization hash code will|which is able to} enhance user authentication process; solely approved person can access the info. Here, the info is encrypted victimization advanced cryptography customary, therefore information is with success and firmly keep on cloud. Third party auditor is employed for public auditing. This paper discusses the handling of some security problems like quick error localization, information integrity, information security

III. SYSTEM ARCHITECTURE

Cryptography technique interprets original knowledge into unclear kind.Cryptography technique is split into cruciate key cryptography and public key cryptography. This method uses keys for translate knowledge into unclear kind. Therefore solely approved person will access knowledge from cloud server[8].

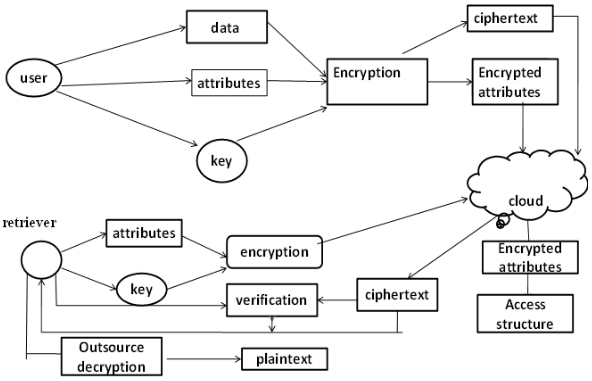


Fig:7.2 : Architectural Design

FEATURES:

- **Key Generation:** It generates the Private Key for security between two parties only.

DOI10.17148/IJARCCE.2017.63178

- Data consistency.
- Data Integrity
- Data security

IV. PROPOSED SYSTEM

In follow multiple parties might collaborate to speak their knowledge sets in Cloud [1]. Throughout this method no party desires to disclose her/his personal knowledge to others. This paper discusses the handling of some security problems like quick error localization, knowledge integrity, knowledge security[8]. The projected style permits users to audit the information with light-weight communication and computation value[9].

MODULES:
1. Setup Phase
2. Encrypt Phase
3. KeygenPhase,
4. Decrypt Phase

MODULES DESCRIPTION:

1) SETUP section

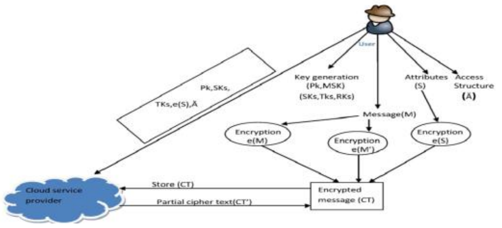
The setup rule takes no input apart from the implicit security parameter. It outputs the general public parameters PK and a master MK.

2) Encipher section

Encrypt(PK,M, A). The encoding rule takes as input the general public parameters PK, a message M, Associate in Nursingd an access structure A over the universe of attributes. The rule can encipher M and manufacture a ciphertext CT specified solely a user that possesses a collection of attributes that satisfies the access structure are going to be ready to rewrite the message[1]. We'll assume that the ciphertext implicitly contains A.

3) KEY information section

Key Generation(MK,S). The key generation rule takes as input the master MK and a collection of attributes S that describe the key. It outputs a non-public key SK



4 DECRYPT PHASE

Decrypt(PK, CT, SK). The cryptography algorithmic rule takes as input the general public parameters PK, a ciphertext CT, that contains Associate in Nursing access policy A, and a privatekey SK, that may be a personal key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithmic rule can decipher the ciphertext and come a message M[4].

AES ALGORITHM:

In contrast to its precursor DES, AES doesn't use a Feistel network. AES may be a variant of Rijndael that includes a mounted block size of 128 bits, and a key size of 128, 192, or 256 bits. [2]In contrast, the Rijndael specification in and of itself is such that with block and key sizes that will be any multiple of thirty two bits, each with a minimum 128 and a most of 256 bits[3].

The key size used for associate AES cipher specifies the quantity of repetitions of transformation rounds that convert the input, known as the plaintext[4], into the ultimate output, known as the ciphertext. The quantity of cycles of repetition ar 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 spherical consists of many process steps, every containing four similar however completely different stages, as well as one that depends on the secret writing key itself. A collection of reverse rounds ar applied to rework ciphertext into the first plaintext exploitation an equivalent secret writing key.

V. CONCLUSION

We introduce the idea of key primarily based cryptosystem for ascendible knowledge sharing in cloud. We have a tendency to well-tried security of the system during a model that offers the someone his alternative of public key and messages forge. Associate in Nursing economical consumer primarily based cryptography with the ability of single combination key's adopted .Our project ensures conviction in terms of confidentiality. In cloud storage, the quantity of cipher texts sometimes grows chop-chop.

Therefore we've got to order enough cipher text categories for the longer term extension. So knowledge privacy and security is maintained by coming up with a non-public key cryptosystem referred to as as AES algorithmic program. We show that our theme is very economical for server colluding attack and malicious knowledge modification attack with minimum computation overhead. Performance analysis and in depth security shows that the projected theme is incontrovertibly secure and extremely economical.

ACKNOWLEDGEMENT

I would wish to impart all the researchers acting on this field WHO in a way or another guided us on achieving our goals. We'd additionally wish to impart all the professors at DYPCOE, DYP faculty of Engineering, Pune WHO were kind enough to share their views and offered some suggestions in creating this project success.

DOI10.17148/IJARCCE.2017.63178

REFERENCES

[1] Qian Wang, Cong Wang, KuiRen, Wenjing Lou, and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactional Paper, 2011.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. Of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession", in Proc. of Secure Comm'08. New York, NY, USA: ACM, 2008, pp. 1–10.

[4] Cong Wang, Qian Wang, Kui Re, Ning Cao, and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactional Paper, 2012.

[5] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," Online at https://www.sun.com/offers/details/sun transparency.xml, November 2009.

[6]. Amazon.com, "Amazon Web Services (aws)," Online at http://aws.amazon.com/, 2009.

[7]. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of Retrievability for Large Files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp.584–597.

[8]. Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification," in Proc. of the 6th Theory of Cryptography Conference (TCC'09), San Francisco, CA, USA, March 2009.

[9]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.

[10]. Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, Accepted for Publication, 2012.