Open access Journal International Journal of Emerging Trends in Science and Technology

Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i04.01

Study of Algorithms for Securing Data Stored in Cloud

Authors

Mrs. K. Vidhya M.E., (PhD)[1], V. Monika[2], S.S. Subasri[3], R.Sukanya[4]

[1]Assistant Professor (Sr.G), Department of Computer Science and Engineering
KPR Institute of Engineering and Technology, Arasur, Coimbatore

[2,3,4]UG Students, Department of Computer Science and Engineering
KPR Institute of Engineering and Technology, Arasur, Coimbatore

ABSTRACT

Cloud computing is a revolutionary computing paradigm, that enables flexible, on-demand, and low-cost usage of computing resources, but when the data is outsourced to some cloud servers, various privacy issues emerge on it. Various encryption schemes have been proposed to secure the cloud storage. However, most work focuses on the data privacy and the access control. Data storage security means securing the data on the storage media. So, security is very much important in cloud computing for ensuring data placed on the secure mode in the cloud. To ensure security from third party's authentication is mandatory. In this paper, we discuss a many techniques which are used to provide security in the field of cloud computing and are compared based on their performance, pros and cons.

INTRODUCTION

The best method of protecting data against passive and active fraud issues is cryptography which has an important role in the security of data storage. It generally happens the sensitive data must be archived by servers in such a way that only specific parties are allowed to read the content. In these situations, enforcing the access control using ordinary public key encryption schemes is not that much convenient as primitives to the higher extent decrease the flexibility of users to share their data. To address these concerns, Sahai and Waters introduced Attribute-based encryption (ABE), which refines Identity-based encryption by associating ciphertexts and private keys with sets of descriptive attributes. Decryption is done only when there is an overlap between the two sets. These results were extended by Goyal, Pandey, Sahai and Waters into richer kinds of ABE, where decryption is allowed when the attributes satisfy a more complex Boolean formula specified by an access structure. There are two flavours in Attribute-based encryption. In Key-Policy ABE schemes (KP-ABE), attribute sets are used to annotate cipher texts and private keys are associated with access tree structure that specify which cipher data the user will be entitled to decrypt. Ciphertext-policy ABE process in dual way, by assigning attribute sets to private keys and letting senders specify an access policy that receiver's attribute sets should comply with.

The Dual Key Encryption approach is considered as a stream of bits and the technique uses dual key, first key (control key) to determine the length of bits block and the second one is used for encryption according to the equation that used addition and multiplication based on mathematical theory of Galois field.

LITERACTURE SURVEY

Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. Identity-based ring signature, which eliminates the process of certificate verification. We further enhance the security of ID-based ring signature by providing forward security. The features of ID based cryptosystem

enhance efficiency and spontaneity of ring signature. Any member can sign a message anonymously on behalf of the group but id of the signer is hidden. Forward security that ensures past signature even if current key is leaked [12].

Cloud Data Storage Security Enhancement Using Identity Based Encryption

Data is outsourced by the data owner on cloud server and the access can be provided to the authorized user. But there are different security issues because cloud is managed by an un-trusted third party. This system provides security against Collusion attack, DDOS attack.

By using re-encryption concept we can get secured data and access permission that who will access the data is decided by only the data owner. Encryption and decryption is done based on Identity Based Encryption algorithm and keys are generated using Base64 algorithm. Security of data can be enhanced by identity based secure encryption and re-encryption. It provides advantages like collusion- resistance and also provides security against Distributed Denial of Service attack with safe data forwarding [11].

Hybrid Cryptography Algorithm Based on Prime Factorization

In RSA public key cryptosystem security is based on the assumption that factoring of a large number is difficult and the private key is also detected. Hence the security is broken in cryptographic system. The security of Rabin cryptosystem is also like that of RSA, is related to the difficulty of factorization. HCAPF is a public key cryptosystem. In public key cryptosystem technique one key is needed for encryption and for decryption a different but related key is needed. Decryption key is very difficult to determine if one knows the algorithm and the encryption key. In HCAPF cryptosystem the security is improved by using dual modulus and the complexity of factoring the modulus is increased exponentially although the speed of encryption and decryption process is slowed down [3].

Attribute-Based Encryptionwith Encryption and Decryption Outsourcing

A new scheme of ABE with encryption and decryption outsourcing capabilities for cipher text policy attribute based encryption. In this scheme relies on the use of two semi-trusted proxies. One is used to outsource computational expensive encryption steps, another to outsource decryption steps. During the encryption process, a host involves the encryption proxy to create cryptographic policy components for a set of specified attributes, in such a way that the proxy unable to learn the message from this partially encrypted text and is enforced to use the given attributes. During the decryption, the decryption proxy is used for policy evaluation. After the successful evaluation the proxy transforms the original cipher text into the El Gamal type of cipher text and then it can be efficiently decrypted by the user. This outsourcing method is used to provide secure in the generic group model and also reduce computational power on mobile devices for both host and user.

An old ABE scheme for cipher text policy attribute based encryption that allows outsourcing of computationally expensive encryption and decryption steps, this scheme constitutes an important building block for mobile applications where both the host and users use mobile devices with limited computational power [6].

Attribute-Based Encryption with Advanced Encryption Standard

The personal health report is stored for access in cloud. The owner can create, manage and share the data on the cloud. But there were some privacy and security issues. The use of Attribute Based Encryption for effective encryption of data provides a high degree of privacy. Therefore for high data security Advanced Encryption Standard is used. It was suggested that the data be encrypted under a set of attributes which enables multiple users to decrypt using the assigned key. The owner can encrypt the data without even knowing the Access Control List.

For efficient data access control ABE is used. For efficient management of data and to prevent centralization of authority MA-ABE is used. Using MA-ABE the data is encrypted in the public domain. In the personal domain the owner directly provides the right for data access to the users using KP-ABE. Hence to enhance the security of the data on the servers AES algorithm is used. First data is encrypted using AES algorithm and later it is encrypted using ABE. The owner should also have the privilege to revoke the data and in times of emergency it should provide break glass access. Combining dual level encryption with AES enhances the security of the data. An intruder cannot find the encrypted data easily. It is used for secure transmission of data in encrypted format. In this system AES is used for sending user authentication data in encrypted format. The secure and scalable sharing of data in a multiple owner, multiple user, multiple authority scenario. ABE is used to encrypt the owner's data and Security is ensured through AES [10].

Dual Key Transformation based on Creation of Multi S- Boxes in AES Algorithm

Using dual keys in encryption and decryption processes in Sub-Byte transformation function. The first key generate multi random S-boxes depend on using multi keys that led to generate S-boxes provided that each one has its inverse associated with it, the second key is a random distribution of the S-boxes, the dual keys lead to increase the complexity in time during the encryption and decryption processes in Sub Byte function. The best method of data protection against any illegal activities is cryptography which has an important role in the security of data transmission. A cipher system is a set of reversible transformations that depend on a secret key and the algorithm, from set of a plaintext into set of cipher text. In the cipher system, the plaintext is divided into the blocks and ciphering procedure is carried out for each block. In cryptography, the two properties to secure cipher are confusion and diffusion.

Diffusion is spreading of the influence of a one plaintext bit to many cipher text bits with intention to hide the statistical structure of the plaintext. While, confusion is transformation that changes dependence of statistics on cipher text by statistics of plaintext. Mostly in cipher systems, the diffusion and confusion are done by means of round repetition. The simplicity lies in this concept is repeating a single round. In modern block ciphers there were four transformations: 1) substitution, 2) permutation, 3) mixing and 4) key-adding. Many researches on S-box design are focused on determination of S-box properties to yield cryptographically strong ciphers.

Mostly the block ciphers are of substitution-permutation (SP) type. S-boxes are used in such cipher systems. If it is a strong block cipher then it should be resistant to various attacks, such as linear and differential cryptanalysis. The first step is to generate multi random S-boxes depend on using multi keys that led to generate S-boxes provided that each one has its inverse associated with it and that represent the first key. The second step is to create a random index distribution of the S-boxes that created in the first step to get more complexity and the same delay time and this represent the second key. The first key that generate multi random S-boxes depend on using multi keys make our approach resistant to linear and differential cryptanalysis. This approach will lead to generate more secure block ciphers, solve the problem of the fixed structure S-boxes, and will increase the security level of the AES block cipher system. The main advantage of such approach is that an enormous number of S-boxes can be generated. The second key which is a random distribution of the S- boxes, lead in increasing the complexity degree within the same delay time during the encryption and decryption processes in Sub-Byte function [8].

Expressive Key-Policy Attribute-Based Encryption with Constant-Size Cipher texts

Attribute-based encryption contains two flavors. In Key-Policy ABE (KP-ABE), attribute sets are used to annotate cipher texts and private keys are

associated with access tree structures that specify which cipher data of the user will be entitled to decrypt. Cipher text-policy ABE (CP-ABE) proceeds in a dual way, by assigning attributes to private keys and let the senders to specify an access providing policy that receivers attributes should comply with Attribute-based encryption (ABE), allows for fine grained access control on encrypted data. In this key-policy system, the primitive enables senders to encrypt the messages under the attribute sets and private keys are associated with access tree structures that specify which cipher texts the key holder will be allowed to decrypt. In most ABE systems, the cipher text size grows linearly with number of cipher text attributes but in the proposed scheme allow for non- monotonic access structures and with constant cipher-text size. The normal identity based encryption scheme yields monotonic KP-ABE system in selective set model. They compared the efficiency among expressive KP-ABE in terms of cipher text overhead, private key size as well as in the number of pairing evaluations and exponentiations. This new efficient Identity-based revocation mechanism, when combined with a particular instantiation of our general monotonic construction, gives rise to expressive KP-ABE realization with constant-size cipher texts [7].

Attribute-Based Encryption with fast decryption

Attribute- based encryption (ABE) is a public key encryption in which encryption and decryption of messages are done based on user attributes. The cipher text size is proportional to its associated number of attributes and decryption time is based on the number of attributes used. In this "unbounded" KP-ABE system cipher texts are decrypted with constant pairing numbers. In this system generalized decryption algorithm and various efficiency tradeoffs are tuned to their liking on a spectrum independently. GPSW (Goyal, Pandey, Sahai and Waters) scheme works on one end and fast decryption scheme works on the other end. The tuning does not change the public parameters or any encryption algorithm. The main feature of this fast decryption scheme is that it requires only two pairings for decryption. This system is secure for recent systems using dual system encryption [10].

Cloud Storage System with Data Confidentiality and Data Forwarding

The functionality of the storage system is limited when general encryption schemes are used for data confidentiality. We propose a new threshold proxy re-encryption scheme to form a secure distributed storage system. This distributed storage system lets a user to forward his data in the storage servers to another user without retrieving the data back along with secure and robust data storage and retrieval. The proxy re-encryption scheme supports encoding operations and forwarding operations over encrypted and encoded messages.

Proxy re-encryption schemes are cryptosystems which allow third parties to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. Data confidentiality is affected when data is stored in third party's cloud. A user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages in order to provide strong confidentiality for messages in storage servers. **Erasure coding** (EC) is a method of data protection in which data is broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different locations or storage media [4].

Key-Policy Attribute-Based Encryption Scheme with Constant Cipher text Length

Attribute-based encryption (ABE) is a new cryptographic primitive which provides a tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. In a Key-

Policy attribute-based encryption (KP-ABE) is an important type of ABE, which enables sender to encrypt messages under a set of attributes and private keys are associated with access structures that specify which type of cipher texts the key can

decrypt. KP-ABE schemes suitable for structured organizations with rules about who may read particular documents. Their construction supports access structure with constant cipher text size to access policy can be expressed as any monotone access structure. The number of ciphertext attributes is independent of ciphertext size and the number of bilinear pairing evaluations is reduced to a constant.

In a Cipher text policy attribute based encryption (CP-ABE) system, when a sender encrypt a message, they specify a specific access policy in terms of access structure over attributes in the cipher text. The CP-ABE mechanism is closer to traditional role based access control method. In most of the scheme, the ciphertext size grows linearly with the number of attributes embeddedin cipher text and also provides security for generic group model [2].

Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields

The Dual Key Encryption approach considered as a variable stream of bits and the technique uses dual key for encryption, first key to determine the length of bits block and the second one is used for encryption according to the equation that used addition and multiplication based on mathematical theory of Galois field.

It achieves best results, where it provides high level of security by using dual key and four dynamic tiny block cipher, to decrypt the cipher text and it is designed with two major factors, first decreasing the time needed for encryption/ decryption. Second level of security should be high enough so attackers cannot obtain the encryption/decryption key easily. The file (plain text) can be recovered using the same algorithm but with reverse mathematical operations processed. It prevents exhaustive key search and differential attacks. Non fixed (dynamic) size block cipher avoid replaying in authentication and attacks that can happen on the fixed sized block cipher algorithms, dynamic block length in algorithm lead to maximum cryptographic confusion and consequently makes it difficult for cryptanalysis. The more rounds of proposed algorithm are increased the higher security is achieved [1].

FPGA (Field Programmable Gate Array) based Dual Key Encryption

Design and Implementation of FPGA (Field Programmable Gate Array) embedded system for time based IDEA encryption. In this technique, time is used as a second dimension of the key. For proper decryption, the correct key entered at the correct time. It uses a dynamically varying number of shifts for both encryption and decryption until the system needs to wait til that time and its forms the time based key input. In this existing system, suffer from Brute Force Attack in which all key combinations are tried out to find the correct key and the possibility of brute force attack is minimized. The proposed system adds complexity to the IDEA encryption algorithm by including the time as a second dimension besides increasing the time required for cryptanalysis and it needs concurrent execution and real time processing.

A novel approach is used to enhance the security level of IDEA encryption algorithm against brute force attack besides retaining its original strength. This approach impedes that, cryptanalysis using brute force attack purely depends on the speed of the system used. The included delays make the cryptanalysis more complex, though the system is capable of performing faster. If more number of systems are used for cryptanalysis, which reduce the level of security of the encryption algorithm when the key space will be shared between them. For example 128bit size of the key provides adequate level of security at the present time, due to the increase in the speed of the system the key size needs to be increased proportionally. The proposed scheme provides an alternative method in which without any modification the strength of the IDEA algorithm is maintained but at the same the system can defend against brute force attack more vigorously [5].

The comparative summary of the above algorithm are tabulated below in Table 1. The table compares key parameters, performance, pros and cons of various algorithms.

Table 1: Comparison between different types of security algorithm

METHODOLOGY	KEY PARAMETERS	PERFORMANCE	PROS	CONS
ABE [6][10][11]	Proxy Re-encryption, Attribute-Based Encryption, Access Policy, Outsourcing	An attacker who cannot be able to attack using a single key to decrypt the cipher text.	1. Log encryption is possible. 2. Used in broadcast encryption in order to lower the number of keys.	1.least efficient 2. Non-existence of attribute revocation mechanism.
KP-ABE [2][7]	Fine grained access control, cipher text	It is proven selectively secure under the decisional bilinear Diffie -Hellman assumption.	1. It is collusion resistance. 2. It Supports fine-grained access control.	1.Scalability and user accountability is not satisfactory
CP-ABE [7]	Cipher text policy, constant key size, ABE,	It is secure under a q-base assumption i.e., the number of terms is parameterized by a value q that depends on the behavior of the attacker.	1. It satisfies User accountability 2. The security can be efficient in any cipher text attacks.	1. It is not Scalable. 2. It is inefficient and its overhead grows significantly with the size of universe attribute sets.
IBE [12]	Data owner, DDOS, Proxy Server, Re-encryption key.	It is difficult to attack as the key reaches its expiration date the extraction of data become declined.	1. It eliminates the need for public key distribution infrastructure. 2. It is possible to encode additional information in to the identifier.	1. The private keys generated by PKG may decrypt any message without authorization. 2. It cannot be used for non-repudiation.
AES [8][10]	Byte substitution, shift rows, mix columns, add round key.	1. Extremely efficient in 128 bit form. 2. Impervious to all attacks except brute force. 3. High speed and low RAM requirement.	1. Fast and flexible 2. More secured and it supports larger key sizes than 3DES.	1. Due to key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
ID based ring signature [4][13]	Security, SSL/TLS (Secure Socket Layer / Transport Layer Security).	It prevents unlocking the private information even if the server's private key is known. The key disappears after sometime so, hackers can't decrypt the data.	1. It prevents the compromise of a long-term secret key from affecting the confidentiality of past conversation. 2. It allows the recovery	1. It cannot defend against a successful cryptanalysis of ciphers. 2. It only protects keys not the ciphers.
HYBRID CRYPTOGRAPHY [3]	Public key encryption, Symmetric key algorithm	It incorporates a combination of asymmetric and symmetric encryption to benefit the strength i.e., speed and security.	1. To overcome the problems associated with encrypting long messages. 2. It provides a solution to key distribution and data transmission issues when using symmetric encryption.	1. It is a complex process 2. Key management is difficult.
DYNAMIC DUAL KEY ENCRYPTION [1][5]	Dynamic block, Dual keys, Encryption and Decryption,	The encryption and decryption time of any larger plaintext size is very much less than AES algorithm.	1.High resistant against brute force attack 2. It provides high level of security.	1. It depends on the key alone for encryption 2. It is vulnerable to brute force attack.

CONCLUSION& FUTURE WORK

There are many existing techniques available which is used to implement security in cloud. In this paper, we discussed algorithms like AES, Attribute Based Encryption (ABE), KP-ABE, CP-ABE and Dual key encryption concepts. From the comparison we can able to say that AES has the best performance and it is stronger against data attacks. Our future work will be combining AES and ABE method to secure PHR data stored in cloud. And also we can combine other privacy-enhancing techniques with cryptographic techniques.

REFERENCES

1. [1]Abdul Monem S. Rahma, Baisima Z. Yacob, "The dynamic dual key encryption algorithm based on joint Galois fields," in International journal of computer science And network security (IJCSNS), vol. 11 no.8, August 2011.
2. Changji Wang, Jianfa Luo, "An Efficient key-policy Attribute-based encryption scheme with constant ciphertext length," Hindawi Publishing Corporation, Mathematical Problems in Engineering, Vol. 2013, Article ID 810969.
3. Indiver Purohit, Raj Kumar Somani, "Hybrid Cryptography Algorithm Based on Prime Factorization," in International Journal of Recent Development in Engineering and Technology,ISSN 2347-6435, vol. 2, Issue 2,February 2014.
4. N.Jenefa, J.Jayalakshmi "A Cloud Storage System with Data Confidentiality and Data Forwarding," in International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, v3, Iss.-1, March 2013.
5. B. Lakshmi, E. Kirubakaran, T.N. Prabakar, "Design and Implementation of FPGA based Dual Key Encryption," in International jou. of computer application (0975-8887), vol. 3- no.3, June 2010.
6. Muhammad Asim, Milan Petkovic, Tanya Ignatenko, "Attribute-based encryption with encryption and decryption outsourcing," December 2014, published in 12th Australian Information Security Management Conference.
7. Nuttapong Attrapadung, Benoit Libert and Elie de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," Research Center for Information Security, AIST (Japan), Universitecatholique de Louvain, ICTEAM – Crypto Group (Belgium), Ecoleno rmale superieure, Cachan (France).
8. Nada Hussein M. Ali, Abdul Monem S. Rahma, "Encryption using Dual Key Transformation based on Creation of Multi S- Boxes in AES Algorithm," December 2013, International Journal of Computer Applications(0975-8887), vol. 83 - no. 10.
9. B. Sri Varsha1, P.S. Suryateja, Bhimavaram, "Using Attribute-Based Encryption with Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud," published in2014, International journal of Computer Science and Information Technologies, Vol. 5(5), 2014, 6395-6399.
10. Susan Hohenberger, Brent Waters, "Attribute-based encryption with fast decryption," May 8, 2013.
11. VarshaS.Agme, Prof. Archana C.Lomte "Cloud data storage security enhancement using identity based encryption," in International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 4, April 2014.
12. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," in IEEE Trans. On computers, vol.64, no.4, April 2015.