4th International Conference on Recent Innovations in Science Engineering and Management
India International Centre, New Delhi
20th March 2016, www.conferenceworld.in
(ICRISEM-16)
ISBN: 978-81-932074-6-8

ATTRIBUTE BASED LZ4 ENCRYPTION WITH EFFICIENT SIGNATURE VERIFIABLE DECRYPTION

R.Vishnu Priya[1], G.Yuvarani[2],

[1]Assistant Professor/CSE, [2]Student/CSE, IFET College of Engineering, Villupuram, (India)

ABSTRACT

Attribute based encryption is a challenging method that server public key based one to many encryption allows the user to encrypt and decrypt file based on own attributes. This method forbids the user from malicious cloud. Attribute based encryption with efficient verifiable outsourced decryption approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The drawback of the verifiable outsourced ABE schemes increases the users and the cloud server's computation costs and is relatively large cipher text size. This method overcomes the efficient issue of the verifiable outsourced ABE schemes. The extended cipher text policy attribute based encryption (CP-ABE) prevents any unauthorized users from accessing data, even if the user stores data in an untrusted server. The new approach sign based cipher text policy attribute based encryption(S-CP-ABE) scheme provides authentication through a public verifier which validate the receiver where the genuine receiver is receiving the file among identical attribute users. The LZ4 compression algorithm is used to reduce the size of the encrypted file.

Index Terms: Data Sharing, CP-ABE, LZ4 Compression Method, S-CP-ABE.

I.INTRODUCTION

Attribute based encryption is a kind of public key encryption [11] [12] in which the secret key of a user and the cipher text are based on attributes [10]. The decryption of a cipher text is feasible only if the set of attributes of the user equivalent to the attributes of the cipher text. Attribute based encryption with efficient verifiable outsourced decryption approach to translate any ABE scheme with outsourced decryption [7] [9] into an ABE scheme with verifiable outsourced decryption. Compared with the previous outsourced ABE, our verifiable outsourced ABE neither increases the users and the cloud server's computation costs nor expands the cipher text size. The receivers may have a same attributes as the sender revealed. In this situation, there is a possibility for leakage of privacy data or hacking of privacy data. Wrong identification of receiver may occur, data transferring may be wrong, one's data is forwarded to others. It occupies lot of space in cloud because it doesn't use any compression method. This method overcomes the efficient issue of the verifiable outsourced ABE schemes [1]. In an ABE scheme, a user's keys and cipher texts are labeled with sets of illustrative attributes and a particular key can decrypt a particular cipher text only if there is a equivalent between the attributes of the cipher text and the user's key[2][6]. Cipher text-Policy Attribute-Based Encryption, by using this techniques encrypted data can be kept unrevealed even if the storage server is suspicious; moreover, our methods are secure against collusion attacks. In our system attributes are used to describe a user's identification and a party encrypting data decide a policy for who can decrypt [3] [4] [5].

II.ALGORITHM DESCRIPTION

2.1. Secure Hashing Algorithm

Step 1:-Padding Add Padding to the end of the authentic message length is 64 bits and multiple of 512.

Step2:- Appending length.

In this step the excluding length is calculated.

Step3:- Divide the Input into 512-bit blocks.

In this step we divide the input in the 512 bit blocks

Step4:-Initialize chaining variables.

In this step we initializing chaining variables here we initialize 5 chaining variables of 32 bit each=160 bit of total.

Step5:-Process Blocks

1) Copy the chaining variables
2) Divide the 512 into 16 sub blocks
3) Process 4 rounds of 20 steps each.

Parameters of SHA: Below equation shows a single SHA operation.

1) Default Parameters

abcde(e+process p_s5(a)+W[t]+k[t]),a,s30(b), c, d

Here:- a, b, c, d, e =chaining variables Process p =status of logical operations

st =<<< W[t] =derived other 32 bits bytes K[t]=five additives constants are defined.

2) Actual Parameters.

Key Length: 128 bits

Block Size: 160 bits

Cryptanalysis: Resistance Strong against Digital Certificate.

Rounds: 4

Total Steps: 20

2.2. Advanced Encryption Standard (Aes)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software performance are faster still. New encryption standard suggested by NIST to replace DES. Encrypts data blocks of 128 bits in 10/12/14 rounds depending on key size. It can be implemented on various platforms particularly in small devices. It is carefully tested for many security applications.

i. Algorithm Steps:

These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. Usual Round :

Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K(round)

iii. Final Round: Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K(10)

iv. Encryption: Each round consists of the following four steps:

i Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii Shift Rows : In the encryption, the transformation is called Shift Rows.

iii Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv. Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the “Mix columns” step.

v. Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key and d) Inverse mix columns.

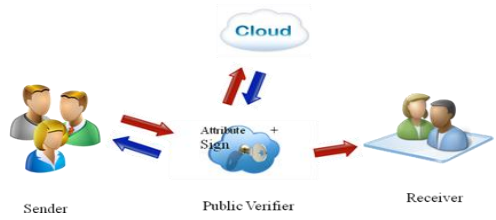
2.3. Lz4 Compression Methods

LZ4 is a lossless data compression algorithm that is intense focused on compression and decompression speed. Compression is type of data compression algorithms that allows the original data to be completely reconstructed from the compressed data. By contrast, lossy compression permits reconstruction only of an approximation of the original data, though this usually improves compression rates (and therefore reduces file sizes).Lossless compression reduces bits by discovering and eliminating statistical redundancy. No information is lost in lossless compression.

III. PROPOSED SYSTEM

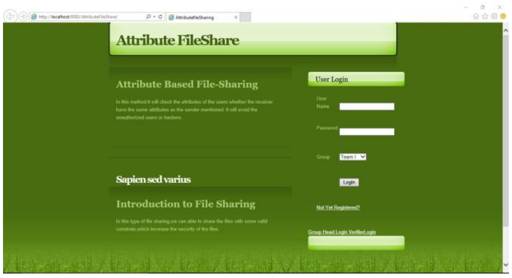
The extended cipher text policy attribute based encryption (CP-ABE) prevents any unauthorized users from accessing data, even if the user stores data in an untrusted server.

The LZ4 compression algorithm is used to reduce the size of the encrypted file. The new approach sign based cipher text policy attribute based encryption(S-CP-ABE) scheme provides authentication through a public verifier which validate the receiver where the genuine receiver is receiving the file among identical attribute users[8].

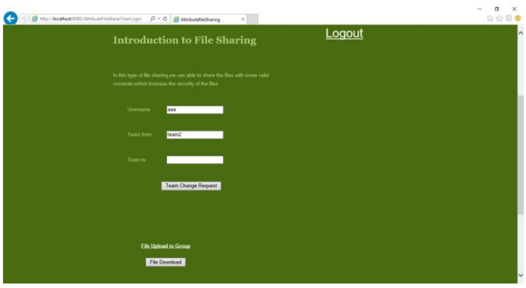


IV. EXPERIMENTATION AND RESULT

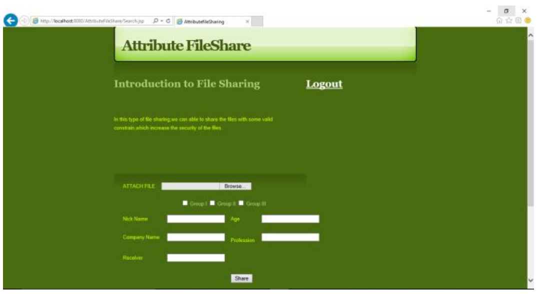
Login:



File upload:



Sharing of File:



File Download:

Security:

In this project, the CA is fully trusted in the system for security. It will not collude with any user, but it should be prevented from decrypting any cipher texts by itself.

Communication Cost:

The communication cost of attribute revocation is linear to the number of cipher texts which contain the revoked attribute. Our scheme incurs much less communication cost during the attribute revocation.

Storage overhead:

The storage overhead is one of the most major issues of the access control scheme in cloud storage systems. In our scheme, besides the storage of attributes, each AA needs to store a public key and a secret key for each user in the system. Thus, the storage overhead on each AA in our scheme is also linear to the number of users in the system.

Efficiency:

The performance and security analysis indicate that the proposed scheme is useful for securely manage the data distributed in the data sharing system.

V. CONCLUSION

In the work, collusion resistance is insured by using a secret-sharing scheme and embedding independently chosen secret shares into each private key. The proposed scheme S-CP-ABE solves the duplicate attribute problem, where given attributes matching two users. The signature and the attribute grouping give high security compared to other existing methods. There is no separate data owners and public verifier for providing keys and authentication process, this will reduce the communication cost and computation cost.

REFERENCES

[1]. Attribute-Based Encryption With Efficient Verifiable Outsourced Decryption Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma, VOL. 10, NO. 7, JULY 2015.

[2]. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.

[5] Y. Rouselakis and B. Waters, “Practical constructions and new proof methods for large universe attribute-based encryption,” in Proc. ACM Conf. Comput. Commun. Secur., 2013, pp. 463–474.

[6] N. Attrapadung, J. Herranz, F. Laguillaumie, B.Libert, E. de Panafieu, and C. Ràfols, “Attribute-based encryption schemes with constant-size ciphertexts,” Theoretical Comput. Sci., vol. 422, pp. 15–38, Mar. 2012.

[7] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in Proc. 20th USENIX Secur. Symp., 2011, p. 34.

[8] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. CCS, 1993, pp. 62–73.

[9] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 465–482.

[10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 456–465.

[11] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632, K. G. Paterson, Ed. Berlin, Germany: Springer-Verlag, 2011, pp. 129–148.

[12] K.-M. Chung, Y. Kalai, and S. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 483–501.