Access Control Model with Attribute Based Multiple Encryption

[1]Aishwarya Shinde, [2]Rupali Kangane, [3]Priyanka Deshmukh, [4]Mr. Satish L. Kuchiwale

[1,2,3]UG Student, [4]Professor, [1,2,3,4]S.I.G.C.E, Mumbai, Maharashtra, India.

[1]*aishwaryashinde026@gmail.com*, [2]*rupalikangane10@gmail.com*, [3]*priyankadeshmukh610@gmail.com*, [4]*slksatish@gmail.com*

Abstract — Users are provided by an online storage space hosted on drobox, accessible anywhere via the Internet. Hierarchical Attributed Set Based Encryption (HASBE) concept used in existing system. User is responsible for keeping the data available and accessible but issues arises such as time complexity, flexibility, data security, scalability. These issues are solved in developed system with the help of Cipher Text-Policy attribute-set-based Encryption (CP-ABE). It is an access control model where data will be stored in encrypted form on drobox and data will decrypted using keys. In developed system, multiple encryption is done using four different algorithms named as AES, Blowfish, RSA and Triple DES. These algorithms are used for images, doc and pdf files etc. Furthermore, integrating all these algorithms with CP-ABE key generation techniques used for encrypting file. When compared to existing system, developed system provides data security with less time complexity.

Keywords — Scalability, Flexibility, Attribute, Cipher text-policy.

I. INTRODUCTION

Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of image data is very important in many areas, such as copyright protection and privacy, security communication, and also in military applications Trust in digital data is characterized in terms of confidentiality, authenticity, and integrity. Confidentiality is ‘the property that information is not made available or disclosed to unauthorized individuals, processes or entities.’ Authenticity is defined as ‘the corroboration that the source of data received is as claimed.’ Integrity is the ‘the property that data has not been altered or destroyed in an unauthorized manner.’ Data (Encryption) is a good method for providing security to image data by making image visually unreadable and also difficult to decrypt it for unauthorized users. Securing data is always of vital importance and because of the critical nature and the large amounts of complex data it carries, the need is even more important. To be effective, data security depends on more than simply applying appropriate data security procedures. Computer based security measures mostly capitalizes on user authorization and authentication. HASBE(Hierarchical Attributed Set Based Encryption)scheme is not scalable and flexible for key generation[1][6]. In traditional encryption schemes, a sender usually needs to know the identities of the intended recipients and needs to pre-share credentials with them. The objective is that a sender encrypts data that can only be decrypted and read by an exact recipient. Given its exclusive benefits. CP-ABE has recently gained much attention and has been adopted on large-scale dynamic systems[2]. Cipher text-Policy Attribute-based encryption(CP-ABE) is an expansion of public key encryption that allows users to encrypt and decrypt messages based on attributes[2].

II. Problem Statement

Users are provided by an online storage space hosted on drobox, accessible anywhere via the Internet. It provides storage for any kind of file type i.e. documents, images, videos etc. Hierarchical Attributed Set Based Encryption (HASBE) concept used in existing system for access control using AES algorithm but it suffers from some disadvantages such as not handling compound attributes of files efficiently and suffering from flexibility, scalability, time complexity, data security issues[1].

In Cipher text-policy attribute set based encryption (CP-ABE) is used for file sharing attributes in developed system. It maintains flexibility, scalability, time complexity and data security. In CP-ABE system compound attributes i.e. (name, size) for files are taken, XOR operation is performed between file attributes and encrypted key is generated. Four algorithms are used, they are as follows: Advanced Encryption Standard(AES) is used for pdf, doc, etc. Rivest Shamir Len-Aldeman (RSA) is accessible only for text whereas Blowfish is used for image and audio, and Triple DES encrypt video, gif, doc, pdf, excel.

III. EXISTING SYSTEM

HIERARCHICAL ATTRIBUTED SET BASED ENCRYPTION (HASBE):

HASBE scheme seamlessly extends the ASBE (Attribute set based encryption) scheme to handle the hierarchical structure of file system .

HASBE scheme, which uses the concept of AES (Advanced Encryption Standard) algorithm. It shows how HASBE is applied for hierarchical user grant; data file creation, file access, and file deletion.

Advanced Encryption Standard (AES) Algorithm:

1) Advanced Encryption Encryption Standard (AES) is a standard algorithm to encrypt and decrypt sensitive information. AES is a symmetric block cipher which accepts a block size of 128 bits. It provides a choice of three different key lengths which can be 128 bits, 192 bits, or 256 bits; referred to as AES-128, AES-192, and AES-256 respectively. Based on the key length the number of rounds in the encryption process is determined, for instance, the number of rounds

- for AES-128 is 10,
- for AES-192 it is 12,
- for AES-256 it is 14.

2) The major loop of AES executes the functions given below:

Functions of Advanced Encryption Standard

- SubBytes()
- ShiftRows()
- MixColumns()
- AddRoundKey()

AES makes use of 10, 12 and 14 rounds. After repeated transformation rounds, the plain text is converted into cipher text.

3) Implementation: AES-128, AES-192, AES-256 (128, 192 and 256 are bits) process the data block in 10, 12, or 14 rounds respectively. The transformations are predefined. All the rounds are similar except the last one where there is no mix-columns. The rounds operate on two 128 bits i.e., state and round key. Each round from 1 to 10 or 12 or 14 uses a different round key.

IV. PROPOSED SYSTEM

The proposed system use the concept of CP-ABE scheme which is the latest among all the ABE access control models. It uses attribute set based structure. CP-ABE had overcome many issues suffered by schemes implemented earlier which is HASBE.

ALGORITHM

1. ADVANCE ENCRYPTION STANDARD(AES)

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

Here, it is restrict to description of a typical round of AES encryption. Each round comprises of four sub-processes. In Fig.1 shows AES encryption and decryption process.

Algorithm:

- Key Expansion: First from the cipher key the round keys are derived using the key schedule of Advanced Encryption Standard.
- Initial Round - AddRoundKey: Then each byte of the state is combined with the round key using bitwise XOR.
- Rounds:

i) SubBytes: This is a non-linear substitution step where each byte is swapped with another according to a lookup table.

ii) ShiftRows: In this transposition step each row of the state is shifted cyclically in a certain number of steps.

iii) MixColumns: A mixing operation operates on the columns of the state, combining the four bytes in each column.

iv) AddRoundKey

- Final Round (no Mix Columns)

v) SubBytes
vi) ShiftRows
vii) AddRoundKey

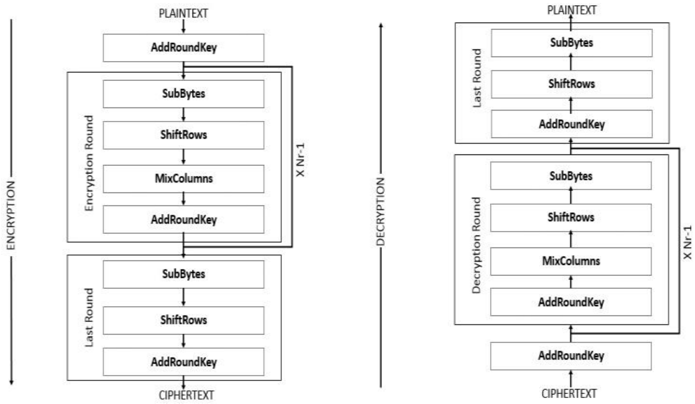


Fig:1 AES encryption and decryption process

2. BLOWFISH ALGORITHM

Blowfish Algorithm is an high performing symmetric key cryptographic algorithm. It was developed by Bruce Schneier. It has some key advantages like it is Fast, Compact, Simple and Secure.

Working of blowfish algorithm: Suppose the encryption is performed on a 64-bit block plain text input Y Here P-arrays and S-boxes will be used for encryption and decryption process. Decryption is also done in the same manner. The working process of blowfish algorithm is shown in below Fig.2

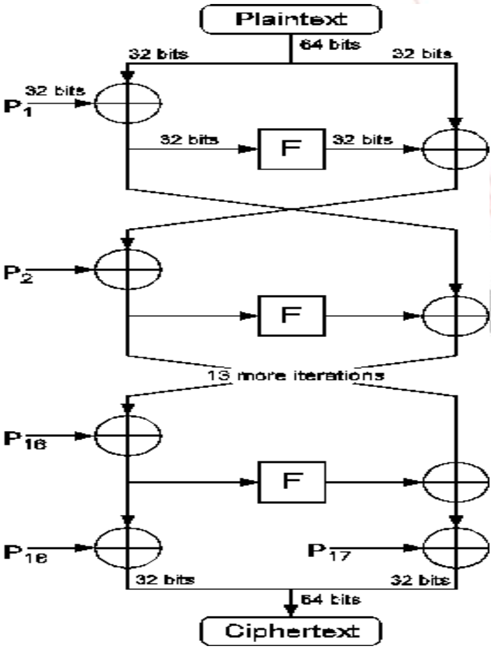


Fig.2 Working process of blowfish algorithm

3. RIVEST SHAMIR ADLEMAN(RSA)

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. RSA is become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. In Fig 3 Steps of RSA algorithm are shown.

A. Key Generation Algorithm:

Step1: Randomly and secretly choose two large primes: p, q and compute n = p. q
Step2: Compute ϕ (n) = (p – 1) (q – 1).
Step3: Select Random Integer: e such as 1 < e < n and gcd (e, ϕ) = 1.
Step4: Compute d such as e. d ≡ 1 mod ϕ(n) and 1 < d < ϕ (n).
Step5: Public Key: (e,n)
Step6: Private Key: (d,n).

B. Encryption process

encrypt m as c = me mod n

C. Decryption Process

decrypt the received message as m = cd mod n.

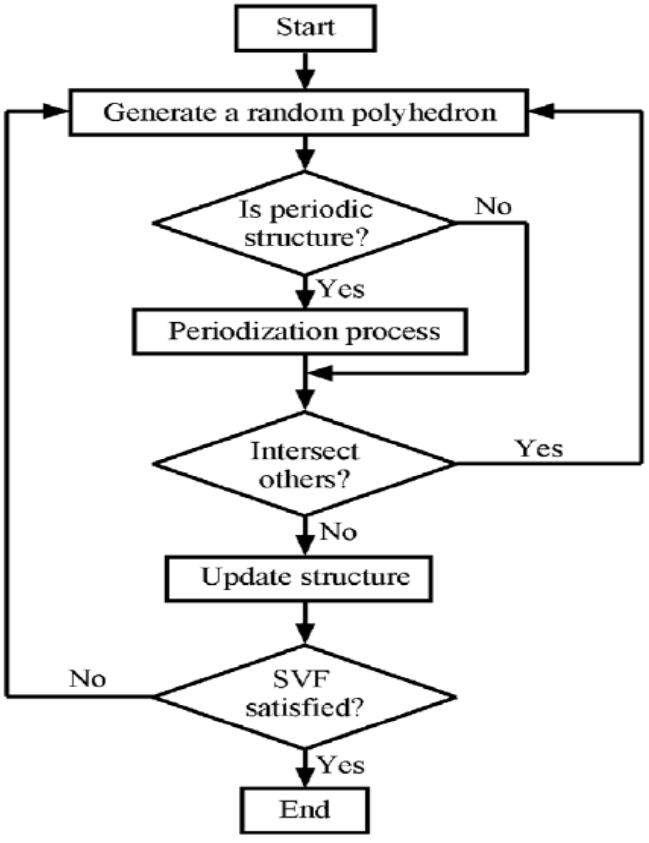


Fig 3 Steps of RSA algorithm

4. TRIPLE DES

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block.

The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. In Fig.4Triple DES process is shown.

Mathematically, Triple DES is represented as:

Pt---->EK1(pt)---->TEMP=EK1(pt)---->EK2(EK1(Pt)) ---->EK3(EK2(EK1(Pt)))---->Cp EK3(EK2(EK1(Pt)))

WHERE,

pt=plaintext
EK1(pt) =encrypted plaintext with key K1
TEMP=EK1(pt) =Temporary variable to store result
EK2(EK1(Pt))= Encrypted result of first cipher text using K2
EK3(EK2(EK1(Pt))=Encrypted result of second cipher text using K2
Cp EK3(EK2(EK1(Pt))) = Final cipher text encrypted using K1, K2& K3

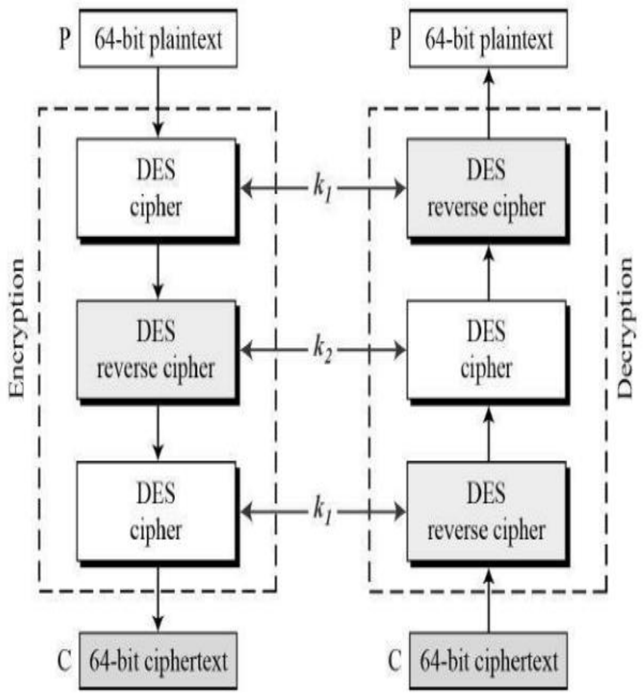


Fig:4. Triple DES

V. COMPARISON BETWEEN HASBE AND CP-ABE SYSTEM

- *HASBE CONCEPT USING AES ALGORITHM*

HASBE scheme was used for encryption of file attribute
In existing system AES algorithm was used for text file.
HASBE scheme is not efficient in handling data security and there was issue regarding integrity and confidentiality.
It is less scalable and flexible. Time complexity is more.

- *CP-ABE CONCEPT USING FOUR ALGORITHMS*

CP-ABE scheme is used for encryption of compound attribute of file. In implemented system four algorithms are used for encryption i.e. Blowfish, AES, RSA, Triple DES. whereas Blowfish and AES are used for image, pdf files, RSA for text file and Triple DES are used for audio, video and zip files.

CP-ABE scheme is more efficient in handling data security and it solves the issue regarding integrity and confidentiality.
It is more scalable and flexible. Time complexity is less for encryption and decryption process.

The below graph presented in Fig.5 shows key generation time difference using AES algorithm for HASBE and CP-ABE scheme.

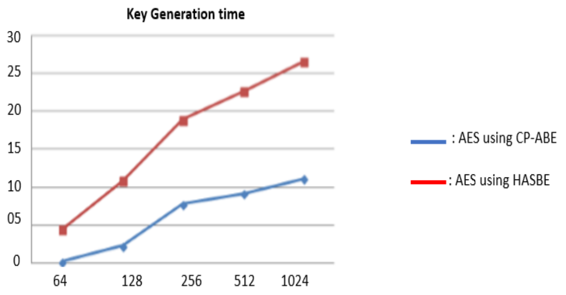
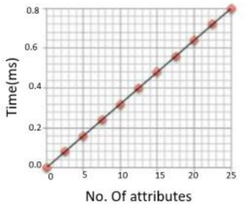


Fig.5: Key generation time

VI. RESULT ANALYSIS

The proposed method introduces the efficient way to analyze the time complexity.The below graph presented in Fig.6 shows number of attribute and total number of time required using Hierarchical Attributed Set Based Encryption (HASBE) scheme on the other hand Fig.7 shows number of attribute and total number of time required using Cipher Text-Policy attribute-set-based Encryption (CP-ABE) scheme.

The computation time is reduced in proposed (CP-ABE) method as compared to existing (HASBE) method.



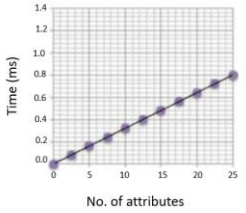


Fig.6: Time complexity using HASBE Fig 7: Time complexity using CP-ABE

VII. FUTURE ENHANCEMENTS

For better performance in future, Comparing with Clustering algorithm, extending this algorithm to data security. When compared to other methods this method shares secure data with certificate less encryption. In the future, work can be done on distributed and scalable Big Data sharing methodology with anonymous authentication on storage system.

VIII. CONCLUSION

Thus, this paper introduced that proposed system provides online storage space hosted on dropbox, which is accessible anywhere via the Internet. Using an enhanced CP-ABE scheme, which is highly efficient in handling data security, flexibility, scalability etc. Time complexity is reduced as compared to HASBE(existing) scheme. Using the various algorithm encryption and decryption process is done by taking compound attribute of file. The future scope of this application is to work on Big Data sharing methodology.

REFERENCES

[1] E.Angel Anna Prathiba and B.Saravanan" *HASBE for Access Control by Separate Encryption/Decryption in Cloud Computing*" International Journal of Emerging Trends in Electrical and Electronics (IJETEE) Vol. 2, Issue. 2, April-2013.

[2] Rajanikanth aluvalu, lakshmi Muddana," *A Survey on Access Control Models in Cloud Computing*"-in Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_7.

[3] O. Takami, N. Irie, C. Kang, T. Ishimatsu, and T. Ochiai, "*Computer interface to use head movement for handicapped people*," in Proc. IEEE TENCON'96, Digital Signal Processing Applications, vol. 1, pp.468–472. 1996

[4] Yang, K., Jia, X., Ren, K., Zhang, B., & Xie, R. (2013). *Dac-macs: Effective data access control for multiauthority cloud storage systems*. Information Forensics and Security, IEEE Transactions on, 8(11), 17901801.

[5] T. Hutchinson, K. P. White Jr., W. N. Martin, K. C. Reichert, and L. A.Frey, "*Human-computer interaction using eye-gaze input*," IEEE Trans. Syst., Man, Cybern., vol. 19, no. 6, pp. 1527–1533, 1989.Eissa, T., & Cho, G. H. (2012, December).

[6] *A fine grained access control and flexible revocation scheme for data security on public cloud storage services*. In Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on (pp. 2733). IEEE.

[7] Sultan Ullah, Zheng Xuefeng and Zhou Feng " *TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing*" International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013.

[8] A.Vishnukumar,G. Muruga Boopathi, S.Sabareessh" *Scalable Access Control in Cloud Computing Using Hierarchical Attribute Set Based Encryption (HASBE)* " International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[9] N.krishna L .Bhavani" *HASBE: A Hierarchical Attribute Set Based Encryption F or F lexible ,Scalable A nd Fine Grained Access Control In Cloud Computing*" International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.