Enhanced CP-ABE Algorithm for Authorisation and Efficient Encryption Decryption Process in Mobile Cloud Computing

Miss. B.J. Jawanjal
SGBAU, Amravati
India.

Dr. Prof. S.S.Sherekar
SGBAU, Amravati
India

Dr.V.M.Thakare
SGBAU, Amravati
India.

ABSTRACT

Mobile device and its applications have revolutionized way the data is stored and shared.It is becoming a warehouse of user'spersonal information. One way of enhancing privacy from data owner point of view is to encrypt thefiles before outsourcing them onto the cloud and decrypt the files after downloading them.This paper focused on analysis of five different techniques Rank Keyword Search Scheme, CLOAK Scheme, Traffic And Energy Saving Encrypted Search (TEES), Key-revocable ABE scheme, RSA-based CP-ABE scheme with constant size secret keys and cipher texts (CSKC).These method contain some issue and drawbacks.To overcome these issue, this paper has proposed anAuthorized and Efficient Encryption Decryption Scheme With AES Algorithm.By security analysis and performance evaluation, the proposed scheme is proved to besecure as well as efficient in mobile cloud computing.

Keywords— CP-ABE;TEES; TCPKE,MCC.

I) INTRODUCTION

With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store or retrieve the data from the cloud [1]. Typically, mobile devices only have limited storage space and computing power. Data access control has been an increasing concern in the cloud environment where cloud users can compute, store and share their data [2]. Cloud computing provides a scalable, location-independent and high-performance solution by delegating computation tasks and storage into the resource-rich clouds [3]. In a CP-ABE scheme should include constant size secret key and constant size cipher text, as well as a cost efficient mechanism for encryption and decryption [4]. Ciphertext-policy attribute-based encryption (CP-ABE) has been proposed to provide fine-grained access control for dynamic group formation in cloud-based data storage solutions. It enables the data owners to create access policiesby designating attribute constraints and embedding the data access policies into the ciphertext, such that any data user has to satisfy the corresponding attributes to access the data [5].

This paper discuss five scheme for the encryption decryption process of the CPABE algorithmare Rank Keyword Search Scheme,CLOAK Scheme, Traffic And Energy Saving Encrypted Search (TEES), Key-revocable ABE scheme, RSA-based CP-ABE scheme with constant size secret keys and cipher texts (CSKC).

But these method also have some problem so to overcome that Authorized and Efficient Encryption Decryption Scheme With AES Algorithmis proposed in this paper.

II) BACKGROUND

In the mobile cloud computing many attribute encryption schemes are used like CPABE. The ranked keyword search scheme for the outsourced cloud data

and for distributed private data statistical queries scheme is used. The ranking technique is proposed for distributed paralleldatabase for efficient accessed of privacy-preserving multi keyword search scheme. A single-keyword encryption search scheme utilizing ranked keyword search, which optimizes network communication between the user and the cloud by transferring the computing burden from the user to the cloud [1].CLOAK is based on stream cipher and takes the help of an external server for the generation and distribution of cryptographically secure pseudo-random number (CSPRN)[2].Atraffic and energy saving encrypted search (TEES) The proposed architecture offloads the computation from mobile devices to the cloud, and further optimize the communication between the mobile clients and the cloud [3].Key-revocable ABE scheme applicable to mobile cloud environments. A key issue in mobile cloud environments is how to reduce the computational cost on mobile devices and delegate the remaining computation to cloud environments. This also consider two additional issues: an efficient key revocation mechanism for ABE based on a concept of token-controlled public key encryption, and attribute hiding encryption from a cloud server[4].RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC) it has O(1) time complexity for each decryption and encryption. This scheme is then shown to be secure against a chosen cipher text adversary as well as been an efficient solution with the expressive AND gate access structures [5].

This paper introduces five scheme follows Rank Keyword Search Scheme, CLOAK Scheme, Traffic And Energy Saving Encrypted Search (TEES), Key-revocable ABE scheme, RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC).

The paper is organised as follows:

Section I Introduction. **Section II** discusses Background.**Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobility models. **Section VI** proposed method and outcome result possible. Finally **Section VIII** Conclude this paper.

III) PREVIOUS WORK DONE

In research literature, many MCC scheme have been studied to provide various mobility schemes and improve the performance for efficient encryption decryption process in CPABE.

C. Wang et al (2012) [1] has proposed primitives for Enabling secure and efficient ranked keyword search over outsourced cloud data.

Amit Banerjee et al (2017) [2] has proposed methodology on a lightweight, computationally efficient protocol, called CLOAK, for the mobile device. CLOAK is based on stream cipher and takes the help of an external server for the generation and distribution of cryptographically secure pseudo-random number (CSPRN). Three versions of the scheme referred as s-CLOAK, r-CLOAK and d-CLOAK.

Jian Li et al (2017) [3] has proposed traffic and energy saving encrypted search (TEES) a bandwidth and energy efficient encrypted search architecture over mobile cloud.

Tsukasa Ishiguro et al (2015) [4] has proposed key-revocable ABE scheme is a public key encryption scheme in which an entity cannot decrypt an encrypted message until the entity obtains additional information called a “token”.

Vanga Odelu1et al (2015) [5] has proposed new RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC) it has O(1) time complexity for each decryption and encryption.

IV) EXISTING METHODOLOGIES

A] Rank Keyword Search Scheme:

In the Rank Keyword Search Schemeupon receiving a trapdoor (encrypted form of search keywords), the cloud would perform a privacy-preserving search from the indexes provided by the provider. Then it selects top-*k* documents that contain the given search keywords. This process is achieved by using the RSBS algorithm shown in Algorithm2 [1].

Algorithm 2 Ranked Serial Binary Search (RSBS) Algorithm

Input:

Noised trapdoors (one per search keyword): $\tau_1', \ldots, \tau_e'$

Encrypted document indexes: $A = \vec{I}_1 \cdots \vec{I}_N$

The number of documents to return: k

Output:

Top-k documents that best match the search request: $D = \{D_1, D_2, \cdots, D_k\}$

1: $Scores = zeros(0, N)$ // create an array of N zeros
2: **for** $i := 1$ **to** N **do**
3: **for** $n := 1$ **to** e **do**
4: Score[i] ← Score[i] + bsearch($\tau_n', \vec{I}_i, 1, s_i$) // search if the keyword appears in any of the s slices of the document
5: **end for**
6: **end for**
7: sorted, indices = sort($Scores$) // sort the score array and get the indices or old element in the sorted array.
8: $D \leftarrow indices[0 : k-1]$ // get the top-k documents
9: **return** D

Algorithm1: RSBS Algorithm

B] CLOAK Scheme:

The CLOAK Schemegoal is to secure personal information stored in MD (images, pdf, doc) of size in the range of 5-10 MBs. The CLOAK protocol is based on stream cipher and takes the help of a cloud or an external server (ES) for generating the key-stream or a cryptographically secure. Figure-1 shows the basic architecture of the CLOAK protocol. In this, it consider a scenario where a user say Alice, using this CSPRN and can either save the CT in SD card or store it in the ES, which completes the encryption process. For sharing the encrypted Alice sends the <uid; fn>to Bob. In the decryption phase, Bob sends a request to the ES specifying <uid; fn> for the CSPRN. The ES consults its database with these parameters, generates the CSPRN of size csand forwards it to Bob. Finally, Bob can decrypt the using the CSPRN. pseudo-random number (CSPRN)[2].

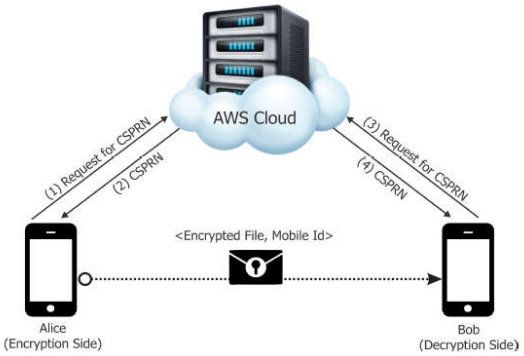

Figure1. Basic Architecture CLOCK

Algorithm 1 CSPRN Generation

Function *CSPRN_Gen (CSPRN size: cs)*

$s \leftarrow$ random_num() ; /* Key or Seed */
$sn \leftarrow$ random_num() ; /* Seq Num */
$CSPRN \leftarrow$ NULL ; /* Init. CSPRN */
$n \leftarrow \lceil cs/128 \rceil$;
while $n > 0$ **do**
$CSPRN \leftarrow CSPRN + AES(s, sn)$;
$sn \leftarrow sn + 1$;
$n \leftarrow n - 1$;
return CSPRN;

Algorithm2: CSPRN Generation

C] Traffic And Energy Saving Encrypted Search Scheme:

Traditional cloud storage system architecture and general procedures are shown in Figure 2.which include: file/index encryption by the data owner, outsourcing the data to the cloud storage, and encrypted data search/retrieval procedureof the data users in cloud computing.The basic idea behind TEES is to offload the calculation and the ranking load of the relevance scores to the cloud. It has been highlighted that offloading some computation[3].

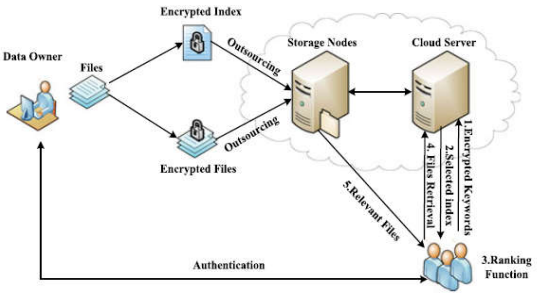

Figure2:TEES

D] **Key-revocable ABE scheme:**

A key-revocable ABE scheme for a mobile cloud environment, which realize the following functionalities:User Revocationscheme is based on the concept of the ABE scheme and achieves efficient key revocation by introducing a new entity i.e. Token Service Provider (TSP). The TSP distributes a "token" to a valid user when the user requests decryption of a cipher text. However, when the user is unauthorized, the TSP does not return a valid token, which revokes the user.

Attribute Hiding. This scheme realize attribute information hiding from a cloud server. The user terminal executes a few computations in order to mask attribute information [4].

E] **RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC):**

RSA-based AND-gate access structure CP-ABE scheme, which offers constant size secret keys and ciphertexts with efficient encryption and decryption mechanism.The proposed scheme provides constant size secret keys and ciphertexts without using bilinear maps. Then demonstrate the security of the scheme under the selective security model. To the best of knowledge, this is the first attempt to design such a provably secure RSA-based AND-gate access structure CP-ABE scheme [5].

V) ANALYSIS AND DISCUSSION

The RKSS show that it can be used distributed paralleldatabase for efficient accessed of privacy-preserving multi keyword search scheme which prove that proposed scheme is efficient and reduce the network traffic [1].

CLOAK is based on stream cipher. The three variants of the proposed scheme are referred as s-CLOAK, r-CLOAK, and d-CLOAK, varying on the modification procedure of CSPRN. The s-CLOAK and r-CLOAK are randomized approaches, while the d-CLOAK is deterministic. This found CLOAK can resist various security challenges like brute force attack [2].

TEES as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. The security of TEES based on important security threats. The most important principle of the design is to prevent the attacker from obtaining any plaintext information regarding the data file set or the searched keyword. [3].

A key-revocable ABE scheme for a mobile cloud The computational cost on a mobile device is $O(1)$, and cloud services can securely provide most computations required for the ABE scheme. Furthermore, the scheme includes a key revocation mechanism for the private keys and an attribute hiding mechanism [4].

The RSA-based CP-ABECSKC scheme offers constant size secret keys and constant size cipher texts with an expressive AND gate access structure without using bilinear maps. It evaluate that the scheme provides an efficient solution to both encryption and decryption with O(1) time-complexity. And also proved that scheme is secure against possible known attacks, such as key recovery and collision attacks, as well as under the chosen cipher text adversary [5].

Scheme	Advantages	Disadvantages
Rank Keyword Search Scheme	For reducing network traffic.	It is hard to achieve efficient network traffic and search time
CLOAK Scheme	It can used insecure wireless media by modifying the CSPRN and securing the message communication	Main security challenge is to protect the CSPRN and CT pair from the adversary.

Traffic And Energy Saving Encrypted Search (TEES)	TEES reduces the computation time	TEES is more time and energy consuming than keyword search over plain-text.
key-revocable ABE scheme	Efficient	The computational cost of ABE schemes is huge.
RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC)	Efficient and Secure against possible known attacks, such as key recovery and collision attacks	Designing a cost efficient and expressive access structure of CSKC with using conventional public-key cryptosystems remains a research challenge

TABLE 1: Comparisons between MCC Schemes

PROPOSED METHODOLOGY

AuthorizedAnd Efficient Encryption Decryption Scheme With AES Algorithm:

The proposed algorithm is for maintaining security in CPABE algorithm. The proposed scheme is used for the authentication of used and to efficient access of data for particular Admin and User. The proposed scheme used ASE encryption and AES decryption algorithm for the secure encryption decryption process. MD5 algorithm is used for the hash value generation and for authentication of valid user and data.

Authorized and Efficient Encryption Decryption Scheme With AES Algorithm:

Step1: Start

Step2: Register Admin and User.

Step3: Query or file selected by the user {q1.....qn}

Step4:Each request transfer to the system for processing

Step5: Encryption process started according to attributes with AES Encryption algorithm

Step6: Derive the set of round keys from the cipher key

While (round key !=10)

{

a. Initialize the state array with the block data (plaintext).
b. Add the initial round key to the starting state array
c. Perform nine rounds of state manipulation.
d. Perform the tenth and final round of state manipulation.
e. Copy the final state array out as the encrypted data (cipher text).

}

Step7: Now encrypted file stored in database.

Step8:If another user wants to access this file, then notification will generate and send to owner of file.

If(notification == Accept)

{

User can download a file;

}

Else

{

Request rejected;

}

Step9:Decryption process started with AES decryption algorithm

Step10:The file authentication will be check by MD5 algorithm

Input file

a) convert file in 512 blocks
b) compress all data in 128 bit
c) Divides the data in 4 blocks of 32bit
d) apply binary shifting to each block
e) Convert each block in hex value
f) combine all blocks

Step11: MD5 generate a hash value for each document. The hash value is generated two times.

First time when user send a file. Second time when another user received the file. Both hash value must be same, if they are different that means the file has been modified.

Step12: If {hash value ==match)
{
SMS will sent to owner of file using SMS gateway;
}
Step13:Stop.

VII) OUTCOME &POSSIBLE RESULT

By security analysis and performance evaluation, the proposed scheme is proved to be secure as well as efficient for encryption decryption processof CPABE algorithm and valid used authentication.

VIII) CONCLUSION

This paper focused on the study of various Rank Keyword Search Scheme, CLOAK Scheme, Traffic and Energy Saving Encrypted Search (TEES) scheme, Key-revocable ABE scheme, RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC).But there are some problems. To overcome this problems the new scheme i.e. Authorized and Efficient Encryption Decryption Scheme with AES Algorithm is proposed which proves secure and efficient scheme to enhanced the CPABE.

IX) FUTURE SCOPE:

From observation, the proposed method can be used in any data security system in future for maintain data security.

REFERENCES

C. Wang, N. Cao, K. Ren, and W. Lou, ``Enabling secure and efficientranked keyword search over outsourced cloud data,"IEEE Trans. Parallel Distributed. System. vol. 23, no. 8, pp. 1467_1479, Aug. 2012.

Zhou, Z. and Huang, D. (2011). Efficient and secure data storage operations for mobile cloud computing. Cryptology
E Print Archive, Report 2011/185.

Y. Yang, H. Cai, Z. Wei, H. Lu, and K.-K. R. Choo, ``towards lightweightanonymous entity authentication for IoT applications," in Proc. Austral.Conf. Inf. Secure. Privacy, 2016.

L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: Towards a cloud definition,” ACM SIGCOMM Compute. Communication.. Rev., vol. 39, no. 1, pp. 50–55, 2008.[2] X. Yu and Q. Wen, “Design of security solution to mobile cloudstorage,” in Knowledge Discovery and Data Mining. New York, NY, USA: Springer, 2012.

G. L. Prakash, M. Pratik, and I. Singh, ``Data encryption and decryption algorithms using key rotations for data security in cloud system," inProc. Int. Conf. Signal Propagate. Compute. Technol. (ICSPCT), Jul. 2014.