Aspect Based Logical Access Over Conceal Outsourced Input Using AES Algorithm

Iyyanar P[1], Subhikha Ku[2], Seethalakshmi S[2]

[1]*Associate Professor, Department Of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India.*

[2]*Student, Department Of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India.*

Corresponding Author: iyyanar.p@sonatech.ac.in

Abstract: - In this application, the main process is securely securing the outsourcing data. The data stored in the repository will be handled by authorized client. The authorized client will decrypt the file for the valid user; the authorized user can only retrieve data by providing a key-value to retrieve data. Searchable encryption value is identified by using Boolean expression technique. This project is based on the formulation of chemical products. The formulation of single or multi product is handled by the admin of the application. Whose data are stored encrypted by Advanced Encryption Standard (AES) algorithm, this algorithm helps to secure the outsourcing data. Those data are viewed only by the authorized laboratory of the company. The data are viewed by Boolean-Searchable expression. This application can be applied in any chemical production of products. Each formulation of products can be stored securely. The malicious attack in the database cannot occur.

Key Words: — ***Cipher text, Searchable Encryption, Public key encryption, Token, Private Keys.***

I. INTRODUCTION

Cloud computing [1] is a powerful technology which uses the Internet and remote servers to maintain large scale-data and perform complex computing. Here, the application is working between organizations from higher personnel to laboratory workers. The authorized people can only be able to control or view the formulation of chemical products and they can send that details to laboratory people. In order to ensure the confidentiality of the formulation of products it is necessary to encrypt the data before outsourcing them to cloud. This, however, prevents users from searching outsourced encrypted data as normal search algorithms cannot be executed in the encrypted domain. Searchable encryption (SE) is a cryptographic technique that allows searching specific information (e.g., keyword) in an encrypted document without learning information about the plaintext data. The key steps are as follows. First, a data owner encrypts a set of keywords which are extracted from a document into a cipher text and uploads both encrypted document and the keyword cipher text to the cloud.

Manuscript revised March 27, 2021; accepted March 28, 2021. Date of publication March 29, 2021.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898

Then, when a user needs the data to retrieve some Documents, he generates a keyword token and sends the token to the cloud. Finally, the cloud uses a search algorithm to verify which keyword cipher text matches the keyword token and sends back the encrypted document with matching keywords to the user. Two main search techniques are searchable symmetric encryption (SEE) and public key encryption with keyword search (PEKS) [2]. In an SSE system, only the secret key holder can generate keyword cipher texts under a data owner's public key, but only the private key can perform searches. Thus, SSE is more suitable for single user write and read data, whereas PEKS is used in multiuser writing and single user reading application scenarios. Most of the existing SE schemes only support single keyword search [3-9]. In such cases, data users must download, filter and process a large amount of data in order to get relevant results, which obviously lack practicality. Multi-keyword SE schemes (e.g., conjunctive and disjunction) can also be found in literature, but they typically support single-user searches, that is, just the data owner can submit search queries.To address the challenge of developing a multi- Keyword mechanism that simultaneously enables multiuser writer and searching over outsourced encrypted data, we propose in this paper a multiuser And multi-keyword public-key searchable primitive Support fine-grained search control by using Attribute-Based Encryption (ABE). We name our approach as attribute-based hybrid Boolean keyword Search over

outsourced encrypted data. Note that, by "Hybrid", we mean in our context that a set of keywords consists of two parts:

Values and **names** as illustrated

The main contributions of this paper are:

- The proposed primitive allows data owners to control the search permission for their outsourced encrypted data according to an access control policy. If his attributes satisfy the access control policy, any user can perform a keyword search. This means that our primitive supports multiuser search.
- In addition, every user with a set of attributes can generate a delegated key for another who has a more restricted set of attributes.
- In our design, all authorized users can perform any desired Boolean keyword expression search such as an access tree structure, which is a more expressive searchable mechanism.
- Our primitive is based on the prime order bilinear groups. We formally define a security model for primitive and prove it to be secure under this model. Performance evaluation shows that our primitive is efficient and practical.

II. RELATED WORK

SE is a technique that allows the data owners to outsource their data in encrypted forms to cloud servers where the encrypted data can be retrieved selectively without leaking any information about the data. In the following, we shall introduce the state of the art symmetric and public key SE schemes.

SSE schemes: In 2000, concept of SSE and presented several practical SSE constructions. In 2003, Go [10] proposed the first security definition for SSE construction and efficient and secure SSE construction based on Bloom filters. In 2005, change and Mitzenmacher [11] proposed a stronger security

Definition for SSE schemes which guarantees query privacy and data privacy. After that, several SSE schemes of various security and efficiency level have been proposed [8]-[9]. However, all these SSE schemes are limited to single-keyword search, which requires the data owners to specify a single keyword to search on and then receives all of the encrypted data with the same keyword. Consequently, a single keyword search is insufficient to meet the practical requirements as most of the practical systems require a more complicated search.

In order to, resolve the above problem, in 2004, Galle teal. First proposed the concept of conjunctive keyword search which makes a search over an encrypted data with several keywords in a single query. Obviously, it is more efficient than repeatedly utilizing a single-keyword query. They defined a security model for conjunctive keyword search on encrypted data and presented two secure SSE schemes. After that, a few multi keyword SSE schemes including conjunctive queries, disjunction queries, Boolean queries, range queries and substring queries have been proposed [12]. Nevertheless, all of these schemes just support single-user queries. In some cases, it is more desirable in SSE schemes that an arbitrary group of parties other than the owner can submit search queries.

PEKS schemes: In 2004, Bone et al. [13] first introduced the concept of PEKS and presented two provably secure PEKS construction based on an anonymous identity-based encryption (IBE) construction, where the cipher text does not leak the identity of the receiver. In 2005, Abdulla et al. [14] demonstrated that an anonymous IBE scheme scan be transformed to a secure PEKS schemes. However, all the above works reveals specific keywords which are contained in cipher text to the cloud server. In 2006, Bone teal solved this problem and proposed an efficient PEKS schemes without revealing any partial information regarding the authorized user's search. In 2008Bao et al, introduced a set of security notation for multiuser SE and proposed a secured construction. Later several multiuser schemes proposed. Nevertheless, all these constructions either dealt with the single-keyword search or are in single user settings. It is also desired with a more complicated search for practical application in multiuser PEKS settings.

In 2004, Park et al defined a security model for PEKS with conjunctive keyword search and proposed two efficient search constructions which partly hide keywords as the search token reveals the positions of keywords which are needed to query encrypted data. Several variation schemes have been proposed to support conjunctive queries. In order to achieve more expressive queries. In 2006, Bone and water constructed a predicate encrypted scheme based on hidden vector encryption with conjunctive, subset and range queries on encrypted data. In 2008, Katz et al also proposed a predicate encryption supporting inner product queries which are strictly more expressive than conjunctions. However, both two

schemes fully expose the privacy for search queries. In 2013, Wang et al presented an ABE schemes with a single keyword search function construction. However, data users need to interact with trusted authorities to obtain the private keys and search tokens. In 2014, Shi et al proposed an authorized keywords search schemes that support arbitrary Boolean formula search and utilizes the variant of dual-policy ABE schemes with partially hidden access structure. However, all these schemes are based on the composite-order bilinear groups, which are less desirable than prime-order bilinear groups due to efficiency and security. In 2014, Zhen get al. [15] proposed attribute-based schemes for verifiable keyword search over outsourced encrypted data, which allows data owners to control policy for encrypted data and allows data owners to verify the correctness of search. Although their schemes are in multiuser settings, it also supports the single keyword search. In this paper we propose an efficient SE schemes supporting hybrid keyword Boolean search and multiuser search in prime-order bilinear groups. In addition, our schemes achieve fine-grained search permission for outsourced encrypted data by utilizing attribute- based cryptography.

III. PRELIMINARIES

A. Bilinear Groups

G is an algorithm, which takes an input a security parameter l and output a tuple (p,G,GT,e) where G and GT are multiplicative cyclic groups with prime order p and e: G X G->GT is a map, which has the following properties:

Bilinearity: e $(g^a,h^b)=e(g,h)^{ab}$ for all g,h subset G and a,b subset Z^p

Non degeneracy: There exist g,h subset G such that e(g,h) $!=1_G$

Computability: There exist an efficient algorithm to compute e(g,h) for all g,h subset G

B. Definition of the Algorithm

We use AES algorithm also known as the Rijndael algorithm is a symmetrical block cipher algorithm that takes plain text in block of 128 bits and converts them to cipher text using keys of 128,192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard.

The following are the AES Encryption Process

- Derive the set of round keys from the cipher keys.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.

We propose an attribute-based Boolean keyword SE scheme which is based on PEKS [35] and ABE [52]. It consists of the following polynomial-time algorithm. Setup (1^l): Take as input a secure parameter l, output a public parameter PK and a master key MK.

*KeyGen (*MK, S): Take as input a master key MK and a set of attribute S, output a private key SK_s.

Encrypt (PK, A, W): Take as input a public parameter PK, an access structure A over the universe of attributes and a set of keywords W, output a cipher text $CT_{(A,W)}$.

Token (SK, Beta): Take as input a private key SK_s and a Boolean expression over the universe of keywords, output a search token $TK_{(s,beta)}$

Search: ($CT_{(A,W)}$,$TK_{(S,BETA)}$): Take as cipher text as input $CT_{(A,W)}$and a search token $TK_{(s,BETA)}$ output as "YES". If the set of attributes S satisfies the access structure A and the set of keywords W satisfies the Boolean expression.

Remark: There does not exist a decryption algorithm in the above definition since, we use private key SK_S to decrypt the cipher text CT $_{(A,W),}$ we only got the intermediate random value.

C. Security Model

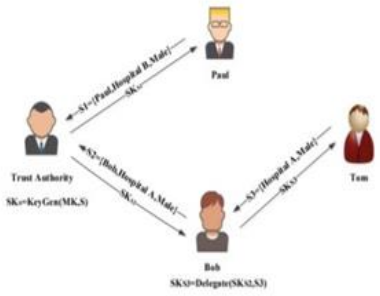

Fig.1. Generate user's private keys

We define a security model for attribute-based Boolean keyword SE in the sense of semantic security under the chosen keyword attack via the following game between a

challenger C and an adversary A is able to obtain trapdoors for any set of keywords of choice. Nevertheless, without any matching search tokens, the adversary A learns nothing about the keyword's values in the challenge cipher text. The security model is slightly weaker one, as the adversary A needs commit the access structure a need to commit an access structure "A" to the challenger C at the beginning of the game.

Setup: First, the adversary A sends a challenge access structure A to the challenge C. then the challenge C runs the setup (L^{l}) to obtain the public parameter PK and master key MK. Finally, the challenger C gives the public parameter PK to the adversary A and keeps the master keys MK by himself.

Phase 1: The adversary A adaptively issues a polynomial number of queries as follows:

KeyGen Query(S): If the set of attribute S satisfies the access structure A*, the challenger C aborts, otherwise C returns SK_S<- KeyGen (MK,S) to A.

Token Query (S, BETA): If the adversary has queried SK_S to the challenger C directly runs ($TK_{(S,BETA)}$)<- Token(SK_S,BETA) otherwise C runs first Sk_S<- KeyGen(MK,S).

IV. Search For Outsourced Encrypted Data

We first describe the architecture if the architecture of the attribute-based Boolean keyword search SE system and then present the details of the algorithm as well as the security analysis.

A. Architecture

The system contains four entities:

- *Data Owner* who outsourced his encrypted data to the cloud and controls who can search his outsourced encrypted data.
- *Authorized User* whose attribute satisfy the access structure of the keyword cipher text and thus who can retrieve the data's owner outsourced data.
- *Cloud Server* who provides the storage and computational services such as storing the encrypted data and searching for the encrypted data on behalf of authorized users.
- *Trust Authority* who generate private keys to all the users in the systems.

In the following we elaborate how the system works. Suppose the data owners have multiple encrypted data, each of which is associated with the set of keywords W, where the set of keywords values forms W_V and a set of keyword name forms W_N. First the data owner encrypts W_V under the access tree T. then an authorized user generates search tokens TK under the desired Boolean keyword values expression. Finally, the cloud server uses the search token TK to retrieve the encrypted data. The detailed process is as follows:

- *Obtain Private Keys:* Each user sends the attribute S to the trust authority to obtain the private keys SK_S Additionally, as illustrated in fig 2 any user who owns the private keys SK_S with respect to the attribute S_i can use private keys to further generate a delegated key SK_S for another user with the attribute S_J where S_j subset of S_i. In such a way of key delegation, the trust authority workload can be reduced.
- *Outsourced Encrypted Data:* For each encrypted data, the data owner first encrypts the set of keyword values W_V under the access tree T.
- *Generate Search Tokens:* An authorized user whose attribute S satisfy the access tree Towns the search permission. He uses his private keys SK_S to generate the search token TK under any desired keyword value expression BV and sends the Boolean keyword value expression B_N along with the search token TK to the cloud server. This is shown in fig 4.

B. Search encrypted Data

The cloud server first finds the minimum subset of keyword names in the keyword cipher text CT satisfying the Boolean keyword name expression BN in the search token TK. Then the cloud server checks the weather the keyword matches the Boolean key words value expression BV in the search token TK. If the match is successful, the cloud server returns all the matched encrypted data to the authorized users. Otherwise, it continues to find the other set of subset names. In our systems there exist six desired functional requirements as follows.

- *Keyword confidentiality:* Without any matching search token, the adversary A learns nothing about the keyword values from the keyword cipher text.
- *Multiuser Search:* Any user whose attribute satisfy the access control policy of the keyword cipher text is allowed to perform retrieval operation upon the encrypted data.
- *Boolean Queries:* Authorized users are able to perform any desired Boolean keyword expression search.

- *Access Control:* The data owner can control the search permission for his encrypted data which is outsourced from the cloud.
- *Key Delegation:* Any user with a set of attribute S can generate a delegated key for another users who has more restricted set of attributes S^1
- *Collusion Resilient:* Unauthorized users cannot obtain any keyword information from the keyword cipher text, even though they collude with each other.

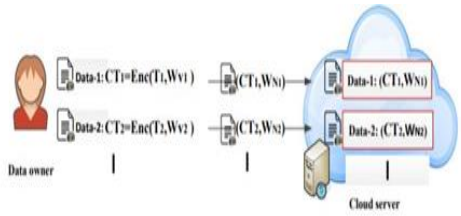

Fig.2. Data owner outsourced his encrypted data to the cloud and a set of search permission according to the access control policy

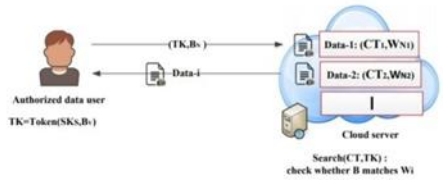

Fig.3. Authorized users performs any desired Boolean keyword expression search

C. Construction

Here presents the concrete algorithm for our attribute-based Boolean keyword SE schemes. The main idea of this scheme is motivational from an attribute-based single keyword search scheme [15]. Here we use algorithm called *AES algorithm* which is more advance than MD5 algorithm where AES algorithm is more secured and more advanced when compared to MD5 algorithm.

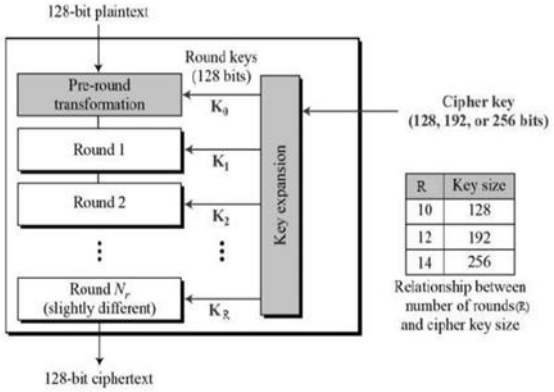

Fig.4. AES Algorithm Structure

AES is an iterative rather than *Festal cipher*. It is based on substitution permutation network. It comprises of a series of linked operations, some of which is involved replacing input by specific output and other involved shuffling bits around (permutation). AES performs all of its permutation on bytes rather than bits. Hence AES treats the 128 bits of plaintext blocks as 16 bytes. These 16bytes are arranged in four columns and four rows for processing the matrix.

Encryption Process: In this AES algorithm encryption and decryption both are involved, in this encryption process

- Byte substitution
- Shift Rows
- Mix columns
- Add round keys

Decryption Process: The process of decryption of AES cipher text is similar to the encrypted process in the reverse order. Each round consists of the four processes conducted in the reverse order

- Add Round keys
- Mix Columns

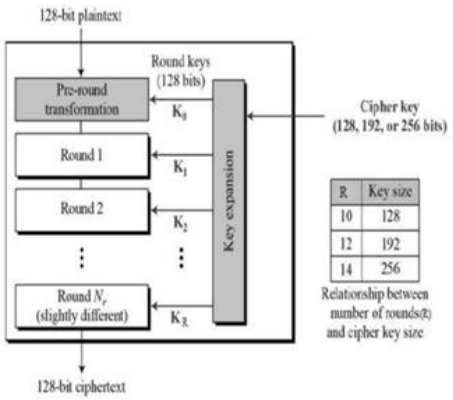

Fig.5. AES Algorithm Festal Structure

- Shift Rows
- Byte Substitution

V. PERFORMANCE EVALUATION

- *Upload Process*: The admin of the company will update the information of each product in secured manner. The data are stored in encrypted form, the technique used to convert the data is MD5 algorithm which converts the normal text to encrypted form, only the authorized member can access the information in decrypted form. The data which stored in secure format so there is no leakage of data.
- *File Transact*: The transaction of data from the highest of the company to the laboratory will be in encrypted form, data are in formulation, increment, form etc.…of each product are transferred from higher of the company to lower official.
- *Keyword Search*: There is technique used for the search process is called Hybrid Boolean Keyword search, this process will select the data from the through of list by using keyword. The Keyword search process is referring the details for the authorized user will be using the data for testing process and then they will promote for the manufacturing process.
- *Download Process:* The download process is for accessing the data for offline purpose, this process is useful for the referring all times. The only authorized member can access the data for the production.

VI. PROPOSED SYSTEM

In this application, the main process is securely securing the outsourcing data. The data stored in the repository will be handled by the authorized client. The authorized client will decrypt the file for the valid user. The authorized user can only retrieve the data. Searchable encryption value is identified by using the Boolean expression technique. The project-based on the formulation of chemical product. The formulation of the single or multi-product is handled by the admin of the application whose data are stored in the encrypted by AES algorithm, this technique helps to secure the outsourcing data, those data are viewed only by the authorized laboratory of the company. The data are viewed by using the Boolean searchable encryption. This application can be applied in any chemical production of products. Each formulation of the product can be stored securely. The malicious attack in the database will not occur.

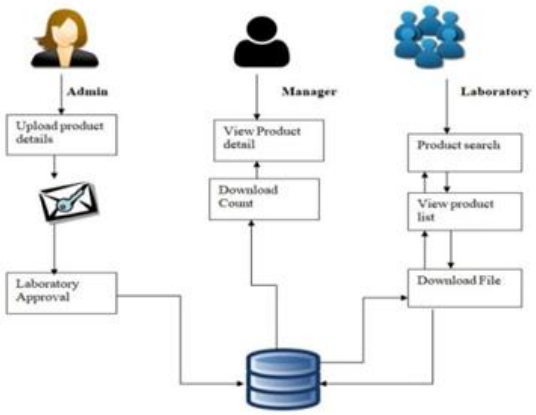

Fig.6. Architecture

VII. CONCLUSION

This paper presented a new cryptography primitive, which supports Hybrid Boolean Keyword search for outsourced encrypted data in attribute –based settings. Especially the data owner can control the search permission for his encrypted data. Additionally, every user can delegate a private key to another user with restricted credentials and we also used AES algorithm techniques and concept which is more secured and advance in technique. The evaluation shows that the primitive is very efficient and practical. We also analyzed the security of the primitive under our security model.

REFERENCES

[1]. M. Arm burst, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Kaminski, G. Lee, D. A. Patterson, A. Rabin, I. Stoical, and M. Zaharias, "A View of cloud computing", Common. ACM, vol. 53, no.4, pp. 50-58, 2010.

[2]. C. Bosch, P. Hartel, W. Jonker, and A. Peter, "A Survey of probably secure searchable encryption, "ACM Computing Surveys, Vol.47, no. 2, pp. 18:1-18.51, 2014.

[3]. S. Kumara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in the ACM conference on computers and communications security, CCS,12, Raleigh, NC, USA, October 16-18, 2012, 2012, pp. 965-976.

[4]. K. Kurosawa and Y. Ohtaki, "Uc- secure searchable symmetric encryption," Financial cryptography and data security - 16th International conference, FC 2012, Kralendijk, Bonaire, February 27 – March 2, 2012, Revised Selected papers, 2012, pp. 285-298.

[5]. S. Kamara and C. Papamouthou, "Parallel and dynamic searchable symmetric encryption", in Financial cryptography and data security – 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers, 2013, pp. 258-274.

[6]. S. Jareki, C. S. Jutla, H. Krawcyzk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in 2013 ACM SIGSAC conference on computer and communications security, CCS'13, Berlin, Germany, November 4-8, 2013,2013, pp. 875-888.

[7]. D. Cash, J. Jarecki, C. S. Jutla, H. Krawcyzk, M. Rosu, and M. Steiner, "Higher-scalable searchable symmetric encryption with support for Boolean queries," in Advances in cryptography – CRYPTO-2013 – 33rd Annual cryptology, Santa Barbara, CA, USA, Aug 18-22, 2013. Proceedings, part I, 2013, pp. 353-373.

[8]. D.Cash, J. Jarecki, C. S. Jutla, H. Krawcyzk, M. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: "Data structures and implemention", in 21st Annual network and distributed system security symposium, NDSS, 2014, an diego, California, USA, February 23-26,2014, 2014.

[9]. M. Naveed, M. Prabakaran, and C. Guntur, "Dynamic searchable encryption via blind storage", in 2014 IEEE symposium on security and privacy, SP 2014, Berkeley, CA, USA, May 18-12, 2014, 2014, pp. 639-654.

[10]. E. Goh, "Secure Indexes", IACR, cryptology eprint Archieve, vol. 2003, p. 216, 2013.

[11]. Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data", in Applied cryptography and network security, Third international conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, proceedings, 2005, pp. 442-455.

[12]. P. Golle, J. Staddon, and B.R. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and network security, second international conference, ACNS 2004, Yellow Mountain, china, June 8-11, 2004, proceedings, 2004, pp. 31-45.

[13]. D. Boneh, G. D. Crescendo, R. Ostrovsky, and G. Persian, "Public key encryption with keyword search," in Advances in cryptology- EUROCRYPT 2004, International conference on the Theory and Applications of cryptographic techniques, Intertaken, Switzerland, May 2-6, 2004, Proceedings, 2004, pp. 506-522.

[14]. M. Abdulla, M. Bellare, D. Catalano, E. Klitz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Pailier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions", in Advances in cryptology – CRYPTO 2005: 25th annual international cryptology conference, santa Barbara, California, USA, august 14-18, 2005, proceedings, 2005, pp. 205-222.

[15]. Q. Zhen, S. Xu, and G. Ateniese, "VABKS: verifiable attribute based keyword search over outsourced encrypted data," in 2014 IEEE conference on computer communications, INFOCOM 2014, Toronto, Canada, April 27 – May 2, 2014, 2014.