Journal of Theoretical and Applied Information Technology
15th March 2022. Vol.100. No 5
2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT ACCESS POLICY WITH MULTI-LINEAR SECRET-SHARING SCHEME IN CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

ANCY P R[1], ADDAPALLI V N KRISHNA[2], BALACHANDRAN K[3], BALAMURUGAN M[4]

[1] Research Scholar, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

[2] Professor, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

[3] Professor, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

[4] Associate Professor, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

E-mail: [1]ancy.prasadam@res.christuniversity.in, [2]adapalli.krishna@christuniversity.in

ABSTRACT

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a system in which attribute are used for user's identity and data owner determine the access policy to the data to be encrypt. Here access policy are attached with the ciphertext. In the form of a monotone Boolean formula monotone access structure, an access policy can be interpreted and a linear secret-sharing scheme (LSSS) can be implemented. In recent CP-ABE schemes, LSSS is a matrix whose row represent attributes and there exist a general algorithm which is proposed by Lewko and Waters it transforms a Boolean formula into corresponding LSSS matrix. But we may want to transform the monotone Boolean formula to an analogous but compressed formula first before applying the algorithm. This is a very complex procedure and require efficient optimization algorithm for obtaining equivalent but smaller size Boolean formula. So in this paper we are introducing an extended LSSS called multi-linear secret-sharing scheme where we can eliminate above optimization algorithm and directly convert any Boolean formula to multi-linear secret-sharing scheme.

Keywords: *Ciphertext Policy Attribute Based Encryption, Access Policy, Multi-Linear Secret-Sharing Scheme, Encryption*

1. INTRODUCTION

Attribute based encryption (ABE) is useful for applications where data provider according to some policy, he wants to share data based on receiver's attribute. Sahai and Waters provide this new scheme for the access control of any encrypted data. It is a form of public key encryption, where instead of one-to -one communication it provide one-to-many communication. ABE works on the concept of set of attributes.Where a user's secret key and cyphertext depend onattributes.And ciphertext decryption is on ly possible if the user key set and the ciphertext attributes matches. ABE has two variants called KP-ABE and CP-ABE called Key-Policy ABE and Ciphertext-Policy ABE. Data owner encrypt the data using attributes and this encrypted data is decrypt using secret key associated by access policy in KP-ABE. And in the case of CP-ABE data is encrypted using access policy and decrypted by secret key associated with set of attributes. In this paper we are focusing on CP-ABE.

Threshold, tree structure called access control tree and secret sharing mechanism are the three categories of access structure that are used mainly. Threshold structure (k, n) by lagrange interpolation theorem divides the secret information s into n sections and the secret s can be only reconstructed when no less than k information cooperates. The tree structure called access control tree effectively

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

enhance the access structures expressiveness[1,2]. In order to allow the access structure to express more complex logical relationships between attributes, it combines many "AND", "OR" and "threshold " operations.In terms of the monotone Boolean formula or monotone access structure, access policy can be represented and can be realised via linear secret sharing schemes (LSSS)[3]. In this paper we are introducing a variation of LSSS called multi-linear secret-sharing scheme.

Most common representation of monotone access structure is LSSS matrices[4]. An algorithm was proposed by Lewko and Waters for converting Boolean formula to LSSS matrices. Ciphertext include (M, ρ) which is nothing but LSSS matrix where M represent matrix and ρ is a function which maps row of matrix to an attribute. As an example an LSSS matrix is given in Fig 1 which representing an access policy.

$$M = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \quad \begin{matrix} \rho(1) = P \\ \rho(2) = S \\ \rho(3) = Q \\ \rho(4) = R \end{matrix}$$

Figure 1: An LSSS matrix example with each row represent attributes P, S, Q and R respectively.

According to the algorithm before converting to LSSS matrices any formula should be in compressed or minimal form. This include more complexity into CP-ABE scheme. So in this paper we propose an extension of LSSS called multi-linear secret sharing scheme in which the we can convert any Boolean formula into LSSS matrix without converting to a minimal form.

1.1 Related Work

Attribute based encryption is first introduced by Sahai and Waters[5] in the paper fuzzy identity based encryption that provide a new means for encrypting data. Goyal et al[6], in there paper divide ABE into two category as KP-ABE and CP-ABE. Data owner encrypt the data using attributes and this encrypted data is decrypt using secret key associated by access policy in case of KP-ABE. And in the case of CP-ABE data is encrypted using access policy and decrypted by secret key associated with set of attributes. In this they mainly focused on KP-ABE. Bethencourt[7] introduces a scheme for the identification of encrypted information with complex access control called CP-ABE. According to the work, the author proposed that even if the storage server is untrusted, the information could be kept confidential. And also, this method is secure against collusion attacks. In this paper, the author used the concept of attributes. The characteristics are used to define the credentials of a user[8,9,10], and information is determined by a party encryption policy for who can decrypt.

Chase, M. [11] suggested a scheme can withstand any number of corrupt authorities. The author applies this technique to attain a multi-authority form of identical access control Attribute-Based Encryption. According to this scheme each user has to prove his set of attributes to the third party to obtain a secret key[12]. The main challenge of single authority Attribute-Based Encryption is preventing collusion. This problem is addressed in this paper by introducing the multiauthority scheme. Currently available CP-ABE schemes are provably secure and used for highly expressed access policies like linear secret-sharing scheme[13,14,15,16]. LSSS matrix are used to represent corresponding monotone access structure[17,18]. A threshold secret sharing scheme was introduced by Shamir[19]. Brickell[20] develop some ideal scheme based on ideal secret sharing scheme for some access structure.

1.2 Our Contribution

In this paper, we propose a new CP-ABE scheme, which is based on extended LSSS called multi-linear secret-sharing scheme. Which does not require a complex conversion or simplification of Boolean formula.

- Our scheme uses multi-linear secret-sharing scheme which can directly apply to any complex Boolean formula and can be convert it into corresponding LSSS matrix.
- Our CP-ABE scheme is constructed with this multi-linear secret sharing scheme as access policy and reduce the complexity and improved efficiency.

1.3 Organization

We present some preliminaries and definitions in section II. In section III and IV we define and describe our construction in CP-ABE scheme with multi-linear secret sharing scheme and security analysis. Section V we include some open problem.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. PRELIMINARIE

This section provides some definitions and background information that are used for the CP-ABE schemes.

2.1 Bilinear Mapping

Consider $\mathbb{G}$ and $\mathbb{G}_T$ as two cyclic (multiplicative) groups and of prime order p. Bilinear mapping is represented as $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ having following three properties.

- Bilinearity: This is for any $g \in \mathbb{G}$ and any $\alpha, \beta \in \mathbb{Z}_p$, $e(g^\alpha, g^\beta) = e(g,g)^{\alpha\beta}$.
- Nondegeneracy: For a generator g of $\mathbb{G}$, $e(g,g) \neq 1_{\mathbb{G}_T}$.
- Computability: That is for any $g \in \mathbb{G}$ and any $\alpha, \beta \in \mathbb{Z}_p$, an algorithm is there to compute $e(g^\alpha, g^\beta)$ in polynomial time.

2.2 Access Structure

Let set $\{P_0, P_1, \ldots, P_{n-1}\}$ denotes parties. The collection $\mathbb{A} \subseteq 2^{P_0, P_1, \ldots, P_{n-1}}$ where access structure $\mathbb{A}$ is called monotone if it satisfies $X \in \mathbb{A}$ and $X \subseteq Y$ imply $Y \in \mathbb{A}$. Access structure is an monotone collection $\mathbb{A}$ of subsets in $\{P_0, P_1, \ldots, P_{n-1}\}$ which should be non-empty. Authorized sets are the sets in $\mathbb{A}$. The set B is called minimal set in $\mathbb{A}$ if and only if $B \in \mathbb{A}$, and for each $C \subsetneq B$ it should be $C \notin \mathbb{A}$[21].

2.3 Linear Secret Sharing Schemes (LSSS)

We can call a secret sharing scheme Π over a set of parties $\mathcal{P}$ as linear (over $\mathbb{Z}_p$) if it satisfies following two conditions such as:

- A vector over $\mathbb{Z}_p$ is formed by shares of party and
- There exists a matrix M called the share-generation matrix for Π. M contains p rows and q columns. And for every i, where i =1,2,…,p, the i^{th} row M_i of matrix M can be denoted by a party $\rho(i)$ where this ρ is a function from {1,2,…,p} to $\mathcal{P}$. Column vector $\vec{v}$ is given such that $\vec{v} = \{s, r_2, r_3, \ldots, r_q\}$, where $s \in \mathbb{Z}_p$ represent the secret which is to be shared and $r_2, r_3, \ldots, r_q \in \mathbb{Z}_p$ are chosen randomly. Vector $M\vec{v}$ is p shares of the secret s according to Π. The share $\lambda_i = (M\vec{v})_i$, ie, the inner product $M_i.\vec{v}$ which belongs to party $\rho(i)$.

As define in [22], any LSSS as we define above is reconstructed as follows. Let authorized set be $S \in \mathbb{A}$, and $I \subset \{1,2,\ldots,m\}$ is defined as $I = \{i: \rho(i) \in S\}$. There exist an constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ satisfying $\sum_{i \in I} \omega_i M_i = (1,0,\ldots,0)$, so that if$\{\lambda_i\}$ are valid shares of secret s, then $\sum_{i \in I} \omega_i \lambda_i = s$. Also, these constants $\{\omega_i\}$ can be calculated in polynomial time in the size of the share-generating matrix M. There is no such constant for unauthorized set. The LSSS is represented by (M, ρ), and the number of rows of M, that is p denotes its size.

3. OUR CONSTRUCTION

3.1 Overview

We provide the construction of the CP-ABE scheme in this section. The system contains below mentioned entities. The diagrammatic representation of system is shown in Fig 2.

- Attribute authority: Attribute authority control attribute universe. It generates its own master secret key and public parameter. Its main duty is to check validity of the user's attribute. If that is an authorized user it sends a secret key according to his attribute.

- Data Owner: Data owner is the one who wants data to store in a third party storage. Based on an access policy that who are all the user that can read his message, he/she will create an access policy and message is encrypted with that access policy.

- User: Each user has set of attributes and its corresponding secret key. If secret key of a user matches the access policy of message he/she can read the message. Otherwise the permission will be denied.

- Semitrusted third party storage: This entity is in charge of storing outsourced data, ie data owner encrypts data and send to third party storage. This is the place where user store data and it can be any kind of storage service.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

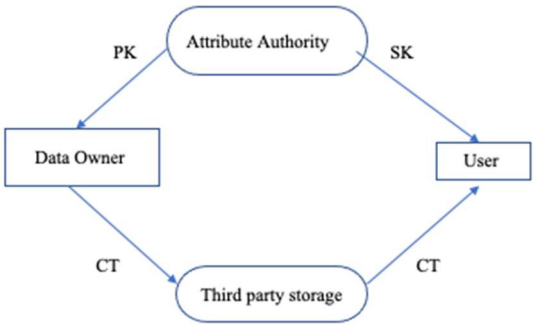


Figure 2: Framework of Attribute-Based Encryption.

3.2 Framework

In our framework we have four algorithms such as: Setup, Encrypt, KeyGen, and Decrypt. We will explain each algorithm in detail.

Setup $(\lambda, \mathrm{U}) \rightarrow (PK, MSK)$ The input to this algorithm are security parameter λ and attribute universe U. Public parameters PK and a master key MSK are the outputs. This algorithm initialise the system.

Encrypt $(PK, \mathbb{A}, M) \rightarrow CT$ This algorithm is to encrypt the message for that it takes input as public parameters PK, a message M, and an access structure $\mathbb{A}$. Output is the respective ciphertext CT. It can decrypt only by an user that having attributes that satisfies the access structure.

KeyGen $(MSK, S) \rightarrow SK$ The algorithm generates private key SK by taking input as master secret key MSK, and a set of attributes S.

Decrypt $(PK, CT, SK) \rightarrow M$ The decryption algorithm decrypts ciphertext and generate back message by taking input as the public parameters PK, a ciphertext CT, which contains an access policy, and a private key SK. If set S of attributes satisfies the access structure, then the algorithm returns message M.

In this frame work we have four algorithm each algorithm is executing in different entity. The algorithms Setup and KeyGen are executed by attribute authority. In the case of Setup attribute authority generate public parameters and master key. And in the case of KeyGen algorithm attribute authority generate private key for each user. The Encrypt algorithm is executed in data owner entity to encrypt the message. The Decrypt algorithm is executed by user side to decrypt the message.

4. MULTI-LINEAR SECRET-SHARING IN CP-ABE SCHEME

4.1 Construction

In this section we have shown the construction of LSSS matrix and multi-linear secret sharing scheme which is the proposed one. In the case of CP-ABE the data owner encrypts the data with access policy and store it in third party storage. This access policy represents who all can decrypt this data. Each user will have a set of attributes. Based on this attribute a secret key is generate. The user will use this secret key to decrypt data. If the attributes in the secret key matches the attribute in access policy, he is an authorized user and he can decrypt the data otherwise he can't access the data.

4.1.1 Linear Secret Sharing Matrix Construction

Lewko and Waters developed an algorithm that construct a LSSS matrix from any Boolean formulas [23]. Below we are explaining this algorithm briefly with an example. The input is any access tree, that is the representation of any monotone Boolean formula. Output is the corresponding LSSS matrix. First, we have to convert monotone Boolean formula to equivalent but shorter form.
For example, if the boolean formula is:
$T \wedge ((P \wedge Q) \vee (P \wedge R) \vee (P \wedge S) \vee (Q \wedge R) \vee (Q \wedge S) \vee (R \wedge S))$
The equivalent but compressed boolean formula is
$T \wedge (((P \wedge Q) \vee (R \wedge S)) \vee ((P \vee Q) \wedge (R \vee S)))$
The algorithm first initializes root node vector, v as (1), is a vector and its length is 1. Then initialize counter variable, c as 1. As next step it goes down each level and labels each node as follows:

- Parent node: OR gate with vector v
  label both child as v
  c is unchanged;

- Parent node: AND gate with vector v,
  Append v with 0's at end and make it same as the length of c
  label left child with vector v||1 (|| represent concatenation)
  right child with vector (0,….,0)||-1 ((0,…,0) is of length c) increment c by 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As an example consider the Boolean formula P AND (S OR (Q AND R)). The access tree representation of the given formula is shown below in Fig 3 with the labels for each node we got after applying Lewko and Waters algorithm.

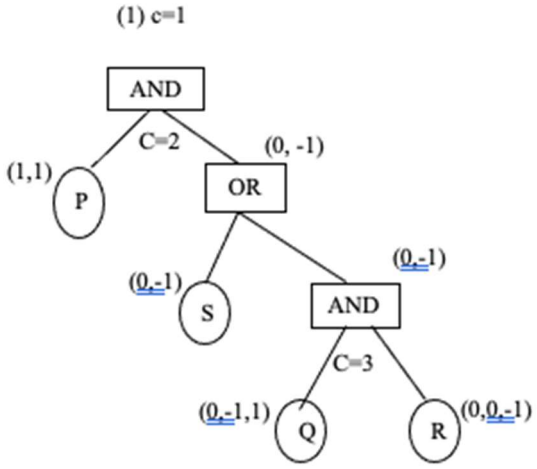


Figure 3: Access tree representation of the Boolean formula P AND (S OR (Q AND R)).

The rows of LSSS matrix are corresponding labelling of leaf node. We append shorter length vector with 0's to form same length vectors. LSSS matrix is:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \begin{matrix} \rho(1) = P \\ \rho(2) = S \\ \rho(3) = Q \\ \rho(4) = R \end{matrix}$$

A secret sharing scheme $\prod$ over a set of parties $\mathcal{P}$ (attributes) is called linear if:

Given a column vector $v = (s, r_2, \ldots, r_n)$

$$v = \begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}$$

The secret is 2 and the share $\lambda_i = (M\, v)_i$, belongs to party $\rho(i)$

$$\lambda_1 = [1 \quad 1 \quad 0] \begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}$$

$\lambda_1 = 6$
$\lambda_2 = -4$
$\lambda_3 = 1$
$\lambda_4 = -5$
$I = \{i : \rho(i) \in S\}$

$I = \{\{1,2\}\{1,3,4\}\}$, Which means the authorized ser are {{P,S},{P,Q,R}}.
There exist constants $\{\omega_i \epsilon Z_p\}_{i \epsilon I}$ satisfying $\sum_{i \epsilon I} \omega_i M_i = (1,0,\ldots\ldots,0)$
So that if $\{\lambda_i\}$ are valid shares of any secret s according to $\prod$, then $\sum_{i \epsilon I} \omega_i \lambda_i = s$

Consider {1,2}

$$\sum_{i \epsilon I} \omega_i M_i = (1,0,\ldots\ldots,0)$$
$$\omega_1[1 \quad 1 \quad 0] + \omega_2[0 \quad -1 \quad 0] = (1,0,0)$$
$$[\omega_1 \quad \omega_1 \quad 0] + [0 \quad -\omega_2 \quad 0] = (1,0,0)$$
$\omega_1 = 1$, $\omega_2 = 1$

$$\sum_{i \epsilon I} \omega_i \lambda_i$$
$$= 1*6 + 1*-4$$
$$= 2$$

which is the secret.
ie, {P,S} is an authorized set.

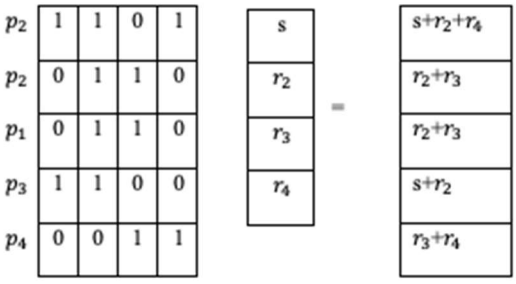
Consider {1,3}

$$\sum_{i \epsilon I} \omega_i M_i = (1,0,\ldots\ldots,0)$$
$$\omega_1[1 \quad 1 \quad 0] + \omega_3[0 \quad -1 \quad 1] = (1,0,0)$$
$\omega_1 = 1$, $\omega_3 = 1$

$$\sum_{i \epsilon I} \omega_i \lambda_i$$
$$= 1*6 + 1*1$$
$$= 7$$

which is not the secret.
ie {P,R} is an unauthorized set.

In general,



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1.2 Multi-linear Secret Sharing Scheme

Multi linear secret sharing scheme are natural generalization of linear schemes[24]. From the above example of LSSS matrix we saw that it use a linear mapping to share the secret. Also, in case of LSSS secret is an one field element but in the case of multi linear secret sharing scheme secret is more than one field element. As it contains secret in more than one field this will increase the security of the whole scheme. In the example below we have shown two rows as secret but we can have any number of rows as secret. For larger case which means for more number of rows we can have more number of secret as it will increase security of the scheme.

As we can see the number of secrets increases the complexity also increases that will increase the security of the whole scheme. As same as normal linear seret sharing scheme this can also apply to any complex Boolean formula. This is easy to implement as same as linear secret sharing scheme and it is applicable to any type of attribute-based encryption. It can be used in KP-ABE or CP-ABE. Also, it can be implemented in any complex access policy. AS it is similar to LSSS which is already using in access policy this is easy to implement just we have to add some modification to the existing scheme.

Below we have shown a general form of multi-linear secret sharing scheme. In this case there is two secret and two random number. This is one case, in general we can have n number of secrets. This will increase the complexity of the structure as well as security. So, there is an option which we can decide on the number of secrets. The whole scheme is worked based on the number of secrets. The main advantage of multi-linear secret sharing scheme is that it ia applicable to any kind of attribute-based encryption scheme also it can apply on any complex Boolean formula.

There are many access policy such as Boolean, access tree, linear secret sharing matrix each has their own advantages and disadvantages. Our scheme is a variation linear secret sharing scheme which has all its feature and advantages plus some more additional features and advantage which makes our scheme more reliable.

In general,

p_1	0	0	1	0	s_1	r_3
p_2	1	0	1	0	s_2	s_1+r_3
p_3	1	0	2	0	r_3 =	s_1+2r_3
p_1	0	1	0	1	r_4	s_2+r_4
p_2	0	2	0	5		$2s_2+5r_4$
p_3	0	4	0	7		$4s_2+7r_4$

We will explain this with an example,

In the below example we have included two secret which is 2 and 4 and the random number is 5. Here we have four users they are P, Q, R and S.

P	1	1	0	2	6
S	0	-1	0	4	-4
Q	0	-1	1	5 =	1
R	0	0	-1		-5

Consider {1,2}

$$\sum_{i\in I}\omega_i M_i = (1,0,\ldots\ldots,0)$$

$\omega_1[1 \quad 1 \quad 0] + \omega_2[0 \quad -1 \quad 0] = (1,0,0)$
$[\omega_1 \quad \omega_1 \quad 0] + [0 \quad -\omega_2 \quad 0] = (1,0,0)$
ω_1=1, ω_2=1

$$\sum_{i\in I}\omega_i \searrow_i$$
=1*6+1*-4
=2

which is the secret.
ie, {P, S} is an authorized set.

$\omega_1[1 \quad 1 \quad 0] + \omega_2[0 \quad -1 \quad 0] = (0,1,0)$
$[\omega_1 \quad \omega_1 \quad 0] + [0 \quad -\omega_2 \quad 0] = (0,1,0)$
ω_1=0, ω_2=-1

$$\sum_{i\in I}\omega_i \searrow_i$$
=0+-1*-4
=4

which is the secret

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Consider {1,3}

$$\sum_{i\in I}\omega_i M_i = (1,0,\ldots..,0)$$

$\omega_1[1 \quad 1 \quad 0]+ \omega_3[0 \quad -1 \quad 1] = (1,0,0)$

ω_1=1, ω_3=1

$\sum_{i\in I}\omega_i \lambda_i$
=1*6+1*1
=7
which is not the secret.
ie {P,R} is an unauthorized set.

$\omega_1[1 \quad 1 \quad 0]+ \omega_3[0 \quad -1 \quad 1] = (0,1,0)$

ω_1=0, ω_3=1

$\sum_{i\in I}\omega_i \lambda_i$
=0+1*1
=1
which is not the secret.
ie {P,R} is an unauthorized set.

In the above example, there is two secret which is 2 and 4. When we consider set P, S it is able to generate both secret that's why it is considered as authorized set. While the set P.R not able to generate both secret so it is unauthorized set. In this example we consider only two secrets but in general we can share any number of secrets. When the number of secrets increase it will also increase the overall security of the whole scheme.

As we can see multi-linear secret sharing scheme is a variation of linear secret sharing scheme in which the number of secrets varies and this will improve the security of the system.

5. DISCUSSION

A new CP-ABE scheme called multi-linear secret sharing is proposed that is based on extended LSSS called multi-linear secret-sharing scheme. Which does not require a complex conversion or simplification of Boolean formula. Our scheme uses multi-linear secret-sharing scheme which can directly apply to any complex Boolean formula and can be convert it into corresponding LSSS matrix.

Proposed scheme is more powerful than existing linear schemes and it is more secure while comparing other access policy. Also, it is easy to implement. Based on the study that we conducted on literature we identified that multi-linear secret sharing scheme can implement in any access policy. It can improve access structure representation when compare to present access policy. While comparing existing access policy used in literature this multi-linear access policy can be used in any complicated access structure where normal access policy can't use.

6. CONCLUSION

Secret sharing scheme are useful in many cryptographic applications. General constructions are based on linear algebra. Multi-linear secret sharing scheme are extension of linear secret sharing scheme. Also in terms of efficiency multi-linear schemes are more efficient than linear scheme. It can be apply to any explicit access structures. Some of the open problems are to identity more applications in which we can replace LSSS with multi linear secret sharing scheme. Another problem is to providing better separation between linear and multi linear secret sharing scheme.

REFERENCES:

[1] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," *Comput. Networks*, vol. 140, pp. 163–173, 2018.

[2] L. Zhang, Y. Cui, and Y. Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," *IEEE Syst. J.*, pp. 1–11, 2019.

[3] Liu, Z., & Cao, Z. (2010). On Efficiently Transferring the Linear Secret-Sharing Scheme Matrix in Ciphertext-Policy Attribute-Based Encryption. *IACR Cryptol. ePrint Arch.*, *2010*, 374.

[4] Liu, Z., Cao, Z., & Wong, D. S. (2010). Efficient generation of linear secret sharing scheme matrices from threshold access trees. *Cryptology ePrint Archive: Listing*.

[5] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, 2005, pp. 457-473.

[6] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98).

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *Proc. - IEEE Symp. Secur. Priv.*, pp. 321–334, 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8] S. V. Gadge, "Analysis and Security based on Attribute based Encryption for data Sharing," *Int. J. Emerg. Res. Manag. &Technolog*, vol. 3, no. 3, pp. 74–78, 2014.

[9] J. Fu and N. Wang, "A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme in Cloud Computing," *IEEE Access*, vol. 7, no. c, pp. 36218–36232, 2019.

[10] R. Guo, X. Li, D. Zheng, and Y. Zhang, "An attribute-based encryption scheme with multiple authorities on hierarchical personal health record in cloud," *J. Supercomput.*, 2018.

[11] Melissa Chase, "Multi-authority attribute-based encryption," *In Theory of cryptography conference,* pp. 515-534, 2007.

[12] Y. S. Rao, "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing," *Futur. Gener. Comput. Syst.*, vol. 67, pp. 133–151, 2017.

[13] H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Cluster Comput.*, vol. 20, no. 3, pp. 2385–2392, 2017.

[14] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.*, vol. 72, pp. 1–12, 2018.

[15] V. K. Arthur Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," *J. Netw. Comput. Appl.*, vol. 129, pp. 25–36, 2019.

[16] Wei, J., Liu, W., & Hu, X. "Secure and efficient attribute-based access control for multiauthority cloud storage". *IEEE Syst. J*, pp. 1731-1742,2018.

[17] T. M. Laing, K. M. Martin, M. B. Paterson, and D. R. Stinson, "Localised multisecret sharing," *Cryptogr. Commun.*, vol. 9, no. 5, pp. 581–597, 2017.

[18] J. Wang, C. Huang, N. N. Xiong, and J. Wang, "Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system," *Inf. Sci. (Ny).*, vol. 424, pp. 1–26, 2018.

[19] Shamir, A.: How to share a secret. Communications of the ACM 22, 612–613 (1979).

[20] Brickell, E.F.: Some ideal secret sharing schemes. Journal of Combin. Math. and Combin. Comput. 6, 105–113 (1989).

[21] Beimel, Amos, and Yuval Ishai. "On the power of nonlinear secret-sharing." *Proceedings 16th Annual IEEE Conference on Computational Complexity*. IEEE, 2001.

[22] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Faculty Comput. Sci., Technion–Israel Inst. Technol., Haifa, Israel, 1996.

[23] Lewko, A., & Waters, B. (2011, May). Decentralizing attribute-based encryption. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 568-588). Springer, Berlin, Heidelberg.

[24] Beimel, A., Ben-Efraim, A., Padró, C., & Tyomkin, I. (2014, February). Multi-linear secret-sharing schemes. In *Theory of Cryptography Conference* (pp. 394-418). Springer, Berlin, Heidelberg.