ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

A Construction for Secret Sharing Scheme with General Access Structure

Niraj Bachhav[1], Swapnil Biradar[2], Mayank Mishra[3], Priti Purbey[4], Monali P. Deshmukh[5]

Student, Dept. of IT, Rajarshi Shahu College of Engineering, Tathawade, Savitribai Phule Pune University, Pune, India

Assistant Professor, Dept. of IT, Rajarshi Shahu College of Engineering, Tathawade, Savitribai Phule Pune University, Pune, India[5]

ABSTRACT: Many efficient secret sharing schemes for general access structures have been developed in efforts to deal with the problems of multi-party computations (MPC), threshold cryptography, and access control. In this paper, we have proposed a novel secretsharing scheme with general access structures that is based on the key-lock-pair mechanism. In our scheme, the dealer can assess a real situation and design the corresponding access structures, Γ = (Γ1; Γ2; : : : ; Γm). The different qualified subset of participants in Γ = (Γ1; Γ2; : : : ; Γm) can cooperate to reconstruct the shared secret, and no unqualified participants can reconstruct the corresponding shared secret. The basic idea in secret sharing is to divide the secret key into pieces, also called as 'shares' and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key. In the outline of threshold schemes, we wanted k out of n participants to be able to determine the key. In practice, it is often needed that only certain specified subsets of the participants should be able to recover the secret. A more general situation is to specify exactly which subsets of participants should be able to determine the key and those that should not. The Access structure describes all the authorized subsets to design the access structure with required capabilities. The goal of the general access structure secret sharing scheme is to provide the flexibility to decide which specified subsets of participants will able to reconstruct the original secret and which subsets cannot. The intent of this paper is to provide an analysis of some existing General Access Structure Secret Sharing Schemes. The comparative study shows there is a need of better General Access Structure scheme to fulfil the need of applications.

KEYWORDS: Data Security, Extended capabilities, General Access Structure, Network security, Secret Sharing.

I. INTRODUCTION

Secret sharing was developed in 1979 by Shamir [1] and Blakley [2], who presented two different methods to construct a threshold scheme, the first of whichwas based on the Lagrange interpolating polynomial and the second of which was based on linear projective geometry. In a secret sharing scheme, a dealer is responsible for creating some pieces of information related to the secret data, known as shadows of the secret data, and distributing these shadows to the participants. By using a secret sharing scheme, secret data can be protected among a finite set of participants in such a way that only pre-determined, qualified subsets of participants can cooperate to reconstruct the secret data, and no unqualified subset of participants can get any information about the secret data. Let P = {p1; p2; : : : ; pn} be the set of participants. An access structure, denoted by Γ, is a collection of qualified subsets of p. The access structure of a secret sharing scheme satisfies the monotone ascending property, i.e., for any A ∈Γ, B ⊆A implies B ∈Γ. The traditional (t, n) threshold secret sharing [3 - 9] is a special case of general secret sharing. Their qualified subsets are those that have at least a certain, pre-determined number of participants. Researchers have investigated (t, n) threshold secret sharing extensively, and it has been performed for a wide range of applications, including key-management problems [10] and key-distribution problems [11, 12]. In 2010, Harn and Lin [13] extended the basic idea of a (t, n) secret sharing scheme and proposed a strong (n, t, n) verifiable secret sharing (VSS) scheme. In their scheme, each participant also can act as a dealer. In 2012, Liu, Harn, Yang, and Zhang [14] proposed an efficient strong (n, t, n) VSS that was more efficient than Harn and Lins scheme [13]. In addition, they proposed an (n, t, n) multi-secret sharing (MSS) scheme to allow

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

participants to share n − t + 1 secrets. However, (t, n) threshold mechanisms have a serious limitation in some applications, and there are still many challenges to be overcome. One of the major problems is the determination of how different approaches can be utilized to construct secret sharing schemes with special access structures, such as multi-level access structures, weighted-threshold access structures, hierarchical access structures, and generalized-threshold access structures. Also, it is worthwhile to identify families of access structures that have other useful properties for secret sharing applications. Shamir [1], in his seminal work on secret sharing, attempted to construct a weighted thresholdsecret sharing scheme in which the participants did not have the same status. Shamir discussed the case of sharing a secret among the shareholders of a company in which each shareholder held a different amount of shadows. In 2007, Iftene [15] also presented a weighted-threshold secret sharing scheme based on the Chinese Remainder Theorem (CRT). Iftenes scheme extended the threshold Mignotte scheme [3] in order to address the weighted-threshold access structure in which each participant is associated with one positive weight, and the secret can be reconstructed when the weights of the cooperating participants are equal to or greater than a fixed threshold. In 2002, Sun and Chen [16] also proposed a weighted-decomposition construction for perfect secret sharing schemes with general access structures.

The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst users by the dealer. Only authorized subsets of participants can reconstruct the original secret. More formally a Secret Sharing Scheme (SSS) is a method whereby n pieces of information called shares or shadows are assigned to a secret key K in such a way that: i) The secret key can be reconstructed from certain authorized groups of shares and ii) The secret key cannot be reconstructed from unauthorized groups of shares. Electronic voting, electronic cash are good applications for general access structure. Let's denote Γ as being a set of subsets of P, and the subsets in Γ as being the subset of participants that should be able to compute the key. Then Γ is denoted as being the access structure and the subsets in Γ are called authorized subsets. Furthermore if we let K be the set of keys and S be the share set, we use the dealer D to share a key k Є K by giving each player a share Si Є S. Sometime later a subset of players might attempt to determine K from the shares they collectively hold.A perfect secret sharing scheme using the general access structure Γ, is a method of sharing a key K among a set of n participants such that P is the set of all participants, in such a way that the following two properties are fulfilled:

I. If an authorized subset of participants B Є P pool their shares, so that they can determine the value of K.

II. If an unauthorized subset of participants C Є P pools their shares, then they can determine nothing about the value of K.

It is noticed that a (k, n)-threshold scheme generates the access structure $\{B \in P \mid |B| \geq t\}$. This structure is referred to by Stinson [5] as the threshold access structure. It is possible to generate a SSS for any access structure as long as this access structure satisfies monotone property:subset B Є Γ and B Є C Є P then C Є Γ. In other words a superset of an authorized set is again an authorized set. The rest of the paper is organized as follows. In Section II some definitions are discussed. Section III covers Literature Survey Crux: general access structure for secret sharing schemes. In section IV performance analysis of these schemes based on various parameters are discussed. Finally in section V, we summarize the comparative results.

III. METHODOLOGY USED

1. Preliminary Method

In 1984, Wu and Hwang [25] proposed a revised version of the key lock- pair (KLP) mechanism [26] that fulfills the requirement of the single-key-lock (SKL) system, in which each user keeps only one key and each resource is associated with a single lock. By an operation on the key of the ith user and the lock of the jthresource, we can obtain the access right of user i for resource j.

In this section, we briefly introduce this key-lock-pair mechanism [26], which is the major building block of our scheme. We can establish an arbitrary m × n matrix A with entries aijrepresented by positive integer numbers in Galois

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Field GF(p), where p is a prime number and $1 \leq i \leq m$, $1 \leq j \leq n$. Many vector pairs exist, i.e., {Ki;Lj}, $1 \leq i \leq m$, $1 \leq j \leq n$, with dimensions $1 \times m$ and $m \times 1$, respectively, and Ki Lj = aij(1) where denotes the operation of inner product over Galois Field GF(p). Therefore, we can assign Ki to user i and Lj to the file j as their single key and lock, respectively.We will give an example that was described in reference [25]. We can establish an arbitrary, non-singular matrix K (|K| K= 0) in Galois Field GF (7) of size 5 for five users:

$$K = \begin{bmatrix} 3 & 1 & 5 & 6 & 5 \\ 1 & 2 & 3 & 5 & 3 \\ 4 & 1 & 1 & 4 & 1 \\ 2 & 6 & 1 & 1 & 2 \\ 5 & 5 & 6 & 5 & 4 \end{bmatrix}$$

Formal foundation of secret sharing was formulated using the information theory. Two important concepts were defined based on information rate: ideal and perfect schemes.

2. The secret sharing scheme with general access structures- In this section, first,we give a definition of secret sharing with general access structures with respect to the proposed scheme. Then, we propose a novel, secret sharing scheme with general access structure.
Definition of general secret sharing. Let P = {p1; p2; : : : ; pn} be the set of participants, and let Γ = (Γ1; Γ2; : : : ; Γm) be an m-tuple of access structures on the set of P, where $m \leq 2^{|P|}$ and 1. The secret data can be shared among these n participants, and each participant holds one piece of information relating to the secret data. Each qualified subset Γi, $1 \leq i \leq m$ of P, pre-determined according to the access structures Γ = (Γ1; Γ2; : : : ; Γm), can cooperate to reconstruct the shared secret data.

3. Information Rate: The information rate was studied by Stinson [5]. It is a measure of the amount of information that the participants need to keep secret in a secret sharing scheme. The information rate for a particular shareholder is the bit-size ratio (size of the shared secret) / (size of that user's share). The information rate for a secret sharing scheme itself is the minimum such rate over all participants [6] [2]. The efficiency of a secret sharing scheme is measured by its information rate.

4. Ideal Secret Sharing: Secret sharing schemes with information rate 1 are called ideal [7]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

- **Perfect:** A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S whatsoever, in the information theoretic sense [6] [2].
- **Qualified subset:** The participants in a qualified set can collaboratively recover the secret. It is denoted by ΓQual .
- **Forbidden subset:** The participants in a forbidden set cannot recover the secret. It is denoted by ΓForb.

IV. RELATED WORK

1.1. Sonali, Kapil, Janhavi[21]:

In [21] author has implemented a simple and lossless general access (n, n) secret sharing scheme using modulo-2 operation. The scheme is ideal as created shares are of same size as original secret image. The scheme is perfect as only qualified subsets of shares can reconstruct the original secret image. The forbidden group of shareholders cannot reveal anything about the original secret image. The complexity of implemented scheme is very low as the method used to create the shares and to get general access structure is very simple. In future parallel algorithm can be used to make this scheme faster.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

1.2. X. Wu, W. Sun[20]:

In [20] author proposed a Random Grid (RG) based visual secret sharing scheme for general access structure. The existing RG based schemes are special cases of the proposed scheme. By using the proposed scheme complicated sharing strategy can be implemented which is fit for practical applications. In this scheme secret image is encoded into n RGs while qualified sets can recover the secret visually and forbidden sets cannot. The advanced merits provided by the proposed scheme are: no pixel expansion, no code book required and no image distortion.

1.3.SunHua and Wang Aimin[18]:

In [18] author proposed a new secret sharing scheme for general access structure based on Shamir's threshold scheme and elliptic curve. In this scheme each participant selects his own secret and the dealer need not deliver any secret information to each participant. The existing secret does not need to be changed when the shared secret is renewed, the access structure is modified, and participants are added or deleted. The proposed scheme is able to prevent adversaries from getting the secret and efficiently guard against the cheating among participants. It has better security and efficiency because of no secret communication required in the secret distribution phase. Multiple secrets instead of only
Subset B Є Γ and B ЄC ЄP then C Є Γ.
In other words a superset of an authorized set is again an authorized set. The rest of the paper is organized as follows. In Section II some definitions are discussed. Section III covers Literature Survey Crux: general access structure for secret sharing schemes. In section IV performance analysis of these schemes based on various parameters are discussed. Finally in section V, we summarize the comparative results.

1.4 Shamir's secret sharing scheme [1979]
Secret image sharing has drawn considerable attention inrecent years. A (k, n) threshold secret image sharing scheme,abbreviated as (k, n)-TSISS, encrypts a secret image into nshadow images (also referred to be shadows) in such a waythat any k shadows can be used to reconstruct the secretimage exactly, but any less than k shadows should provideno information about the secret image. The secret pixel canbe hidden in the constant term of a (k - 1)-degree polynomialusing Shamir's (k,n) secret sharing scheme, abbreviated asShamir's (k, n)-SSS , and the secret image can be perfectlyreconstructed from any k shadows by Lagrange'sinterpolation. In Such a case, each shadow is the same sizeas the secret image. For example, to encrypt a 10GB satelliteimage by a (5, 10)-TSISS, and get 10 shadows, each withsize 10GB; and to reconstruct the 10GB satellite image, andthen have to collect 5 shadows, which sum up to 50GB. Thelarger the amount of information grows, the severer theabove problem suffers from. To solve this large shadow sizeproblem in secret image sharing, Thien and Lin embed thesecret pixels in all coefficients of a (k-1)-degree polynomialand reduce the shadow size to 1/k of the secret image

1.5 T. Tassa, Hierarchical threshold secret sharing [2007]
Contemplate the matter of threshold secret sharing in groups with hierarchical data structure. In such settings, the key is shared among a bunch of participants that's partitioned into levels. The access structure is then determined by a sequence of threshold requirements: a set of participants is permitted if it's a minimum of k0 members from the best level, additionally as a minimum of k1 > k0 members from the 2highest levels so forth. Such issues might occur in settingswhere the participants disagree in their authority or level of confidence and also the presence of upper level participants is imperative to permit the recovery of the common secret. Although secret sharing in hierarchical teams has been studied extensively within the past, none of the prevailing solutions addresses the simple setting wherever, say, a bank.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

V. EXPERIMENTAL SET UP

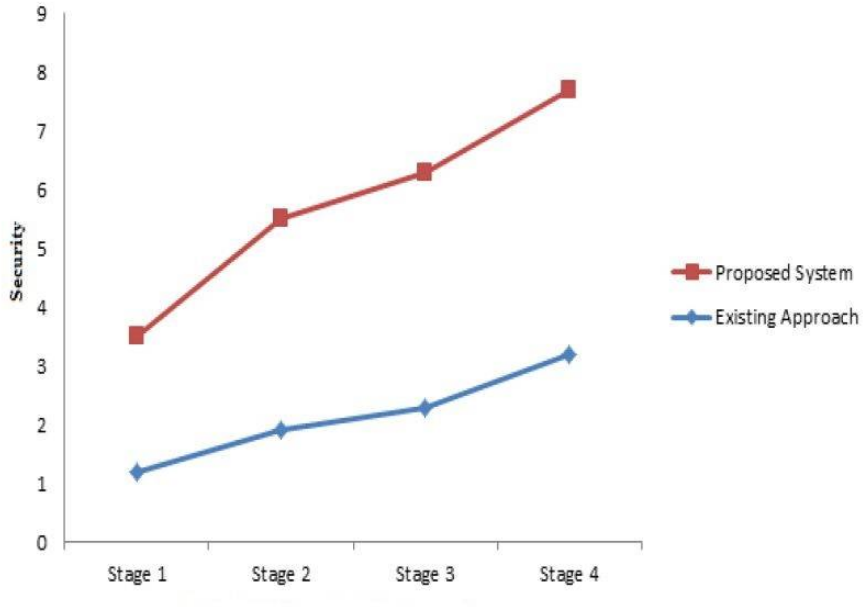

Fig No 01 Comparison of existing and proposed

Graph showing the difference between two approaches From the above graph it can be observed that our proposed approach has yielded high security when compared with native approach. The different stages are occurring in cloud computing are considered as the data from one system to other. It can also be observed that at each stage the proposed strategy obtained high security.

VI. CONCLUSION

In this paper, we proposed a novel, secret sharing scheme for general access structures based on the key-lock-pair mechanism. In a set of participants P = {p1; p2; : : : ; pn}, the dealer can design the corresponding access structures Γ =(Γ1; Γ2; : : : ; Γm) in terms of the real situation. Each qualified subset of P = {p1; p2; : : : ; pn} in these access structures Γ = (Γ1; Γ2; : : : ; Γm) can reconstruct the shared secret. The correctness and security analysis showed that the shared secret only can be reconstructed by the corresponding qualified subset of participants and that no unqualified participants can reconstruct the corresponding shared secret.In our results we mainly show that there is vast difference in security provided by existing approach.

VII. FUTURE WORK

There is a lot advancing in the field of secret sharing. Applications for secret sharing schemes seem to be getting more important. The comparative study shows that to add extra functionalities like enrolment and disenrollment of shareholders, renewing of existing shares is difficult with general access structures. In future a better general access structure secret sharing can be implemented with all the extended capabilities.

REFERENCES

[1] Shamir, A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.
[2] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[3] Mitsuru Ito, Akira Saito, Takao Nishizeki, "Secret Sharing Scheme: Realizing General Access Structure", GLOBECOM IEEE 1987.
[4] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27-35.
[5] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.
[6] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 524-528
[7] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp. 207–216.
[8] G. Blakely, "Safeguarding cryptographic keys", presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1997, pp. 313–317.
[9] K. Srinathan, N. TharaniRajan, and C. PanduRangan, "Non-perfect secret sharing over general access structures," in INDOCRYPT, 2002, pp. 409–421
[10] Pang, L.-J., Li, H.-X., Wang, Y.-M., "A secure and efficient secret sharing scheme with general access structures", Lecture Notes in Computer Science v 4223 LNAI, Fuzzy Systems and Knowledge Discovery - Third International Conference, FSKD 2006, Proceeding 2006, p. 646-649.
[11] SurjadiSlamet, Kiki AriyantiSugeng, Mirka Miller "Sum Graph Based Access Structure In a Secret Sharing Scheme" Journal of Prime Research in Mathematics Vol. 2(2006),1113-119.
[12] Chunming Tang, Zheng-an Yao, "A New (t, n)-Threshold Secret Sharing Scheme", International Conference on Advanced Computer Theory and Engineering, IEEE 2008 p. 920-924.
[13] WEI Yun, ZHONG Pucha:" A multi-stage secret sharing scheme with general access structures" 978-1-4244-2108-4/08/$25.00 © 2008 IEEE
[14] Sai-zhi Ye, Guo-xiang Yao, Quan-long Guan, "A multiple secret sharing scheme with general access structure, International Symposium on Intelligent Ubiquitous Computing and Education, 2009 IEEE
[15] Runhua Shi, Hong Zhong, "A Secret Sharing Scheme with the Changeable Threshold Value", International Symposium on Information Engineering and Electronic Commerce, IEEE 2009 p. 233-236.
[16] Chao-Wen Chan, Chin-Chen Chang, Zhi-Hui Wang, "Cheating Resistance for Secret Sharing", International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009 IEEE p. 840-846..
[17] Yung-Chen Chou, Chih-Hung Lin, Pao-Ching Li, Yu-Chiang Li, "A (2, 3) Threshold Secret Sharing Scheme Using Sudoku", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE 2010.
[18] Sun Hua and Wang Aimin ," A Multi-Secret Sharing Scheme with General Access Structures based on Elliptic Curve" 3rd International Conference on Advanced Computer Theory and Engineering 2010 IEEE