© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Survey of Various Secret Sharing Scheme

Utpal B Patel
Computer Science and Engineering, Parul Institute of Engineering and Technology, Vadodara, Gujarat, India

ABSTRACT

A Secret Sharing is a technique for increasing the security of sensitive information. Secret Sharing is that a secret will be Split into a number of pieces between a numbers of participants. All number of pieces of secret can be merge together to generate the original secret. In nowadays world use of these secret sharing concepts are widely used for protecting sensitive information. Different-Different application uses the secret sharing schemes in different ways depending on the demand of the application. This widely use of secret sharing has extended to large research on this subject. In this we have studied different-different secret sharing scheme and classified based on their characteristics.
Keywords: Cryptography, Secret Sharing Scheme, Proactive, Verifiability, Threshold.

I. INTRODUCTION

There is a growing demand for processing and data sharing in an open distributed environment with the development of internet. There is need to provide expressive access control and data confidentiality when communicating with users. In Cryptography a secret sharing scheme is a technique for splitting a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the share are combine together Individual shares not generated the secret. In a secret sharing scheme there is one central authority and n participants. The central authority gives a share of secret to the participants but only when specific condition are full filed [1].

1. All n Participants share can be combine together and reconstruct original secret.
2. Less than n parties cannot reconstruct the original secret.

A Secret Sharing is an effective way to splitting a secret information into two or more number of pieces (i.e. Share), and retrieving the information by combined all pieces. [1] The pieces of information are called shares and process responsible for the division is called central authority. Secret sharing scheme will be divided into two phase.

Distribution of secret: In distribution phase the secret can be divided into n number of pieces and distributed group of participants. Show in Figure 1, where P= number of participants, S = Secret, $S_1, S_2, S_3 \dots \dots \dots S_n$ is share of secret.

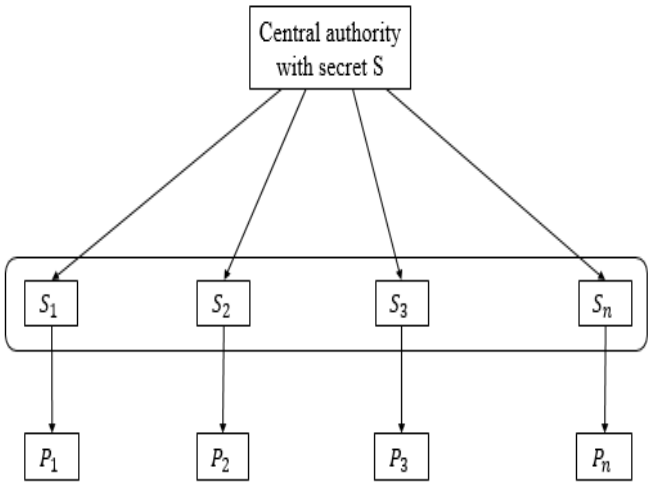

Figure 1: Distribution of secret.

Reconstruction of secret: In reconstruction phases n participants share are combined together and original secret can be reconstructed. Less than n participants cannot reconstruct the original secret. Show in Figure 2, where P= number of participants, S = Secret, $S_1, S_2, S_3 \dots \dots \dots S_n$ is share of secret.

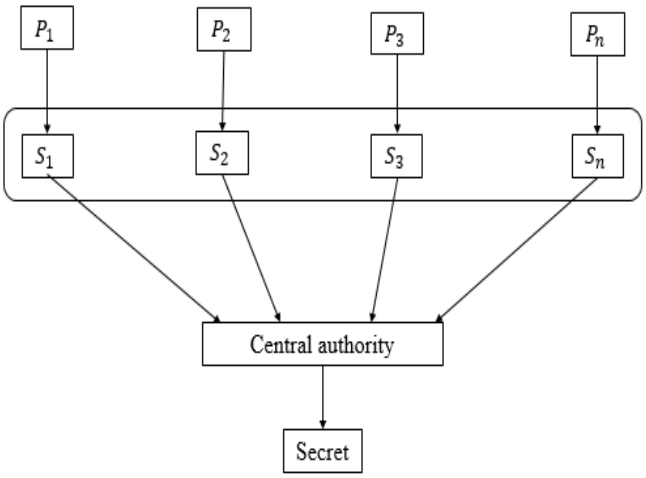

Figure 2 : Reconstruction of secret.

The secret sharing scheme have been independently introduction by Shamir [1] and Blakely [7] as a solution for securely share cryptographic key.

Example: Secret Sharing Scheme is applied to a server system such as a cloud system. Central authority secret information from an employee table is split into shares and distributed to multiple data server or cloud system. [8] A central authority collect shares from the data servers and combines them to recover the secret. Show in Figure: 3.

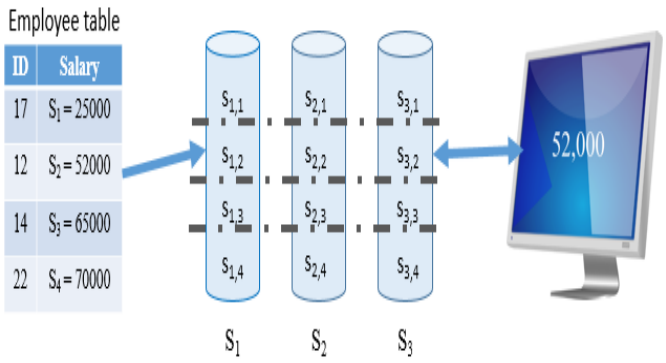

Figure 3: Example of secret sharing.

II. METHODS AND MATERIAL

Secret Sharing Scheme

Secret sharing was proposed with the motivation of preserving and securing the sensitive information in a group oriented application which involves many users forming a private network to communicate with each other. (i.e. Key distribution, Communication, Digital Bank Wallet, etc.) In secret sharing the information (Secret) can be divided in to n number of pieces is called a share. All pieces of secret can be split in group of participants. All group of participants can be combined all pieces ten determined the original secret is called a secret sharing. Secret sharing scheme can be classified in various category.

1 Classification of Secret Sharing Scheme

Secret Sharing schemes can be classified into different – different categories according to various criteria.

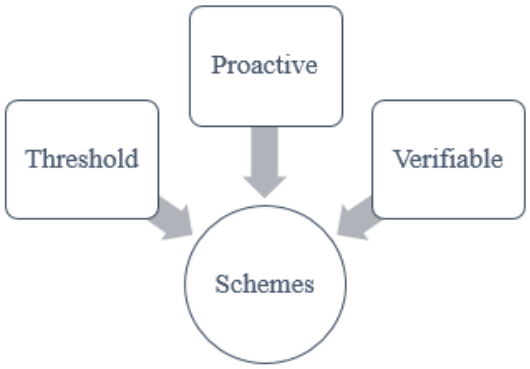

Figure 4 : Classification of secret sharing scheme

Threshold scheme: In threshold secret sharing scheme, Let S is some secret information. This secret can be split in n number of pieces. All Secret pieces can be combined together generate original secret. The less than n of the pieces leaves secret can be undermined. This problem can be consider first by Shamir's [1] and Shamir proposed a (t, n) threshold scheme. In this type of schemes there is a central authority and n number of participants. The Central authority gives a share of the secret to the participants. The participants be able to reconstruct the secret from their shares the central authority accomplishes this by given each participants a share in such a way that any group of t (threshold) or more participants can together reconstruct the secret but no group of fewer then t participants cannot reconstruct the secret Such as system is called (t, n) threshold scheme show in Figure 4.

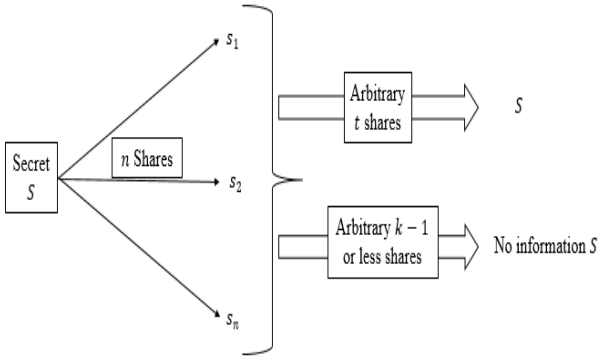

Figure 5: Threshold Scheme

Proactive scheme: Secret sharing scheme protect secret or sensitive information by splitting them over different –different participants. In (k, n) threshold scheme, Security is as sure if all over the entire continuance of the secret. The attacker is controlled to compromise less than k of the n participants, for long time sensitive information protect may be insufficient. This problem can be solve Amir Herzberg [2] in 1998 by using efficient proactive secret sharing scheme. In this types of schemes use for share protecting against such long time. There is a central authority and n number of participants. The central authority split share of the secret to the n number of participants. The participants store their shares on insecure computer server. An attacker crack the shares. In this some condition central authority can change the threshold number while share updates, then share can be renewed and the participants remove old share. An attacker cannot recover any information about the original secret is called proactive scheme.

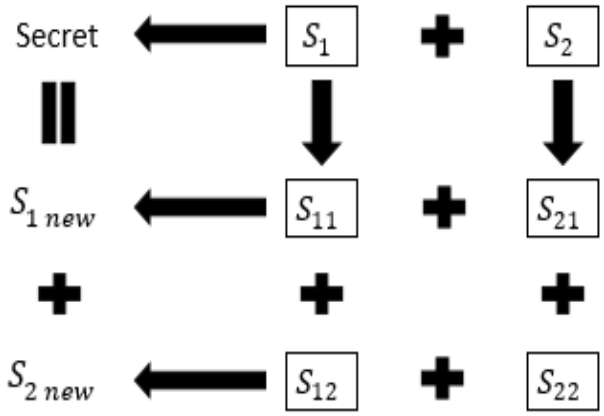

Figure 6: Proactive Scheme

The core properties of pro-active secret sharing:

- To renew existing shares without changing the secret, so that previous exposures of shares will not damage the secret (old shares will become useless).
- To recover lost or corrupted shares without compromising the secrecy of the shares.

Verifiable Scheme: In secret sharing the central authority divides the secret and splitting shares to participants without making any mistake. Any participants must unconditional trust that the received share is valid. In this types of schemes information is included that allows parties to verify their shares as consistent [5]. Specifically a Verifiable secret sharing scheme is necessary to withstand the following two types of attacks [5].

- Central authority inconsistent or incorrect shares to some of the participants during the distribution phase.
- Participants submitting incorrect shares during the reconstruction phase.

2 Classification of Secret Sharing Techniques.

Secret Sharing schemes can be classified into different – different techniques.

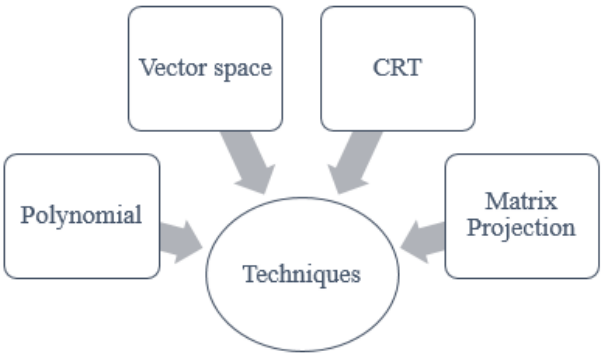

Figure 7 : Classification of secret sharing techniques

Polynomial based secret sharing: Shamir's secret sharing is based on polynomial interpolation. Shamir's created the idea about of a (t, n) threshold secret sharing techniques. It allows a central authority to split a secret S to n number of participants. Such that at least participants are required to reconstruct the original secret, In the polynomial based secret sharing scheme, the protocol is information theoretically secure, i.e., any fewer than t participants cannot gain any information about the secret. Shamir scheme is split into two phase. For more information about this scheme referred to the original paper [1].

Share Generation: The encoder uses a linear polynomial function to generate the secret shares. The central authority first select a random polynomial F(x) of degree t-1. $f(x) = a_0 + a_1x + a_2x^2 + \ldots\ldots + a_{k-1}x^{k-1}$. Where k is an integer and a_0 is the share of secret s Then, input $1,2,\ldots.,n$ into this polynomial function and generate the secret shares as $S_1 = f(1)$, $S_2 = f(2)$,……, $S_n = f(n)$. The central authority splitting each share s1 to participants P1 secretly.

Secret Reconstruction: By collecting all of the n shares can generated the original coefficients of the polynomial and reconstruct the secret S by the function of "Lagrange interpolation", as show in Equation, where p is a prime number.

$$L_j = \prod 0 \le m \le k; m \ne j \frac{x - x_m}{x_{j-x_m}} \; mod\; p, \text{ [1]}$$

Vector based secret sharing: Blakley's secret sharing scheme [7] uses hyper plane geometry to solve the secret sharing problem. To implement a (t, n) threshold scheme [1], each of the n participants is given a hyper-plane equation in a t dimensional space over a finite field such that each hyper plane passes through a certain point. The intersection point of the hyper planes is the original secret. When t participants come together, they can solve the system of equations to find the original secret. The secret is a point in a t dimensional space and n shares are affine hyper planes that pass through this point. An affine hyper plane in a t-dimensional space with coordinates in a field F can be described by a linear equation of the following form [7]:

$$a_1 x_1 + a_1 x_1 + \cdots \ldots \ldots \ldots \ldots + a_t x_t$$

Reconstruction of secret is simply finding the solution of a linear system of equations. The intersection point is obtained by finding the inter-section of any t of these hyper planes. The secret can be any of the coordinates of the intersection point or any function of the coordinates. For more information about this scheme referred to the original paper [7].

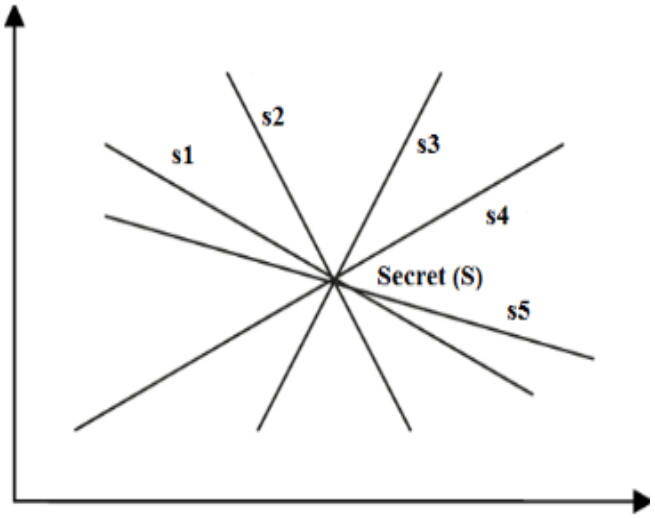

Figure 8: Vector based secret sharing [7].

CRT based secret sharing: Mignotte's threshold secret sharing scheme [9] uses special sequences of integers, referred to as the Mignotte sequences.

Given an (k, n) – Mignotte sequence [9], the scheme works as follows:

- The secret S is chosen as a random integer such that $\beta < S < \alpha$, where $\alpha = m1 \cdots mk$ and $\beta = mn - k + 2 \cdots mn$;
- The shares I_i are chosen by $I_i = S \bmod m_i$, for all $1 \le i \le n$;
- Given k distinct shares $I_{i1}, \ldots, I_{ik}$, the secret S is recovered using the standard Chinese remainder theorem, as the unique solution modulo $m_{i1} \cdots m_{ik}$ of the system

$$\begin{cases} x = I_{i1} \bmod m_{i1} \\ \vdots \\ x = I_{ik} \bmod m_{ik} \end{cases}$$

Figure: 9 CRT based technique [9].

Matrix projection based secret sharing:

Li-Bai [4] in 2006 created a secret sharing scheme using the matrix projection property. Here we describe the secret sharing scheme using matrix projection. In this scheme divided into two phase.

Construction of share Here Secret matrix S and created the share.

1) Create an $m \times k$ random matrix M of rank k where $m > 2(k-1) - 1$.
2) Select the n random $k \times 1$ vector x_i.
3) Compute share $v_i = (M \times x_i)(mod\ p)$ for $1 \le i \le n$.
4) Calculate $\mathbb{S} = proj(A)$.
5) Find a Remind matrix $R = (S - \mathbb{S})(mod\ p)$.
6) The secret matrix S, Destroy matrix M, the vector $x_i S$, the projection matrix $\mathbb{S}$.
7) Split the n share v_i, and R publicly know.

Reconstruct Secret: Reconstruct the secret S with k or more number of shares. The steps is as follows:

1) Create a matrix D using only k shares as $D = [\, v_1, v_2 \ldots\ldots\ldots\ldots v_k]$.
2) Compute the Projection matrix$\mathbb{S} = proj(D)$.
3) Verify the $tr(\mathbb{S}) = k$.
4) Calculate$S = (\mathbb{S} + R)(mod\ p)$.

III. RESULTS AND DISCUSSION

Comparison of Secret Sharing Scheme

Table 1. Comparison of various secret sharing schemes

Reference	Technique	Threshold	Proactive	Verifiable
[1]	Polynomial	Yes	Yes	No
[2]	Polynomial	Yes	Yes	No
[3]	CRT	Yes	No	No
[4]	Matrix Projection	Yes	No	No
[5]	Polynomial	Yes	No	Yes
[6]	Matrix Projection	Yes	Partial	No
[7]	Vector	Yes	No	No
[8]	Polynomial	Yes	No	No
[9]	CRT	Yes	No	No
[10]	Polynomial	yes	No	No

IV. CONCLUSION

This paper presents the basic concept of the secret sharing scheme and the various schemes as per the properties of the secret sharing scheme; Shamir's can be used polynomial based techniques for secret sharing. This paper can be useful for those who are wishing to carry out research in the direction of the cryptographic used for secret sharing. This survey can be helpful to know which and how various secret sharing schemes are being used for applying secure communication, Information hiding, and privacy preservation and information security. There are various secret sharing schemes described in this paper At last the comparison of all secret sharing schemes is done which may help to extend current research techniques.

V. REFERENCES

[1] A. Shamir, "How to Share a Secret," ACm, vol. 22, pp. 612,613, 1979.

[2] A. Herzberg, S. jarecki, H. Krawczyk and M. Yung, "Proactive Secret Sharing Or: How to Cope With Perpetual Leakage," Springer, 1998.

[3] Subha Rao Y V and Chakravarthy Bhagvati, "CRT Based Threshold Multi Secret Sharing Scheme," Internation Journal of Network Security, vol. 16, pp. 249-255, 2014

[4] Lai Bai, "A Strong Ramp Secret Sharing Scheme Using Matrix Projection," IEEE, 2006.

[5] Lein Harn and Changlu Lin, "Strong (n,t,n) verifiable secret sharing scheme," ScienceDirect, pp. 3059-3064, 2010.

[6] Li Bai and XuKai Zou, "A Proactive Secret Sharing Scheme in matrix projection method," Int.J.Security and Networks, vol. 4, pp. 201-209, 2009

[7] Ernest F.Brickell, "Some Ideal Secret Sharing Schemes," Springer, 1998.

[8] Taihei Watanabe, Keiichi Iwamura and Kitahiro Kaneda, "Secrecy Multiplication Based on a (k,n)-Threshold Secret -Sharing Scheme Using Only k server," Springer, pp. 107-112, 2015.

[9] Maurics Mignotte, "HOW TO SHARE A SECRET," Springer, pp. 371-375, 1983.

[10] Laio-Jun Pang and Yu-Min Wang, "A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing," Elsevier, pp. 840-848, 2005.