Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 2, February -2016

A Survey: Secret Sharing

Kinjal Patel[1], Ankit Chouhan[2]

[1] *Computer Science & Engineering Dept., PIET*
[2] *Computer Science & Engineering Dept., PIET*

Abstract —*In the 21st century, technology is omnipresent in our lives. Widespread a rapid increase in number of data and the growth of communication technologies have enabled collaborative computations among multi parties. Preserving privacy of data owned by parties is becoming crucial day by day. So, security is the main issue in multi party communication. Secret sharing is one of the approaches for this secure communication. Secret sharing is a technique to securely share information between multiple parties. Secret is divided into pieces, distribute among parties, and recovered by an authorized set of parties. Various secret sharing techniques have been developed to secure data. The intent of this paper is to hold a review of different secret sharing schemes.*

Keywords*-Security,Secret Sharing,Classification of Secret Sharing Schemes,Techniques for Secret Sharing*

I. INTRODUCTION

Security has been an issue from the time human beings started to live together. Important things and confidential informations have been always there to be kept safe from loss or misuse.

In a general scenario, sometimes secret will be safe in a single hand and at other times it is thought to be secure in multiple hands. For example, to protect a password, we can store it in a single, well-guarded location like a computer, a human brain, or a safe.[4] But, this scheme is unreliable since a single misfortune like a computer breakdown, sudden death, or destroy of equipment can make the information inaccessible.[4] So, another option is to divide the password in multiple pieces and store those pieces at different different location. Here the concept of secret sharing comes.

Secret Sharing Schemes (SSS) refer to a method in which one party called a dealer has a secret message and want to distribute among multiple parties. A secret message is divided into pieces and each party is allocated a piece of secret message, called as a share.[6] Secret message can be recovered only when sufficient number of authorized parties come together and combine their shares together. So, single shares are of no use on their own.

Hence, secret sharing gives mainly two benefits:

1. Gives tight control and removes single point vulnerability.
2. Individual key share holder cannot change or access the data.

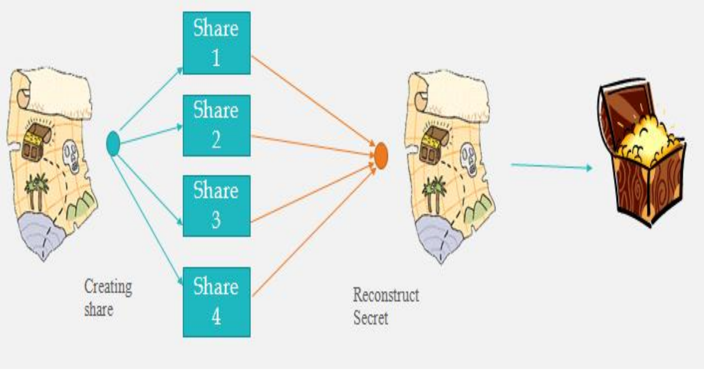

Figure1. Secret sharing

1.1 Applications of Secret Sharing[2]

- E-voting
- Secure multiparty computation
- Key management in network security
- Information hiding
- Secure online auctions
- Key management in ad-hoc networks

- Threshold cryptography

II. CLASSIFICATION OF SECRET SHARING SCHEMES

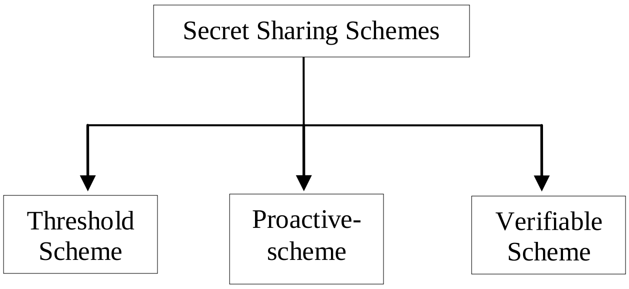

Figure 2. Classification of Secret Sharing Schemes

1. Threshold Scheme

In 1979, Adi Shamir and George Blakely independently bring before the public for the first time the concept of securely sharing the confidential informations. Both shamir and blakely schemes are threshold secret sharing schemes. The definition of threshold secret sharing scheme is given as:

"Let t and n be two positive integers, t ≤ n. A (t,n)-threshold secret sharing is a method of sharing a key K among a set of n players, in such a way that any t participant can compute the value of K, but no group of t-1 participants can do that."[1]

Here a threshold value t is chosen by a particular person is called as a dealer. When the dealer wants to share a secret key K amongst the n parties he divide the key K and distribute it between the parties and this pieces called as shares. This shares should be distributed secretly, so no other party can know about the other's share. Later, a subset of t parties combine their shares to recover the key K back.

Blakely's scheme is based on the vector space. Shamir's scheme is information theoretically secure scheme. In this scheme, the message M is splited into n pieces, $M_1, M_2, M_3, \dots, M_n$, in such a way that, for a specified value k, (2 ≤ k ≤ n)[4],

1. M is computable- if k or more pieces are known
2. M is not computable or undetermined- if k-1 or fewer pieces are known.

Such a scheme is known as (k,n)-Threshold secret sharing scheme[18]. Here the parameter k ≤ n is called a Threshold value.

So, mainly two properties of secret sharing scheme are:

- Recoverability: Given any t shares of the secret S, we can recover the secret S.[3]
- Secrecy: Given any < t shares, absolutely nothing is learned about S. [3]

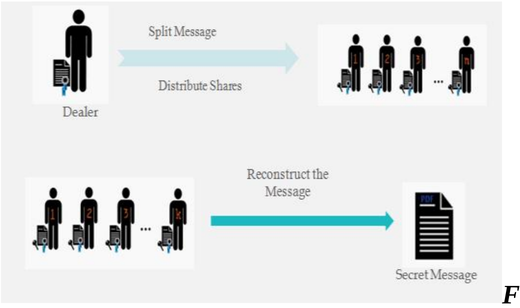

Figure 3.
Threshold Scheme

2. Proactive Scheme

Existing secret sharing scheme assumes long-lived shares, but this schemes may not provide sufficient security. In a secret sharing scheme, if any shareholder feel that his share is no more secure or there is a possibility of an attack then, the shareholder can change his share pro actively. In this scheme whenever this kind of situation is arise, the dealer of the scheme generate a new random polynomial with constant term as zero. Then the dealer again distribute the shares among the parties with x-coordinator value as same as old x-coordinator value[3]. All parties now add the old y-coordinator value and new y-coordinator value and get the new share. So now an attacker can not get any information from this shares. And if an attacker has some old shares then also he can not get any information because he need all the old shares which are now newly regenerated and if he get any new shares then they are of no meaning. Additionally, an attacker can not obtain any information about the secret from newly generated files because it contains only random information. The dealer can change the Threshold value and update it while distributing updates, but must always remain carefully observant of parties keeping expired shares.

3. Verifiable Scheme

In a secret sharing scheme, it is possible that distributed shares are fake that means a dealer is an attacker or some unauthorized party who misbehaving in the scheme and sharing the wrong information, so that parties will not be able to recover the secret. It is also possible that any shareholder might lie about his share to access the information of other shares or secret.[3]So using verifiable secret sharing scheme, a shareholder can verify that whatever information or share he got is correct or not and prevent such malicious behavior. A verifiable scheme also allows parties to verify that no other parties are lying about the contents of their shares, up to a reasonable probability of an error. Such schemes can not be computed conventionally; the parties must collectively add and multiply numbers without any individual's knowing what exactly is being added and multiplied. Another definition given by Oded Goldreich as "Verifiable secret sharing is a secure multi party protocol for computing the randomized functionality corresponding to some non-verifiable secret sharing scheme." Verifiable secret sharing scheme is very important in secure multi party computation. Secure multi party computation is typically accomplished by making secret shares of the inputs, and manipulating the shares to compute some function.

III. CLASSIFICATION OF SECRET SHARING TECHNIQUES

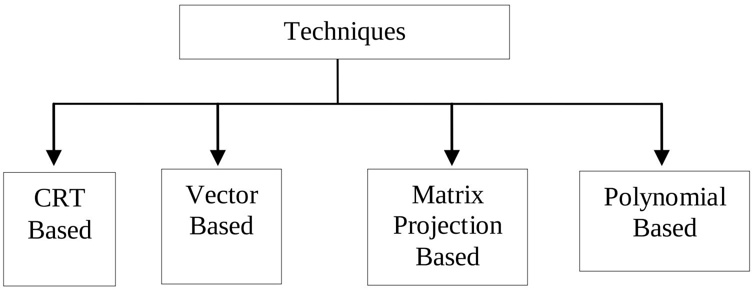

Figure 4. Techniques for secret sharing

1. Chinese Remainder Theorem Based Scheme: Mignotte's Threshold Secret Sharing Scheme

Chinese remainder theorem has many applications in computer science, e.g. RSA decryption. The Chinese remainder theorem can also be used in secret sharing. For that it provides us with a method to uniquely determine a number S modulo k many relatively prime integers $m_1, m_2, \dots\dots, m_k$, given that S < $\prod_{i=1}^{k} m_i$. Different Threshold secret sharing schemes differ from each other in method of generating the shares. Like, Shamir's threshold secret sharing scheme is based on the polynomial interpolation to recover the secret S from set of shares. Blakely's secret sharing scheme is based on the geometric methods to recover the secret S. Whereas Chinese remainder theorem based secret sharing scheme uses special sequence of integers with CRT, for example Mignotte and Asmuth-Bloom secret sharing schemes. Below the basic working of Mignotte's secret sharing scheme is given.Mignotte's secret sharing scheme uses a special sequence of integers is called a Mignotte sequences.

"Let n be an integer, n ≥ 2, and 2 ≤ k ≤ n. An (k,n)-Mignotte sequence is a sequence of positive integers, which is pairwise co-prime, $m_1 < \dots < m_n$ such that (m_i, m_j) = 1, for all 1 ≤ i < j ≤ n, and $m_{n-k+2} \dots m_n < m_1 \dots m_k$."

Given an (k,n)-Mignotte sequence a scheme works as follows:

- The secret S is chosen as a random integer such that β < S < α, where α = $m_1 \dots m_k$ and β = $m_{n-k+2} \dots m_n$.
- The shares I_i are chosen by I_i = S mod m_i , for all 1 ≤ i ≤ n.
- Given k distinct shares $I_{i_1} \dots I_{i_k}$, the secret S is recovered using the standard Chinese Remainder Theorem, as the unique solution modulo, $m_{i_1} \dots m_{i_k}$ of the system,

$$\begin{cases} x \equiv & s_{i_1} \bmod m_{i_1} \\ & \vdots \\ x \equiv & s_{i_k} \bmod m_{i_k} \end{cases}$$

Scheme works as it will determine a secret S given any k shares (in this case, the remainder of S modulo each of the numbers m_i), but will not reveal the secret for k-1 shares. Ultimately, we choose n relatively prime integers such that S is smaller than the product of any choice of k of these integers, but at the same time is greater than any choice of k-1 of them. In this manner, we can uniquely determine secret S from any set of k or more shares, but can not from any k-1 shares.

2. Vector Based Scheme: Blakely's Secret Sharing Scheme

Blakely's secret sharing scheme work on the following mechanism. Two nonparallel lines in the same plane intersect at exactly one point. Three nonparallel planes in space intersect at exactly one point. So generally, any 'n' nonparallel (n-1)-dimensional hyperplanes intersect at a specific point. In this the secret is encoded as any single coordinate of the point of intersection. Now if the secret is encoded using all the coordinates, even if they are random, then an insider (someone in ownership of one or more of the (n-1)-dimensional hyperplanes) obtain data about the secret since he knows it must lie on his plane. Thus, if an insider can obtain any more information about the secret than an outsider can, then the scheme no longer has information theoretic security. So if we want the scheme in which an insider can not gain more information than an outsider (i.e., that the secret must lie on the x-axis for a 2-dimensional system) then, choose only one of the n coordinates. Each party is given enough information to define a hyperplane; the secret is recovered by calculating the planes' point of intersection and then taking a specified coordinate of that intersection.

Compare to Shamir's scheme, Blakely's scheme is less space-efficient. Whereas in Shamir's scheme restriction is on the size of the share that is each shares are only as large as secret message, but Blakely's shares are t times longer, where t is the threshold number of parties. Blakely's scheme can be make more secure by adding restriction on which planes are usable as shares. The resulting scheme is equivalent to Shamir's scheme.

3. Matrix Projection based Secret Sharing Scheme

In this scheme, secrets are the elements represented in a square matrix S. The secret matrix S can be shared among n different participants using a matrix projection technique where: 1) any subset of k participants can collaborate together to reconstruct the secret, and 2) any subset of (k-1)or fewer participants cannot partially discover the secret matrix.[5] The advantages of this scheme are its large compression rate on the size of the shares and its strong projection of the secrets. In this scheme Ramp Secret Sharing is used. When exposed information is proportional to the size of unqualified group, these types of SSS are regarded as ramp secret sharing (RSS). RSS scheme achieve the goal of reducing the size of the shares, but at the cost of some degraded protection on the secret.[5] Li Bai has proposed this scheme in 2006, which is threshold as well as proactive secret sharing scheme. It is also provide partial verification in the scheme. He has used shamir secret sharing scheme and extended it with matrix projection method. Thus, this scheme has many desired properties due to its information concealment capability. Also, the size of the share is significantly smaller than the size of the secret.[5]

4. Polynomial Based: Shamir's Secret Sharing Scheme:

In 1979, Shamir introduced a basic simple and elegant threshold secret sharing scheme. In shamir's secret sharing scheme the domain of secrets and shares is the elements of the finite field F_q for some prime-number q>n. Let α_1 ,……., α_n € F_q be n distinct non-zero elements known to all parties[18]. To share a secret k € F_q the dealer choses t-1 random elements α_1 ,……, α_{t-1} from F_q independently with uniform distribution. This random elements together with the secret define a polynomial $P(x)= k+\sum_{i=1}^{t} a_i x^i$. The share of P_j is $s_j = P(\alpha_j)$.[4] So in this scheme a secret message is divided into the n pieces and distribute among the n parties. Now to recover the secret, some predefined threshold value is decided and only this authorized parties can combine and recover the secret, but less than this threshold can not recover the secret.

The correctness and privacy of Shamir's scheme follow from the Lagrange's Interpolation Theorem: for every field F, every t distinct values x_1 ,…….. x_t , and any t values y_1 ,…….., y_t , there exist a unique polynomial Q of degree at most t-1 over F such that $Q(x_j)= y_j$ for 1 ≤ j ≤ t.

In this scheme, any t out of n shares may be used to recover the secret. The system relies on the idea that you can fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic curve, and so on. That is, it takes t points to define a polynomial of degree t-1. The method is to create a polynomial of degree t-1 with the secret as the first coefficient and the remaining coefficients picked at random. Next find n points on the curve and give one to each of the parties. When at least t out of the n parties reveal their points, there is sufficient information to fit a (t-1)th degree polynomial to them, the first coefficient being the secret.

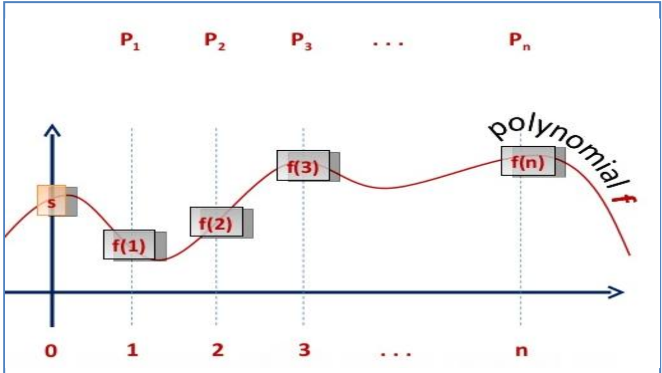

Figure 5: Polynomial based secret sharing[7]

IV. COMPARISON OF EXISTING SCHEMES

Table 1. Comparison of Existing Schemes

References	Technique Used	Proactive	Verifiable	Threshold	Disadvantages
Shamir	Polynomial based	No	No	Yes	-It is not secure against cheaters. -Not provide any extended features.
Blakely	Vector space based	No	No	Yes	-It is not perfect & Ideal SSS as Shamir's SSS. -It is less space efficient than Shamir's scheme.
Mignotte	CRT based	No	No	Yes	-It is not perfect secret sharing scheme.

IV. LIMITATIONS OF EXISTING SCHEMES

In existing secret sharing schemes, basically a secret is divided into shares and shares are distributed amongst the parties. There is no concept of verification of shares, an authentication of dealer and shareholders, periodically renew shares, multiple secret sharing. So this basic secret sharing schemes are extended with this functionalities which provide more security. But still there is not efficient scheme is there. That is, using homomorphism and polymorphic concept, we can make more secure and efficient secret sharing scheme. So the limitation of existing secret sharing scheme is not a single scheme provide all this functionality related to security and efficiency.

REFERENCES

[1] Carsten Baum, Ivan Damgard and Claudio Orlandi, "Publicly Auditable Secure Multi-party Computation", Aarhus University, Denmark, (SCN 2014).

[2] K.N.Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari, "A Review of Secret Sharing Schemes", Research Journal of Information Technology ISSN (2013).

[3] Sonali Patil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications (2012).

[4] Adi Shamir, "How to share a Secret", In ACM (1979).

[5] Li Bai, "A Strong Ramp secret Sharing Scheme Using Matrix Projection", In IEEE (2006).

[6] Amos Beimel, "Secret Sharing Schemes: A Survey", IWCC 2011, LNCS 6639, pp. 11-46,2011, Springer-Verlag Berlin Heidelberg 2011.

[7] https://www.google.co.in/search?q=shamir+polynomial+secret+sharing+scheme&rlz=1C1CHJW_enIN466IN466&espv=2&biw=1366&bih=623&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiM2ryew9jJAhUBvo4KHZtVB9IQ_AUIBygC