ABSTRACT: Concept of secret sharing is that a secret will be divided into a number of shares among a number of users. Only a specified minimum number of shares can be combined together to form the original secret. In today’s world use of such secret sharing concepts are widely used for securing data. Different applications use the secret sharing schemes in different ways depending on the needs of the application. This wide use of secret sharing has led to extensive research on this topic. Various secret sharing schemes have been developed. The intent of this paper is to explain the extended capabilities of secret sharing schemes and analyze the relation in application semantics and multifarious secret sharing schemes.

KEYWORDS: secret sharing, information security, cryptography, multi-functionality

I. INTRODUCTION

A secret sharing scheme can secure a secret over multiple servers and remain recoverable despite multiple server failures. The dealer may act as several distinct participants, distributing the shares among the participants. Each share may be stored on a different server, but the dealer can recover the secret even if several servers break down as long as they can recover at least t shares; however, crackers that break into one server would still not know the secret as long as fewer than t shares are stored on each server. First threshold schemes were independently invented by both Adi Shamir [5] and George Blakely [6] in 1979. The definition outlined in [1] to describe what a threshold secret sharing scheme is:

Definition:
Let t and n be positive integers, t ≤ n. A (t, n) - threshold scheme is a method of sharing a key K among a set of n players (denoted by P), in such a way that any t participants can compute the value of K, but no group of t-1 participants can do so. The value of t is chosen by a special participant which is referred to [1] as the dealer. When D wants to share the key K among the participants in P, gives each participant some partial information referred to earlier as a share. The shares should be distributed secretly, so no participant knows the share given to any other participant. Some of the threshold based SSS schemes are explained in the further sections.

II. RELATED WORK

A. Shamir’s secret sharing
Shamir secret sharing is based on polynomial interpolation over a finite field. Shamir developed the idea of a (t, n) threshold-based secret sharing technique (t ≤ n). The technique allows a polynomial function of order \((t-1)\) constructed as,
\[ f(x) = d_0 + d_1x_1 + d_2x_2 + \ldots + dt^{-1}t^{-1} \mod p, \]
where the value \(d_0\) is the secret and \(p\) is a prime number.
The secret shares are the pairs of values \((x_i, y_i)\), where \(y_i = f(x_i), 1 \leq i \leq n\) and \(0 < x_1 < x_2 \ldots < x_n \leq p - 1\).
The polynomial function \(f(x)\) is destroyed after each shareholder possesses a pair of values \((x_i, y_i)\) so that no single shareholder knows the secret value \(d_0\). In fact, no groups of \(t-1\) or fewer secret shares can discover the secret \(d_0\). On the other hand, when \(t\) or more secret shares are available, then we may set at least \(t\) linear equations \(y_i = f(x_i)\) for the unknown \(d_i\)’s. The unique solution to these equations shows that the secret value \(d_0\) can be easily obtained by using Lagrange interpolation.
Some of the useful properties of Shamir’s \( (k, n) \) threshold scheme are:

1. **Secure**: Information theoretic security.
2. **Minimal**: The size of each piece does not exceed the size of the original data.
3. **Extensible**: When \( k \) is kept fixed, \( \frac{n}{k} \) pieces can be dynamically added or deleted without affecting the other pieces.
4. **Dynamic**: Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5. **Flexible**: In organizations where hierarchy is important, we can supply each participant different number of pieces according to their importance inside the organization. For instance, the president can unlock the safe alone, whereas 3 secretaries are required together to unlock it.

### III. Blakley’s secret sharing scheme [5]:

Blakley’s SSS uses hyperplane geometry to solve the secret sharing problem. To implement a \((t, n)\) threshold scheme, each of the \(n\) users is given a hyperplane equation in a \(t\) dimensional space over a finite field such that each hyperplane passes through a certain point. The intersection point of the hyperplanes is the secret. When \(t\) users come together, they can solve the system of equations to find the secret. The secret is a point in a \(t\) dimensional space and \(n\) shares are affine hyperplanes that pass through this point. An affine hyperplane in a \(t\) dimensional space with coordinates in a field \(F\) can be described by a linear equation of the following form:

\[
 a_1 x_1 + a_2 x_2 + \ldots + a_t x_t = b
\]

Reconstruction of original secret is simply finding the solution of a linear system of equations. The intersection point is obtained by finding the intersection of any \(t\) of these hyperplanes. The secret can be any of the coordinates of the intersection point or any function of the coordinates.

### IV. Li Bai’s secret sharing:

Li Bai developed a threshold secret sharing based upon the invariance property of matrix projection. The scheme is divided in two phases:

**Construction of Secret Shares from Secret Matrix \( S \)**

1. Construct a random \(m \times k\) matrix \(A\) of rank \(k\) where
2. \(m > 2(k - 1) - 1\).
3. Choose \(n\) linearly independent \(k\times1\) random vectors \(x_i\).
4. Calculate share \(v_i = (Ax_i) \mod p\) for \(1 \leq i \leq n\), where \(p\) is a prime number.
5. Compute \(S = (A (A'A)^{-1} A') \mod p\).
6. Solve \(R = (S - S) \mod p\).
7. Destroy matrix \(A\), \(x_i's\), \(S\), and
8. Distribute \(n\) shares \(v_i\) to \(n\) participants and make matrix \(R\) publicly known.

**Secret Reconstruction**

1. Collect \(k\) shares from any \(k\) participants, say the shares are \(v_1, v_2, \ldots, v_k\) and construct a matrix \(B = \{v_1, v_2, \ldots, v_k\}\).
2. Calculate the projection matrix \(S = (B (B'B)^{-1} B') \mod p\).
3. Compute the secret \(S = (S + R) \mod p\).

### V. COMPARATIVE STUDY

The proposed scheme is compared with existing Threshold Secret Sharing Schemes like Shamir’s Secret Sharing, Blakley’s Secret Sharing and Li Bai’s Secret Sharing.
TABLE I. COMPARATIVE STUDY

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Shamir’s secret sharing</th>
<th>Blakley’s secret sharing</th>
<th>Li-Bai’s secret sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Ideal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security of scheme</td>
<td>More</td>
<td>Less</td>
<td>Less</td>
</tr>
<tr>
<td>Multiple secret sharing</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The above table shows the comparative study of the existing secret sharing schemes.

VI. CONCLUSION

In this paper, we have done a review of the existing threshold-based secret sharing schemes and performed a comparative study on the secret sharing schemes. Table I shows comparison of the secret sharing schemes with respect to various parameters.

REFERENCES