A Method for Secure Health Care System in Multi-Parties

A.B Rajesh Kumar,
Dept of Computer Science,
S.V. University, Tirupati, A.P. India
subhashamud@yahoo.com

Prof. M. Padmavathamma
Dept of Computer Science,
S.V. University, Tirupati, A.P. India
prof.padma@yahoo.com

Abstract: Security requirements have more impact on the information technology. In the information distribution over multiparty need to provide confidentiality and authentication. In this paper, we introduced an algorithm to preventing malicious party based on patient details. The objective of the algorithm is to maintain confidentiality and authentication on multi-parties during constructing the information based on shamir's secret sharing scheme.

Key Words: *Shamir's secret sharing scheme, key distribution, security, multi-party computation*

I. INTRODUCTION

Safeguarding cryptographic keys are essential in shamir's sharing scheme is divided into 'n' shares by a authority and shared among 'n' parties. So that 't' shares can reconstruct the secret. Shamir's is based on interpolating polynomial. In cryptography, multiparty to ensure confidentiality in distributed networks environment has emerged in various domains. Particularly health care information system is major concern for utilization to maintain patient privacy withour intervention of others from outside because patient may feel sensitive to reveal his data. In such a scenario, doctor authority needs to exchange communication between patient and doctor need authentication and confidentiality to maintain security and prevent from malicious party for reconstructing secret values. In this context, we introduced method for algorithm preventing malicious party during distribution of reconstruction of secret values i.e. keys based on shamir's secret share scheme. In this paper, we introduced an algorithm to preventing malicious party based on patient details. The objective of the algorithm is to maintain confidentiality and authentication on multi-parties during constructing the information based on shamir's secret sharing scheme. [2]

II. RELATED WORK

2.1 Shamir's Secret Sharing Scheme:

In cryptography, a secret sharing scheme is a method for distributing 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 shares are combined together individual shares are of no use on their own. Here, there is a One dealer and 'n' players. The dealer gives a secret to the players. But only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share. In such a way that any group of 't'(threshold) or more players can together reconstruct the secret but no group of less than 't' players such a system is called a (t,n) – threshold scheme.[6]

Secret sharing schemes were originally introduced by both Blakley and Shamir independently in 1979. As a solution for safeguarding cryptographic keys in a secret sharing scheme. A secret 't' is divided into 'n' shares and shared among a set of 'n' share holders by mutually trusted dealer. Shamir's (t, n) secret sharing scheme is very simple and efficient to share a secret among 'n' shareholders. When the share holders present their shares in the secret reconstruction phase. Dishonest share holders can always exclusively derive the secret by presenting faked shares and but the other honest shareholders get nothing but a faked secret. Here shamir's original scheme does not prevent any malicious behaviour if dishonest share holders doing fair reconstruction phase.

2.2 Some properties of this (t, n) threshold scheme:

The size of each piece does not exceed the size of the original data. When ‘t’ is kept fixed D_i pieces can be dynamically added or deleted withour affecting the other D_i pieces without changing the original data D. all we need is a new polynomial q(x) with the same free term. A frequent change of this type can greatly enhance security since the pieces exposed by security breaches can not be accumulated. Unless all of them are values of the same edition of the q(x) polynomial. By using tuples of polynomials values of D_i pieces [7]

Ex: P → three values of q(x)

VP → two values of q(x)

Each executive → one value of q(x)

Then (3, n) threshold scheme enables checks to be singed by either by any three executives or by any executives one of who is vice president or by the president alone.

A simple (t, n) threshold scheme

This scheme is based on polynomial interpolation given ‘k’ points in the 2-dimensional plane (x_i, y_i) ------, (x_k, y_k) with distinct x_i. There is one and only one polynomial q(x) of degree t-1 such that $q(x_i) = y_i$ for all ‘i’ without loss of generality. We can assume that data ‘D’ is a number to divide it into pieces D_i. we pick a random k-1 degree polynomial $q(x) = a_0 + a_1x + \text{----} + a_{k-1}x^{k-1}$ in which a_0 = D and evaluate: $D_1 = q(D_1$,---------$D_i = q(i)$, ------------, $D_n = q(n)$ we can find the coefficients of q(x) by interpolation, D = q(0). To make this claim more precise we use modular arithmetic instead of real arithmetic. [4, 6]

2.3 Example:

Lagrange’s Interpolation:

d={4,7,8,6} d=4-1=3

$p(d) = 2d^3 + 5d^2 – 6x+2$

$p(d) = 2d^3 + 5d^2 – 6d+2$

d=1

$p(4) = 2(4^3) + 5(4)^2 – 6(4) + 2$

=128+80-24+2

=184

d=2

$p(7) = 2(7^3) + 5(7)^2 – 6(7) + 2$

=168+245-42+2

= 891

d=3

$p(8) = 2(8^3)$

=1024+320-48+2

= 298

p(6) = 432+180-36+2

= 578

d	p(d)
4	184
7	891
8	1298
6	578

Find out and evaluate the unknown value for given range of values.

$$\frac{(x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)} f(x_0)+$$

$$\frac{(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)} f(x_1)+$$

$$\frac{(x-x_0)(x-x_1)(x-x_3)}{(x_1-x_0)(x_2-x_1)(x_2-x_3)} f(x_2)+$$

$$\frac{(x-x_0)(x-x_1)(x-x_2)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)} f(x_3)$$

$$=\frac{(5-7)(5-8)(5-6)}{(4-7)(4-8)(4-6)}\ (184)+$$

$$=\frac{(5-7)(3)(1)}{(7-4)(7-8)(7-6)}\ (89)+\frac{1.2.1}{4.1.2}(1298)+\frac{1.2.3}{2(+)(-2)}(578)$$

$$\text{P(5)=}\frac{-3}{24}(184)+\left(\frac{3}{+3}\right)(891)\frac{1}{8}(1298)\frac{6}{4}(578)$$

= -23 + 891 + 162.25 + 433.5

= 1463.75

$i \rightarrow 5$

p(i) $\rightarrow$ 1465.75 $\rightarrow$ this is a interpolated value

P={p_1, p_2, ……….p_n}

N=10 ; t=4

D $\rightarrow$ dealer

f(x) = $3x^3$+$2x^2$-5x+2

The constant value is

2=Secret Value (S)

Construction Phase

$S^1 = f_{(1)} = 3+2-5+2 = 2$

$S^2 = f_{(2)} = 24+8-10+2 = 24$

$S^3 = f_{(3)} = 81+18-15+2 = 86$

$S^4 = f_{(5)} = 375+50-25+2 = 402$

....

....

$S_{10} = f_{(10)} = 3000+200-50+2$

$= 3152$

$\text{n}-\text{shares} = (S_1, ..., S_n)$

$$\begin{array}{l} =(2,\ 24,\ 86, 402, ...3152) \\ \quad\downarrow\ \downarrow\ \ \downarrow\ \ \downarrow \qquad\qquad \downarrow \\ \quad p_1\ \ p_2\ \ p_3\ \ p_4 \qquad\quad p_{10} \end{array}$$

Reconstruction Phase

t=4

Picks randomly out of 10 shares say

$\{-2,\ 24,\ 86,\ 402\} = (S_{i_1}, S_{i_2}, S_{i_3}, S_{i_4})$

$\{i_1, i_2, i_3, i_4\} = \{1,2,3,5\}\ C\{1,2,3,4,....,10\}\ \{p_1\ p_2\ p_3\ p_4\}$

(2, 24, 86, 400)

(1, 2), (2, 24) (3, 86) (5, 400)

$$g(x) = \frac{(x-x_1)(x-x_2)(x-x_3)}{(x-x_1)(x_o-x_2)(x_o-x_3)}y_0 +$$

$$\frac{(x-x_0)(x-x_2)(x-x_3)}{(x-x_0)(x_1-x_2)(x_1-x_3)}y_1 +$$

$$\frac{(x-x_0)(x-x_1)(x-x_3)}{(x-x_0)(x_2-x_1)(x_2-x_3)}y_1 +$$

$$\frac{(x-x_0)(x-x_1)(x-x_3)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)}y_3$$

degree d=t-1

Algorithm: dishonest identification

t=4, n=10, S=2, J=5

(-2, 24, 86, 402, 206)

T={1,2,3,4} {2,3,4,5}

{1,3,4,5} {1,2,3,5} {1,2,4,5}

U=5

Pick T_i say $T_1 \in M$

Compute $S^1 = F(T_1)$

$F_{T_1}(S_{i_1}, S_{i_2}, Si_3, Si_4)$

$= F_{T_1}(2, 24, 86, 206)$

S^2=F_{T2} (24, 86, 206, 402)

$S^3 = F_{T_3}(-2, 86,\ 206, 402)$

$S^4 = F_{T_4}$

$S^5 = F_{T5}$

$\nu = 3$ subsets

(Partitioning S^i, it should be mutually disjoint)

$U_1 = \{S^2, S^3\}$

$U_2 = \{S^1\}$

$U_3 = \{S^4,\ S^5\}$

$U_1 \cap U_2 = \phi,\ U_1 \cap U_3 = \phi,\ U_3 \cap U_1 = \phi$

and $w_i = |U_i|$

$w_1 = |U_1| = 2$

$w_2 = |U_2| = 1$

$w_3 = |U_3| = 2$

w_z = max {w_i}

= 2

$\therefore S^{wz} = S^2$ majority secret

Pick T_2

Such S= $F\left(T_2\right) = F_{T_2}$ (24, 86, 206, 402)

and

Set R=J-{2,3,4,5}

= {1,2,3,4,5} – {2,3,4,5}

= {1}

$i_{r=1} \in R$

Compute $S^r = F\left(S_{i_1}, S_{i_2}, S_{i_{23}}, S_{i_{24}}\right)$

= F (-2, 86, 206, 202)

If S^r = S then {1} is honest

Else

{1} is dishonest. [7]

2.4 Secure Multiparty Computation:

Two or more parties would like to perform some computation with their secret value but none of them wants to disclose its value to others is a typical problem for Secure Multiparty Computation (SMC) and also basic technique shamir's secret sharing. [5]

III. SYSTEM MODEL

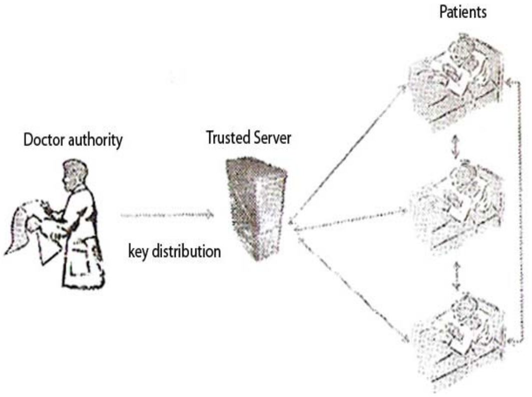

Fig.1: System Model and Patients

1. The Present which can be used as the model for secure data sharing.

2. The system a distributed environment consisting of N.

IV. METHODOLOGY

1. Doctor authority generates polynomial say $f(x) = a_0x^n+a_1x^{n-1}$+------+a_nx^{n-1} → (1)
2. Compute shares using f(x)
3. sending the shares to respective patients
4. Reconstruction Phase

   (a) Verification Phase and Reconstruction

   To avoid malicious patient for the treatment sake need to be avoided. First and foremost patients can verify shares for integrity using their own certificate of information. In which certificate contains patients summary of information about the secret sharing such as (name, address, disease etc.,)

   (b) Reconstruction Phase starts on verification of all shares during verification phase (1) extract from certificate (2) compute (3) compute and compare with share is authenticated if they are the same and assumed modified otherwise verification phase performs share authentication using certificate before the reconstruction phase.
5. Doctor authority gets the information from the patients.
6. At the receiving we prevent the malicious behaviour.
7. Doctor keeps a set of additional shares.
8. Individual patients sets the share to doctor.
9. Interpolate the results send by the each individual.
10. By combing with the additional shared points from the doctor.
11. If the interpolated value is matched, then the patient is honesty else the patient is dishonest.
12. If patient is dishonest prevent, the patient i.e. not taking the information from the patient.

V. THE PROPOSED ALGORITHM FOR MALICIOUS PARTIES

The authority generates the secret values to the patients for reconstruction. During which, the unnecessary shares can be used for prevent the shares. In this algorithm patients generated by doctor authority to reconstruct the secret at the same time prevention can be maintained during reconstruction phase.

Algorithm:

```
Input: n, t, s, j
1. Generate a random polynomial of degree t-1;
   $f(x) = a_0x^t+a_1x^{t-1}+------+a_t$
2. Compute the shares of 'n' patients using f(x)
3. Distribute the shares to patients
4. Reconstruction input ($i, i_1, i_2, ---- i_k, s_1, s_2, s_3, --------s_k$)
   (i)    Input the secret shares of patient's 'ss'
   (ii)   Interpolate 's' using the points ($i_1, s_1$) ($i_2, s_2$) ($i_{ss}, s_{ss}$) ---------- ($i_k, s_k$)
          the output of the interpolated value say '$s^r$'
   (iii)  Is $s^r = s$
   (iv)   Then put $i_r$ into H otherwise put $i_r$ into C
   (v)    Return step (ii) until $J = \phi$
```

VI. CONCLUSION

In this paper we proposed an algorithm for utilization of cryptographic technology on multi-parties through shamir's secret sharing scheme. Particularly this provides safeguard keys during reconstruction of information in multi-parties.

VII. REFERENCES

1. "Secret Sharing Homomorphisms: Keeping Shared of a Secret", John Cohen Benaloh, 1988.

2. "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority", Tal Rabin, Michael Ben-Or, Institute of Mathematics and Computer Science, The Hebrew University, Jerusalem, Israel, 1989.
3. "A Method for Obtaining Digital Signature and Public Key Cryptosystems", R.L. Rivest, A. Shamir and L. Adleman, MIT Laboratory for Computer Science and Department of Mathematics.
4. "Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes", Daniel Pasaila, Vlad Alexa, Sorin Ifetene, Department of Computer Science, A1.I.Cuza University, Iasi, Romania.
5. "Privacy preserving decision tree learning over multiple parities", F. Emekci, O.D. Sahin, D. Agarwal, A. El Abbadi.
6. "How to Share a Secret Communications of the ACM", A. Shamir, 1979, Vol. 22(11). p.no. 612-613
7. "Detection and Identification of Cheater's in (t, n) secret sharing scheme", Lein Harn, Changlu Lin.
8. "Strong (n, t, n) verifiable secret sharing scheme", Lein Harn, Changlu Lin, 2010.
9. "Survey on Privacy Preserving Data mining", Pingshui Wang.
10. "Secret Sharing Schemes with applications in security protocols", S. Iftene, University of Lasi, Faculty of Computer Science.