National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN: 2456-3307

Cheater Detection Scheme for Dynamic Secret Key Generation

Sunil Dalal[1], Sangeeta Bhan[2], Susobhan Das[3]

[13]Department of Information Technology BGSB University, Rajouri, J&K, India
[2]Computer Science and Engineering, Delhi Technological University, Delhi, India
sunildalal57@gmail.com[1], sangeetabhan7@gmail.com[2], sdas1980@gmail.com[3]

ABSTRACT

Any secret sharing scheme is considered to be strong if the complexity of cryptanalysis is very high. In cryptography the brutal attack is the type of attack in which all the possible keys of the algorithm are tried for obtaining the secret. Various types of cryptanalytic methods for a given scheme are compared with complexity of the brute force attack. If the complexity of various cryptanalytic attacks is of the same order as that of brute force attack, then the system is said to be computationally strong. In our method of dynamic multi-secret sharing the security analysis mainly depends upon the application of hash function to calculate C matrix and modular arithmetic over primitive element. In this paper, two methods are proposed which remove the need of secret share distribution by the dealer using secure channel and to find out the cheater in the group.

Keywords: Secret Key, Cheater Detection, Cryptanalysis.

I. INTRODUCTION

In any kind of network [8] whether wired or wireless, communication reliability and security are two important issues, especially when networks are used in national security and safety critical applications. The secure and reliable way to send information on network [5] is to encrypt the information with the help of encryption algorithm and a secret key. So in this case we have to mainly protect the cryptographic [1] key in order to protect the encrypted data from disclosure as encryption algorithm is publically known due to limited in number and follow a definite pattern to encrypt data, so cryptanalysist can easily know about encryption algorithm [9]. The secure scheme keeps the key safe by putting it in single location but such a scheme is unreliable in case of a single misfortune occurs. To keep multiple copies of a key is also unsecure from theft point of view. Here we need more robust secure way to protect the key and this can be done by sharing of the secret key/ Password using various schemes [7].

There are situations, where a military troop has many missiles but all do not have the same launch code. To launch missiles in war by sharing the launch codes one can use single secret sharing method n-times. Alternatively Multiple-Secrets sharing method can be used. In, 2006 Li Bai [6] developed multiple-secret sharing scheme based on matrix projection. Li Bai method of multiple-secret sharing is also threshold method of secret sharing. But if military troop have to change the launch code at regular intervals to keep it safe without changing the secret shares values or new codes have to be assigned to new missiles without changing the secret share values then in such cases dynamic multi-secret

secret plan can be utilized. Many times this scheme is also not enough for giving the reliability such as we need to keep up a secret on-line. We can store the secret on server.

Therefore Lin-Yeh developed a dynamic multi secret sharing scheme that can be used, when we have to change the secret without need to change secret shares. Therefore this scheme is more capable to stop intruders. The cheaters are those who are shareholder in scheme or the dealer itself who is distributing wrong secret shares to users. In such cases, There should be a method for detect the cheater from good shareholders and also a method so that dealer not able to know about secret shares. Lin-Yeh scheme does not provide such kind of solution. We can apply here a verification process to detect the cheater and also the problem regarding dealer. Dynamic multi- secret sharing schemes includes secret shares selection by users themselves using modular arithmetic and verification can be done by calculating W matrix and publish it publically. Now the verification and cheater detection process take place.

II. RELATED WORK

The Shamir's Scheme [2] of Secret Sharing method consist of two stages, namely (a) Shares Generation Phase, (b) Secret Reconstruction Phase Steps followed in each of these stage as presented in are as follows:

A. Shares Generation Phase

1) Select the limit plot (k, n) for conveyance of secret and in view of estimation of k, compose a polynomial p(x) of degree k-1
2) It can be randomly chosen (k-1) degree i.e. polynomial according to mathematical equation, like $q(x) = (a_0 + a_1x + ... +a_{k-1} x^{k-1}) \bmod P$ a_0 i.e. a_0 is a value to be used for secret key. Select a constant value for $a_1, a_2 \ldots a_{k-1}$.
3) Find more valuable result for modular arithmetic to be applied on GF(P) ,hence P is greater than (S, n). Here S = secret value that will be shared.
4) Select n diverse estimations of x to get the distinctive estimations of y. The sets framed by gathering (y, x), are diverse offers for members. Appropriate these offers among the members.

B. Secret Reconstruction Phase

1) Gather k or more number of members share.
2) Utilizing Lagrange's introduction strategy, reproduce the secret. Secret from the interjection strategy is ascertained from this equation.

$$q(x) = \sum_{i=1}^{k} (D_i) \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(x - x_j)}{(x_i - x_j)}$$

Here, put the value of x= 0 then formula is reduce t

$$q(0) = \sum_{i=1}^{k} (D_i) \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(- x_j)}{(x_i - x_j)}$$

$$q(0) = \sum_{i=1}^{k} (D_i) L_i$$

q(0) provide the value of secret data. So, we can see that how one can distribute and reconstruct the secret using Shamir's secret sharing scheme.

In the same year i.e. in 1979, Blakely [3] developed a method of secret sharing based on hyper-plane. Two non-parallel lines intersect at exactly one point on a plane, three non-parallel planes intercepts exactly at one point. Analogous to this theory any n non-parallel planes intersect exactly at one point. Blakely proposed method of secret sharing by using the above said property of non-parallel planes. According to his algorithm, any secret to be shared can be encoded as single coordinate or all coordinates of the intersected point. His method of secret sharing was not as secure as to Shamir's method as any person (participant) who owns any one plane information can encode other plane because the point will also lie in the other plane. Therefore, it is not theoretically secure for information sharing.

III. PROPOSED METHOD

In proposed method of Dynamic multi-secret sharing scheme employs hash function [10] and modular arithmetic concept on primitive element. In first proposed method modular arithmetic operation are applied on primitive elements. Master secret shares xj are choosing by user. Then user calculate yj using equation ($y_j = g^{xj}$ mod p, where g is a primitive element) and send this value to the dealer. The dealer can checks that no two users choose same secret shares by comparing their respective y_j values he got from users. There is no secure channel is required by the dealer to distribute secret shares and users choose their master secret shares by themselves.

The proposed scheme called as "Cheater Detection scheme for Dynamic Secret Key Generation" consists of three stages namely (A) System initialization and construction stage (B) The Pseudo Secret Share Generation Stage (C) The Group Secret Reconstruction Stage The steps followed in each stage are as follow:

A. System Initialization and Construction Stage

In the framework initialization phase the dealer D is select the accompanying parameters.

1) P: A vast prime number can have any value depend on number of client and group secrets value, p -> (group secrets, n).

2) g: The primary component upon GF (p).

3) h(.): The safe one-way hash function that acknowledges contributions of the any dimension i.e. creates a settled length input.

4) IDj : With respect to the client the value assigned to Identifiers is Uj (user) for j = 1 to n. here n is the number of clients which are having the secret share value.

B. The Pseudo Secret Share Generation Stage

Suppose there is a Dealer with name D that can share group i.e. k secrets $(S_1, S_2, \dots, S_i)$, for i= 1 to k i.e n clients.

1) Each user Uj (j=1, 2, 3⋯ n) select value of master secret share xj itself. Then it compute = g^{x_j} mod p, keeps xj secretly and send yj to the dealer by public channel so that dealer can ensure that yj' ≠ yj.

2) k number of secrets the D i.e. dealer has ($S_1,S_2,\dots S_k$). At that point he creates k is the no. of polynomial fi(x) of (i-1) degree, for i= 1 to k, comparing to the privileged insights takes after

f1(x) = S1 where f1 (0) = S1

f2(x) = S2 + d1x where f2 (0) = S2

.

.

.

fi(x) = Si + d1x + … +d(i-1) x(i-1) where fi(0) = Si

Where (S1,S2,………,Si) are the insider facts themselves whose equation. that equation is polynomial to be computed and d1 to d(i-1) i.e. chosen arbitrarily by the merchant of any constants from GF (p).

3) To evaluate for i= 1 to k and j= 1 to n

Vij (i ϵ k, j ϵ n)= fi(IDj) mod p =

$$\begin{bmatrix} f_1(ID_1) & f_1(ID_2) & \cdots & {}_{n}) \\ f_2(ID_1) & f_2(ID_2) & \cdots & {}_{n}) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(ID_1) & f_k(ID_2) & \cdots & {}_{n}) \end{bmatrix}$$

4) Each user compute C_ij(pseudo secret share) by using hash function and master secret share $\boldsymbol{x_j}$.

C_{ij}= $(h^i(x_j) \oplus x_j)$ mod p, where $h^i(x_j)$, indicates i progressive uses of h to x_j.

$$\text{i.e. } C_{1j} = (h\,(x_j) \oplus x_j) \text{ modulo } (p)$$

$$C_{2j} = (h\,(h\,(x_j)) \oplus x_j) \text{ modulo } (p)$$

.

.

$$C_{kj} = (h^k(x_j) \oplus x_j) \text{ modulo } (p)$$

And then sends C_{ij} to the dealer.

5) Dealer now compute

$$\boldsymbol{R_{ij}} = \boldsymbol{V_{ij}} - \boldsymbol{C_{ij}} \text{ modulo (p).}$$

$$W_{ij} = h\,(h^i(x_j) \oplus x_j) \text{ modulo (p).}$$

C. The Group Secret Reconstruction Stage

To reproduce mth bunch secret, called $S_m$out of (S_1,S_2 ,… ,S_k) i.e. S_m is belongs to (S_1,S_2 ,… ,S_k) at any rate m members out of n clients should helpfully play out the accompanying strides with the gathering secret merge.

1) To compute the pseudo secret share of every user U_j, for j = 1 to m, (condition is m ≤ n) as follows:

C_{mj}= (h^m (x_j) ⊕x_j) mod p and at that point it will post to the gathering secret merge over a protected channel.

The gathering secret combiner checks legitimacy of every member's pseudo secret share Cmj by the accompanying conditions:

$$W_{mj} = h\ (h^m(x_j) \oplus x_j) \bmod p.$$

If any user is cheating at the time of reconstruction of secret by giving wrong secret share then we can check by analyzing hash function on its share scheme and match it with respective value in W_ij matrix and find that secret share given is right or wrong. This cheater detection technique is not available in Lin Yeh method.

2) After accepting all C_{mj}, for j = 1 to m, effectively gathering secret combiner remakes the mth assemble secret Sm takes after: [4]

$$S_m = \sum_{j=1}^{m}(C_{lj} + R_{lj}) \prod_{r=1,r\neq j}^{m} \frac{-ID_r}{ID_j - ID_r} \text{ MOD P.}$$

As framework R_{ij} is publically known in this way the gathering secret combiner get R_{mj} relating to the particular C_{mj} and ID_j of the individual clients from R_{ij} lattice (i.e. in the event that third secret is to be recreate and first, second and third clients are takes an interest in secret remaking then R_{3j} have values R_{31}, R_{32} and R_{33} taken from R_{ij} lattice known publically).

Thusly one can disperse insider facts and remaking of privileged insights should be possible by utilizing above depict plans. The plan can be effectively executed. In the event that another secret is to be included by merchant then he does not need to convey the ace secret shares among clients.

IV. RESULTS AND ANALYSIS

In Lin Yeh's scheme the dealer has to select master secret shares x_j where j=1 to n Where n is number of users) and master secrets Si i.e. i = 1 to k. where k is number of master secrets). Dealer distribute with the respective user's j master secret shares x_j over secure channel shown in Figure 1. Second, there is no method to verify the secret shares given by user at the time of secret reconstruction. Therefore, any user can give a wrong share to group secret combiner.

In proposed scheme the user's themselves select the master secret shares x_j (Therefor j= 1 to n. where n is number of users). Dealer has to select only master secrets Si (Therefore i = 1 to k. where k is number of master secrets). Each of the users calculates a value y_j using his master secret share x_j and a primitive element g by using equation y_j = (g^{x_j}) mod p and post it to the dealer over public channel, so that he can verify that no two y_j have same values shown in Figure 2. Therefore, there is no need of secure channel in initial distribution of master secret shares; moreover it is not possible for any other person to know about master secret shares. Second, there is a method to verify the secret shares given by user at the time of secret reconstruction. A $W_{(ij)}$ matrix is calculated by applying hash function on C_{ij} matrix. Therefore, in the event that a pernicious member U_j may post a false secret share C_{ij} which can be checked by the group secret combiner by applying hash function on the received C_{ij} values and verify it with the help of respective values in $W_{(ij)}$ matrix since he have the knowledge of $W_{(ij)}$ matrix.

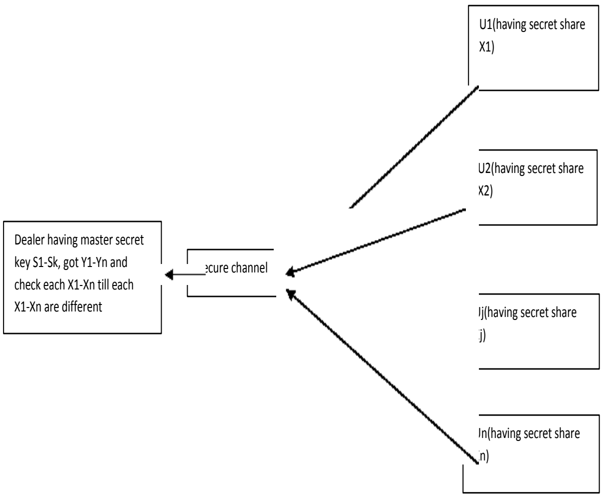
U1(having secret share X1)
U2(having secret share X2)
Jj(having secret share j)
Jn(having secret share n)
Dealer having master secret key S1-Sk, got Y1-Yn and check each X1-Xn till each X1-Xn are different
ecure channel

Figure 1.

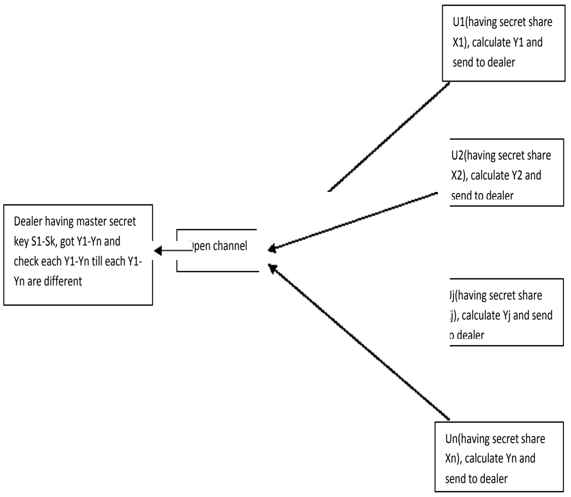
U1(having secret share X1), calculate Y1 and send to dealer
U2(having secret share X2), calculate Y2 and send to dealer
Jj(having secret share j), calculate Yj and send o dealer
Un(having secret share Xn), calculate Yn and send to dealer
Dealer having master secret key S1-Sk, got Y1-Yn and check each Y1-Yn till each Y1-Yn are different
Jpen channel

Figure 2.

The comparison of system performance among the two schemes using various parameters discussed. How our scheme takes equal time as taken by Lin-Yeh's scheme [4] but it provides more security with decrease in complexity level. Here, we introduce a method due to which even dealer cannot think of becoming a cheater. Various parameters are being discussed below in the Table 1.

Capability	Lin Yeh's scheme	Proposed Scheme
Need of security channel during secret share distribution	Yes	No
Need of security channel during sending pseudo secrets to dealer as well as group secret combiner.	Yes	Yes
Participant choose his secret share	No	Yes
Group secrets corresponding threshold value	Yes	Yes
The group secret combiner is able to check whether participant's pseudo secret share is true or not	No	Yes

V. CONCLUSION

The secret sharing is a critical technique to understand the disseminated data security utilizing information encryption. It is additionally a basic apparatus in multi-party setting. It has been connected in numerous applications, for example, secret mission information, and computerized money, amass marks et cetera. Over twenty years has gone since the main secret sharing convention has been designed. Various secret sharing plans were proposed from that point forward, which viably quickened the improvement of the hypothesis of data security and the broadly utilization of results of data security. Here we propose a dynamic secret sharing arrangement, in light of XOR operation, the unmanageability of discrete logarithm and hash capacities. The proposed plot has justifies then Lin-Yeh's plan. In proposed conspire each member picks the secret share by her/him. Is completely incomprehensible for merchant to wind up plainly a con artist and it needn't bother with a protected channel during initial distribution phase. The scheme has simple verifiable phase. So this scheme can be used in same practical cases such as secret sharing in electronics commerce, electronic govt. etc. The presented work can be extended to Insertion of authentication scheme and some more complicated cryptographic technique as elliptic cryptographic curve techniques can be used at time of secret distribution process. The elliptic curve cryptography is a way to deal with open key cryptography in view of the arithmetical structure of elliptic curve over limited fields and has strong algebraic properties.

VI.REFERENCES

[1] Atul Kahate, Cryptography and network security, second edition, India: Tata McGraw-Hill.

[2] Shamir Adi, "How to share a secret", Communication of ACM, vol. 22(11), pp. 612- 613, November 1979.

[3] Blakely G., "Safeguarding cryptographic keying", In Proc. Of AFIPS, National computer conference, 1979.

[4] Lin Han-Yu and Yeh Yi-Shiung, "Dynamic Multi-Secret Sharing Scheme", Int. J. Contemp. Math. Sciences, Vol. 3, no.1, pp. 37-42, 2008.

[5] William Stallings, Cryptography and Network Security, third edition, India: Pearson Education.

[6] Bogdnav Dan, "How to securely perform computation on secret share data" ,Master's thesis, University of Tartu, 2007.

[7] Menezes, P. Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press.

[8] Hallberg, Networking a beginning guide, TMH.

[9] Diffie W., Hellman M., "New directions in cryptography", IEEE Transactions, on Information Theory, IT-22 (6), pp. 644-654, 1976.

[10] He J., Dawson E., "Multistage secret sharing based on one-way function", Electronics Letters, vol. 30 (19), pp. 1591-1592, 1994.