www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13606-13609

Group Authentication Using Threshold Secret Sharing

[1]Parvathy Sudheer., [2]Zainul Abid T. P.

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
parvathysudheer125@gmail.com

[2] Assistant Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
zain.mes6@gmail.com

Abstract: ***Secret sharing has drawn much attention in the research community, Secret sharing refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together, individual shares are of no use on their own. Message divides into n pieces and called shares or shadows, any t(threshold value) of them can be used to reconstruct the message. A threshold value is set based on the required number of context conditions for permitting data access, if a threshold number of context parameters are satisfied then the decryption key is generated from the corresponding key shares and the data is decrypted. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important.***

Keywords: Matrix Projection, Integer polymatroid, Plane geometry, Polymatroid, Publicly Verifiable Secret Sharing, Secret Sharing, Suduko, Threshold Secret Sharing.

1. Introduction

Secret sharing (also called secret splitting) refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together[1] , individual shares are of no use on their own. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Traditional methods for encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability. This is because when storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy, or keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors, there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem, and allow arbitrarily high levels of confidentiality and reliability to be achieved. Secret sharing (also called secret splitting) refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a suffcient number, of possibly different types,
of shares are combined together, individual shares are of no use on their own. Message divides into n pieces, called shares or shadows any t(threshold value) of them can beused to reconstruct the message. A threshold value is set based on the required number of context conditions for permitting data access, if a threshold number of context parameters
are satisfied then the decryption key is generated from the corresponding key shares and the data is decrypted.
Threshold cryptography deals with access control of highly secure stored data, transmitting data and the secure access control for different levels based on their location ,time, status, identity information etc. The data is stored in the server in an encrypted form using the RSA cryptographic algorithm. Data is encrypted in the application level rather than the storage level to prevent any transmission attacks. The RSA public key is used for encryption and private key for decryption. The decryption key is splitted to different shares based on shamir secret sharing scheme and these shares are stored in the server ,here each share corresponds to different context condition. A threshold value is set based on the required number of context conditions for permitting data access. If a threshold number
of context parameters are satisfied then the decryption key is generated from the corresponding key shares and the data is decrypted. Confidentiality and authentication are
two basic requirements in secure group communication. Specially, confidentiality ensures the transmitted message is only recognizable for an intended receiver, and authentication guarantees that the communication entity is an authorized member. To provide these two basic functions, key establishment protocols are deployed to share a common one-time session key among group members, which are often classified into key agreement protocols and key transfer protocols. The former involves all member's participation to generate a session key without a trusted third party, but the process of authentication may take a long time, especially when the number of members is large. The latter relies on a trusted key generation center to firstly select session keys, and then securely distribute these session keys to all communication members. Secret sharing schemes have been independently introduced by shamir.
In shamirs secret sharing scheme, a secret is divided into n pieces 1 , . . . , s n,which satisfies
_ Knowledge of any t or more s pieces makes s easily computable.
_ Knowledge of any t-1 or fewer s pieces leaves s completely undetermined.

The Access control using threshold secret sharing for ubiquitous computing environments, introduces a context-aware access control mechanism that utilizes threshold secret sharing and multilayer encryption to provide a dynamic and truly distributed method for access

2. Related works

Blakley (1997) discussed the major challenges and key issues in Threshold Secret Sharing using Hyper plane geometry. Two non parallel lines in the same plane intersect at exactly one point. Three non parallel planes in space intersect at exactly one point. More generally, any n non parallel (n-1) dimensional hyper planes intersect at a specific point. The secret may be encoded as any single coordinate of the point of intersection. If the secret is encoded using all the coordinates, even if they are random, then an insider (someone in possession of one or more of the (n-1) dimensional hyper planes) gains information about the secret since he knows it must lie on his plane. If an insider can gain any more knowledge about the secret than an outsider can, then the system no longer has information theoretic security. If only one of the n coordinates is used, then the insider knows no more than an outsider (i.e, that the secret must lie on the x-axis for a 2-dimensional system). Each player is given enough information to define a hyper plane, the secret is recovered by calculating the planes' point of intersection and then taking a specified coordinate of that intersection randomly Computation time and complexity is low for this method. It is not Perfect and Ideal Secret Sharing method. No general access structure. No need for periodical renew of shares. No Enroll / Disenroll shareholders. No discovery of lost shares. No cheater identification. No verifiability of shares present.

Tang and Yao (2008) proposed a threshold scheme based on multi prover zero-knowledge arguments and secure multi-party computation protocol to avoid the malpractices by dishonest participants. It checks for minimum required honest participants before sharing the secret.They construct a (t, n) threshold secret sharing scheme in which the secret key K will be shared forever if at most t-1 participants are dishonest and discrete logarithm problem is hard. It is based on Multi party computation, Create method for parties to jointly compute a function over their input and keep the input private. Given number of participants P1, P2....Pn each have private data d1, d2.....dn participants want to compute value of public function F on N variables at the point d1, d2.....dn. It is more secure nothing can be learned from the public function. Computation time and complexity is low. It is Perfect and Ideal Secret Sharing method. Verifiability of shares present. No Periodical renew of shares. No Enroll / Disenroll of shareholders. No discovery of lost shares. No cheater identification and general access structure present.

Chou, Lin and Li (2010) used sudoku as key to hide data or secret information onto an image. RGB color image used as cover media. Secret information can be any form of digital media, such as text, image, audio, video etc. Sudoku solution matrix converted into Base-9 form by subtracted 1 from all values. 9x9 Sudoku solution matrix (M) is used as key for both data embedding and extraction. Here M is called reference matrix. Before embedding, one or more media files are compressed and encrypted to increase the efficiency and security of the method. Sudoku Matrix act as key for embedding and extraction. Computation time and complexity is too low. It is Perfect and Ideal Secret Sharing method. General access structure present. Enroll / Disroll shareholders. No Periodical renew of shares. No discovery of lost shares. No cheater identification. Verifiability of shares not present.

Markum Stadler (1997) used publicly verifiable secret sharing method. It resist malicious attackers, not only the participants but also others can verify the shares. Publicly Verifiable secret sharing have 2 phases of initialization. Here of pooling shares means using the string proof to exclude the participants which are failed to decrypt. Reconstruction can be done from the shares of any qualified set of participants. Executing Initialization Verifying Shares Executing Initialization Dealer creates s1, s2.....sn for each participants P1, P2, ...Pn, dealer publishes the encrypted Ei (Si) for each Di dealer also publishes a string proof to show that each Ei encrypts S Verifiable Shares Anybody knowing public key of encryption can verify shares, if one or more verification fails the dealer fails and protocol discarded. Reconstruction Decryption of shares and then it release string proof. Computation time and complexity is high. It is Perfect and Ideal Secret Sharing method. Cheater identification is possible. Verifiability of shares present. No Enroll / Disenroll shareholders. No discovery of lost shares and general access structure present. No Periodical renew of shares.

Li Bai (2009) developed a threshold secret sharing based upon the invariance property of matrix projection. The scheme is divided in two phases:

- Construction of Secret shares
- Secret reconstruction

Li Bai Scheme suggested invariance property of matrix projection. Matrix projection method makes the handling of data in more secure way. Here we can enroll / disenroll Shareholders and recovery of lost shares which is an advantage as compared to previous methods. Computation time and complexity is high. It is Perfect and Ideal Secret Sharing method. Entroll / Disroll shareholder. Recovery of lost shares present. No general access structure present. No need for periodical renew of shares. No cheater identification present and verifiability of shares present.

3. Proposed work

A new type of authentication[2] called group authentication, which authenticates all users belonging to the same group at once. The group authentication is specially designed for group-oriented applications. The group authentication is no longer a one-to-one type of authentication as most conventional user authentication schemes which have one prover and one verifier but, it is a many-to-many type of authentication which has multiple provers and multiple verifiers. A basic t-secure m-user n-group authentication scheme (t;m; n) GAS), where t is the threshold of the proposed scheme, m is the number of user participated in the group authentication, and n is the number of members of the group, which is based on Shamirs (t; n) secret sharing (SS)scheme. The basic scheme can only work properly in synchronous communications. We also propose asynchronous (t; m; n) GASs, one is a GAS with one-time authentication and the other is a GAS with multiple authentications. The (t; m; n) GAS is very efficient since it is sufficient to authenticate all users at once if all users are group members; however, if there are non members, it can be used as a preprocess before applying conventional user authentication to identify non members.

3.1 Shamir's Scheme

Shamirs secret sharing scheme based on a linear polynomial[8]. The scheme consists oftwo algorithms,
Shamir Secret Sharing have two algorithm.

- Share generation
- Secret reconstruction

- Share generation

-Dealer D picks a random polynomial f(x) of degree t-1
- f(x) = a0 + a1x + ……..a_t-1x^t-1 mod p
- Secret s = f(0) = a0for all coefficient ai , i = 0; 1; 2; 3;……..t - 1 , p > s
- D computes n shares yi = f(xi) i = 1; 2; 3……..n
-xi public information associated with share holder Ui
- Dealer distributes each share yi to share holder Ui

- Secret Reconstruction

- Assume t shares holders (U1; U2; U3…….Ui) want to recover secret t
- Share holders release the shares
-Use Lagrange inter interpolating formula for calculation of shares
- Secret is reconstructed

3.2 Synchronous Group Authentication Scheme

Here threshold t is an important security parameter[9] that affects the security of the group authentication. Using a (t, n) SS scheme to issue tokens in the registration can prevent up to t - 1 colluded inside attackers to derive the secret polynomial f(x) selected by the GM and to forge valid tokens, since (t, n) SS scheme has been used to issue tokens,
the GM only needs to issue new token to any new member who just joins the group. On the other hand, when any member leaves the group, it assumes that one token has been compromised.The GM needs to make this information available to all remaining members.The GM keeps on counting the number of leaving members. When this number reaches the threshold t GM needs to issue new tokens to all remaining group members.This scheme cannot prevent outside adversaries to impersonate to be group members when there are more than t users and all tokens are released asynchronously.

- Share generation

-There are n group members Ui where element of U ,i = 1, 2,3…..n registered at GM to form a group.
- During registration, GM selects a random (t - 1)th degree polynomial f(x) with f(0) =s
-Computes secret tokens of members as yi = f(xi), i = 1, 2, …..n where Xi is the public information associated with member Ui.
-GM sends each token yi to member Ui secretly.
- GM makes H(s) publicly known.

- Secret Reconstruction

- Assume that m users,P1, P2, P3……Pm participated in group authentication.
-Each user Pi releases the token f(xi) to all users.
-After knowing all tokens f(xi); i = 1 ,2, 3…m
- Put in Lagrange interpolating formula
- H(s1) = H(s),all users have authenticated successfully otherwise non members.

3.3 Asynchronous Group Authentication Scheme

Here in this scheme (t; m; n) GAS[10] which allows m (i.e .$t \leq m \leq n$) users to release their values asyncnchronously

- Share generation
  - GAS which allows m users to release their values asynchronously
  - GM needs to select k (kt > n - 1) fl(x); l = 1, 2….k having degree t - 1each,and generates tokens for each group member Ui
  - For any secret s GM can always and integers wj , dj , j = 1,2…….k,in GF(p),such that s = $\sum$ djfj(wj) where wi ≠ wj
  -GM makes integers wj , dj , j = 1,2…..k and H(s) publicly known.
- Secret Reconstruction
  - Each user Pi uses the token fl(xi),l = 1, 2……k
  -Compute and release Lagrange component
  -If H(si) = H(s) all users will be authenticated otherwise they are non members.

4. Results and Analysis

In group authentication scheme there is chance that a member can leave the group in that case that token is no longer used, there is a chance that group manager may reissuethe same token to the new user.This is a threat the whole secret sharing technique.Herein group authentication use polymatroid methods in order generate the token but if use
integer polymatroids then reissue of token can be avoided. In Polymatroid method decimals may be rounded such that same token may be repeated and that affects its efficiency but in integer polymatroid method we choose whole number such that above disadvantage can be avoided. In polymatroid method we can schoose a few values ie space is limited
as compared to that of integer polymatriod method which uses infinite space.An effcient method is introduced which is the modifed version of threshold secret sharing using polymatroid. The modification is done such that token generation in the Shamirs algorithm using polymatroid is replaced by integer polymatroid method. The following section outlines the detailed modification steps, using integer polymatroid method.

- Token generation using polymatroid method

The system experiences repeated generation of same token in some cases,suppose aperson leaves the group the token left by him will be used if we use polymatroid method, it is a threat to the security of whole system. Secret sharing scheme is a method todistribute a secret value into shares in such a way that only some qualified subsets of participants are able to recover the secret from their shares.A polymatroid is a pair S = (Q; f) formed by a finite set Q, the ground set, and a
rank function f : P (Q) →R satisfying the following properties:
_ f(Θ) =0

_f is monotone increasing: if $A \subseteq B \subseteq Q$; then $f(A) \leq f(B)$
_f is submodular: $f(A \cup B)+f(A \cap B) \leq f(A)+f(B)$for every $A,B \subseteq Q$
If (E; f) is a polymatroid Q, if f is normalized, submodular and increased then E isthe ground set of Q while f is the rank

function for a positive integer k, a polymatroid (E; f) is a k polymatroid if f(z) ≤ k for z in E. In polymatroid given a monotonic function
f :2^v→{0, 1, 2, 3……r} , and integral threshold t {1, 2,3….r} which can be denoted by Bt= Bt (f) family of all minimal subset X ⊆ Y for which f (X) ≥t. A set X ϵ E;is said to be submodular cover of(E; f) if f (X)=f (E) suppose both f and c are polymatroid function on 2^E , the minimisation problem min c(X) :f (X)=f (E) , X ϵ E, known as Minimum
modular cover.

- Token generation using integer polymatroid method

An integer polymatroid P with groundset Eis a bounded set of non-negative integer valued vectors coordinatized by Esuch that P includes the origin,and any non-negativeinteger vector is a member of P if it is less than or equal to some member of F,and for any non-negative integer vector y, every maximal vector x in P which is less than or equal to
y has the same sum $|x| \equiv x(E) \equiv \sum(xj : j \epsilon E)$; called the rankr (y) of vector y in P.A polymatroid is called integer if the rank function is integer valued.Integer polymatroid is used in multipartite secret sharing which is a necessary and suffcient condition for multipartite access structure. Since the integer polymatroid can be represented by family of vector subspace there will be no chance of reuse of tokens. Integer polymatriod is representable over large enough space field, so they provides a family of access structure that admit vector space secret sharing over very large enough field. By using integer polymatroid we can construct a secret sharing scheme with optimal information for every rational uniform access function. Ideal hierarchical access structure possible due to integer polymatroid method.

Integer polymatroid Z can be represented over a large enough field.

Proof:
For that we have to prove it holds toZ1.For every large enough finite field k there exist a subspace (Vi) i ϵ [1,m] for k vector space V forms a representation of of the s-truncation of the modular polymatroid with ground set [1,m] defined by the vector. Then the subspaces(Wi,j) (i, j) ϵ J of V with (Wi,j) = Vi for every j ϵ[1, n]form a representation of Z1.

5. Conclusion

Here in group authentication, which is specially designed for group-oriented applications. The group authentication applying shamirs 's algorithm using polymatroid method for token generation regenerates token after a particular interval of time. Also there is chance for the same token to be repeated if a person leave the group due to the limited
vector space of polymatroid method.The polymatroid method for token generation in shamir's algorithm is replaced by integer polymatroid metheod. In integer polymatroid method since the vector space is maximum there is no chance of regeneration of token after a long period, also there is no chance of repeatation of the token even though a member leaves the group. In integer polmatroid method we choose integers so that there is no optimization of numbers present, but in polymatroid method no such restriction such that there is a chance of rounding of numbers which increases the chance of repeatation of same token.

References

[1] P. Paillier.(1997). "On ideal non-perfect secret sharing schemes," *Security Protocols Workshop*, pp. 207–216.

[2] G. Blakely.(1997). "Safeguarding cryptographic keys", presented at the Proceedings of *the AFIPS 1979 National Computer Conference, vol. 48, Arlington*, VA, pp. 313–317.

[3] Chunming Tang, Zheng-an Yao.(2008). "A New (t, n)-Threshold Secret Sharing Scheme*", International Conference on Advanced Computer Theory and Engineering, IEEE.* 920-924

[4] Yung-Chen Chou, Chih-Hung Lin, Pao-Ching Li, Yu-Chiang L.i (2010) . "A (2, 3) Threshold Secret Sharing Scheme Using Sudoku", *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE* .

[5] M. Stadler. (1997). "Publicly Verifiable Secret Sharing", *Lecture notes in Computer Science*, 1997, 190-199 (Advances in Cryptology – EUROCRYPT"96).

[6] Bai, L. and Zou, X. (2009), "A Proactive Secret Sharing Scheme in matrix projection method", *Int. J. Security and Networks*, Vol. 4, No. 4, pp.201–209.

[7] Lein Harn. (2013)."Group Authentication" *IEEE Transaction on computers*, vol. 62, No. 9.

[8] Oriol Farr`as1, Carles Padr´o, Chaoping Xing, and An Yang" Natural Generalizations of Threshold Secret Sharing"*IEEE vol 9,214*