I J C T A, 10(9), 2017, pp. 949-955 ISSN: 0974-5572

Delegation of Authority in Organisations with Hierarchical Secret Sharing

Sonali Patil* and Kapil Tajane*

ABSTRACT

In this digital era, giving the key access for important decisions to a single person is a big problem, due to reduced trust. People are preferring to have group of people to finalize any big decision or accessing secure documents or sharing the passwords. Also, sometimes only the specific group of people are required for accessing the secret information. For such applications, general access structures are very much needed. Also, in the major organizations deciding the group of people for delegation of authority, for a specific purpose is a challenge. This paper proposes a new methodology using secret sharing, which is very useful in such organizations to decide the access structure of people for delegation of a task. The proposed scheme can be very effectively utilized without affecting the required level of authority. It provides the flexibility as easily new members can be added. Also the scalability is easily obtained at any level. This will help in expediting the important tasks with high security and trust.

Keywords: General Access Structure, Information Security, Authority Delegation, Secret Sharing

1. INTRODUCTION

1.1. Secret Sharing

A technique to transfer secret information among group of shareholders, where each shareholder is given with a unique share of the secret is called a secret sharing. The original secret data can be generated back only when enough shares, as per threshold, are combined [1].

1.2. General Access Structure:

Secret sharing distributes the secret among the group of members in terms of shares. General Access structure secret sharing allows only the specified group of members to reconstruct the original secret back by using their shares. To provide more flexibility to the threshold secret sharing schemes, access structure based approaches are very important. In such approaches, which group of people will reconstruct the secret and which group can not, is designed properly based on general access structure. As per requirement allowed group of participants gets the access for the secret and not intended group of participants are banned with such techniques [2].

1.3. Need of General Access Structure

In many applications, different set of people are needed to give the access to secret missions or secret information. Sometimes it is very much necessary to specify exactly which subsets of participants should be able to determine the secret and also which subset of participants should not determine the secret [3]. For such implications general access structure plays a vital role.

General access structure can be implemented in multiple ways. In one of the approach, multiple shares are allotted to each participant. In such schemes, the problem is large space complexity associated with

* Pimpri Chinchwad College of Engineering, Pune, *Emails: sonalimpatil@gmail.com, kapiltajane@gmail.com*

each participant. Another approach is called hierarchical or level wise approach to implement access structure. This approach allots one share to each shareholder. The space complexity is much reduced in such schemes.

1.4. Hierarchical Secret Sharing

The hierarchical secret sharing based on tree structure. In hierarchical secret sharing schemes the participants of the scheme are arranged in hierarchical levels or multi-levels. The number of participants increases up to the bottom level of the hierarchical structure.

The motivation behind proposed scheme is to provide a flexible authority delegation system in the organisations. Along with the delegation of authority the hierarchy system of an organisation should also get maintained. The most powerful member of an organisation will be top (at root level) in tree structure. The lower level participants will act on behalf of the absentee or unavailable higher level participants [3].

2. LITERATURE SURVEY

Lets consider Ã as a set of subsets of P, and the subsets in Γ as being the subset of participants that should be able to compute the key. Then Ã is denoted as being the access structure and the subsets in Γ are called authorised subsets Different researchers had developed schemes for general access structure. Ito, Saito [6] developed the new scheme to convert the (t, n) threshold scheme to a general access structure scheme. The problem identified with this scheme is number of shares applied in the scheme. Which sometimes quite large although it is bounded. K. Srinathan [7] devised the mechanism for hierarchical access structure and studied tolerability properties associated with it. It is a non perfect secret sharing scheme.

Benaloh [8] has focused to make general access structure in more simpler. He tried to prove that threshold scheme is only a particular case of general access structure. General access structure can be get by using monotone access structure. For any given polynomial P, the number of n-variable monotone formulae of size no more than P(n) is exponential in P(n). However the total number of monotone functions on n variables is doubly exponential in n. Therefore, most monotone access structure cannot be realised with a large number of polynomial sized shares. [5] have implemented a lossless and simple general access (n, n) secret sharing scheme using modulo-2 operation. The scheme is ideal because share images and original image are having same size. Pang [9] proposed more efficient sharing scheme for general access structure.

Multiple secrets can be shared among participants and get retrieved from different access structures. Sai-zhi [10] proposed a low computational complexity general access structure scheme for multiple secret sharing. It is based on Shamirs secret sharing scheme and the discrete logarithm problem. Access structure can be changed dynamically without updating any participants already allocated share.

2.1. Hierachical Acess structure.

Atanu Basu, Indranil Sengupta [13] has proposed scheme, in which position or rank of participant is considered to arrange them in a hierarchical structure as shown in Fig: 2.1. According to their position or rank and each first level participant as a parent node delegates his power to the lower level hierarchical group members. The group members help to reconstruct the secret shares of their parent nodes in their absence and the secret key is reconstructed even if at least one parent node is present. The secret shares are transmitted between the participants and the trusted dealer through our Elliptic Curve Cryptography (ECC) based signcryption scheme. The formal security analysis shows that our proposed scheme is protected from the adversaries.

[14] have proposed hierarchical secret sharing concept along with encryption techniques. These encryption techniques are adding more computational complexities.

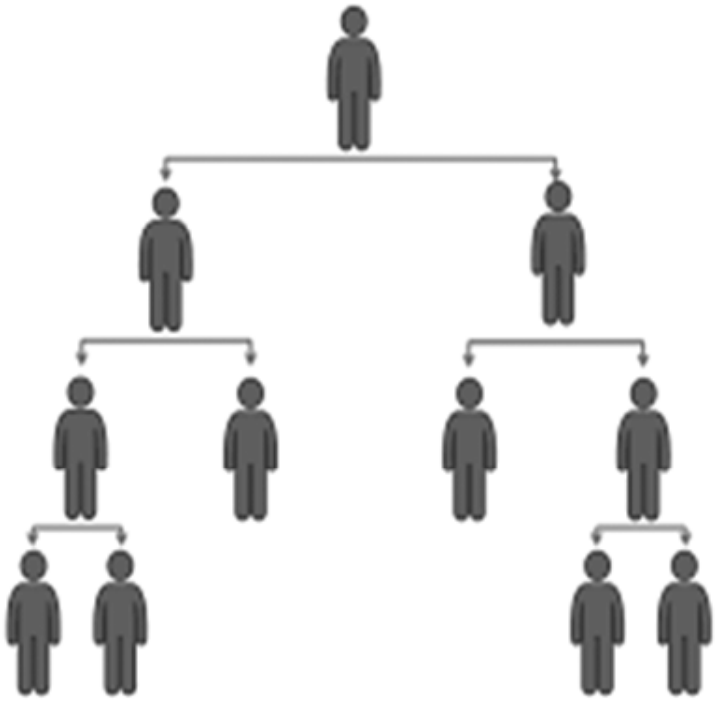

Figure 1: Hierachical Acess structure.

Oriol Farràs and Carles Padró [15] has suggested hierarchical secret sharing schemes, in which share size is same as secret size. It uses matroids and multi partites to provide access structure.

Proposed technique is based on simple hierarchical tree structure secret sharing. In this scheme at each level nodes can used to reconstruct the secret based on threshold based secret sharing.

The next section explains about the delegation of authority using hierarchical general access structure secret sharing.

3. PROPOSED SYSTEM

The proposed system is based on hierarchical access structure where members/employees of the organisation can be arranged at different levels as per their hierarchy in the organisation.

The proposed system is basically satisfies the need of delegation of authority in the organisations. The authorised participant at each level can further extend their access to the next level participants by creating the shares of their received secret/share using secret sharing.

The polynomial based Secret Sharing [1] is used to create the parts/shares. The Shamir's scheme uses Lagrange's interpolation to construct the parts of the secret, and also to get the original secret back from shares/parts.

To extend the rights to the next level construction of shares need to be called and reconstruction procedure need be called to get the original secret back. In absence of any particular authority the next level participants can be utilised based on threshold structure.

In the proposed system Shamir's threshold scheme also called as (t, n) scheme is implemented. In (t, n), '*n*' is total number of participants used to pass the rights to the next level in absence of a particular authorised employee. Out of those *n* shares any '*t*' number of employees need to collaborate their shares/parts to get the original secret back.

In Fig: 3.1 hierarchy of organisation is shown. Here, there are total 4 levels are assumed. Level 1 is

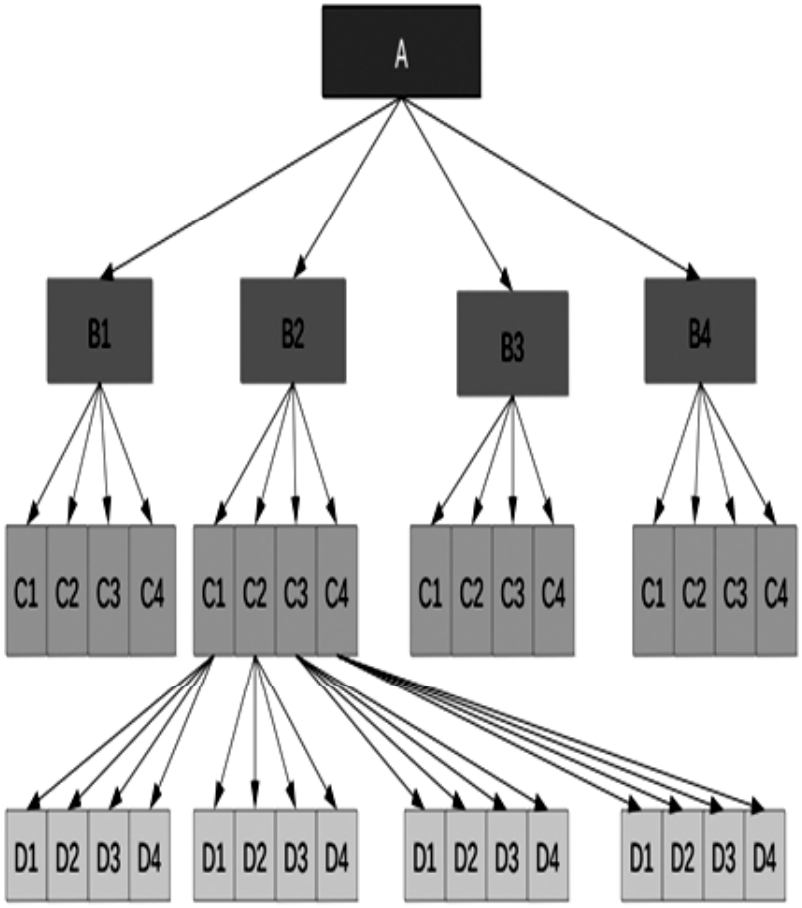

Figure 2: Proposed Architecture

represented by group A, level 2 is represented by group B, level 3 is represented by group C and level 4 is represented by group D. Here n = 4 and t = 2 i.e, (2, 4).

A is at root level or top level. The original secret authority he/she wants to delegate to the next level of employees in the hierarchy of an organisation. At As A is at top level in hierarchy and it wants to delegate its authority to next level i.e in group B. A will implement (t, n) secret sharing construction of shares to create the n parts of the secret. The *n* parts are distributed to n number of employees as their share. At each level, the each individual can extend their authority of that share/secret/part to others at next level using the same process. This can be extended up to any level and up to any n number of employees.

3.1. Distribution of Authority/ Distribution of Shares

Any t shares/part need to be combined to get the original shared part or secret. As shown in Fig: 3.1, it is (2, 4) threshold scheme at each level secret will get divided into corresponding 4 shares. As shown in fig: 3.1 in level 1, A will get divided into 4 unique shares and which will be allocated to next level among group B (i.e B1, B2, B3 & B4). Similarly B1, B2, B3 and B4 will get divided individually in 4 unique shares and will be allocated to respective members of next level.

Let's consider B2 will get divided into 4 unique shares and which will be allocated to next level among group C (i.e B2.C1, B2.C2, B2.C3 & B2.C4).

Similarly B2.C1, B2.C2, B2.C3 and B2.C4 will get divided individually in 4 unique shares and will be allocated to next level respective members. Lets consider B2.C1 will get divided into 4 unique shares and which will be allocated to next level among group D (i.e B2.C1.D1, B2.C1.D2, B2.C1.D3 & B2.C1.D4).

3.2. Reconstruction of shares

As it is hierarchical general access structure secret sharing scheme, which is based on Shamir's threshold scheme or (t, n). Lagrange's Interpolation formula is used to reconstruct the secret back. As here n = 4 and t = 2 i.e, (2, 4). Minimum two shares are required from each level to get the distributed part in that level.

Suppose in the absence of level 1 member i.e A, any two members from next level group can combine their unique shares and will be able for authorised decision. If only B1 is available, and from other members B2, B3 and B4 no one is available. Suppose we want share of B2, then next level respective 2 members can bring their unique shares and generate the share of previous level i.e (B2. C1) and (B2.C3) together generate the share of B2 and that share will be combined with B1 to get the original secret of A. This shows that in absence of B2 also the works get done.

Assume the case study of Academic System. The academic organisation having the hierarchy such as

Principal-> Deans-> Professor-> Associate Professor-> Assistant Professor

All these post of members have different levels of authority. In such systems, Principal will delegate the authority to Deans in his/her absence. Similarly Deans will delegate the authority to Professors, Professors will delegate the authority to Associate Professors and Associate Professor will delegate the authority to Assistant Professors.

Subsequently, the secret of respective level will be recovered by corresponding subsets. If all the corresponding secrets from all levels are revealed then master secret from higher level will be revealed finally.

Consider the threshold scheme of (2, 3), the proposed system will look like as shown in Fig: 2.

The main intention of the proposed system is to delegate the authority to the authorised subsets of the employees. The other important aspect is work should not stopped in absence of any particular employee. It also addresses the problem of reduced trust.

The proposed system is tested for its accuracy and security. The results are discussed in next section.

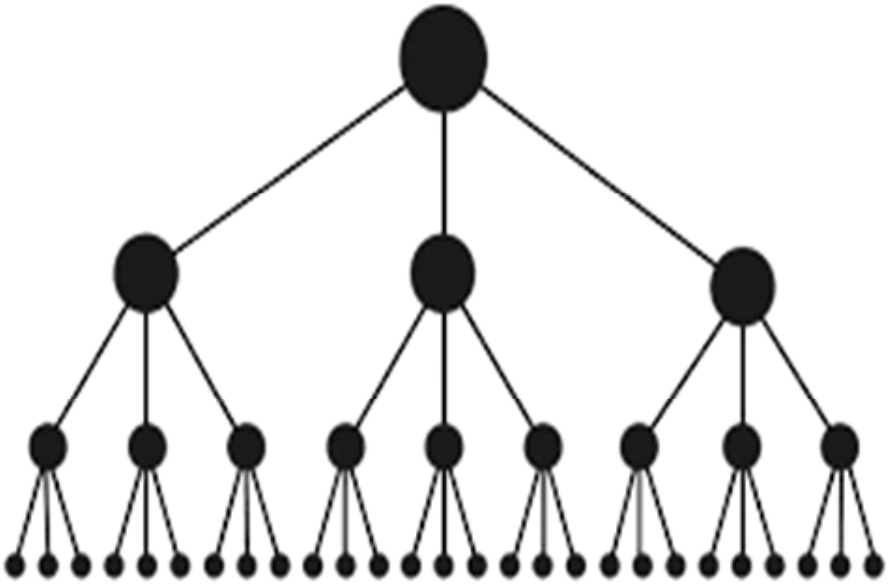

Figure 3: Threshold scheme of (2, 3)

4. RESULTS

To test the accuracy of the proposed scheme the scheme is tested by taking subsets of allowed shareholders and the reconstructed secret is checked with original value.

Similarly unauthorised group of shareholders are asked to submit their shares and checked with original value.

The below table demonstrates the authorized and unauthorized group of shareholders based on the structure discussed in proposed system. The possible authorized subsets and unauthorized subsets are mentioned. These are derived from the structure shown in Fig: 3.

Table 1
Authorized and unauthorized grouping

Sr. No.	*Authorised Subsets*	*Unauthorised Subsets*
1	{B1 & B2}, {B2 & B3},{B3 & B4}, {B1 & B4}	{B1 & B2.C1}, {B2 & B3.C2},{B3.C1 & B4}, {B1 & B4.C4}
2	{B1 & (B2.C1 &B2.C2) }, {B1 & (B2.C1 & B2.C3)}, {B1 &(B2.C2 & B2.C4)},	{B1 & (B2.C1 &B3.C2) }, {B1 & (B2.C1 & B4.C3)}, {B1 &(B2.C2 & B3.C4)},
3	{B1 & (B2.C1.D1 & B2.C1.D2 & B2.C2.D1 & B2.C2.D2)}, {B1 & (B2.C1.D1 & B2.C1.D2 & B2.C2.D1 & B2.C2.D2)}	{B1 & (B2.C1.D1 & B3.C1.D2 & B2.C2.D1 & B2.C2.D2)}, {B1 & (B2.C1.D1 & B4.C1.D2 & B2.C2.D1 & B4.C2.D2)}

These groups of shareholders are asked to submit their shares and reconstruction of secret is implemented.

Table 2
Accuracy Results

Sr. No.	*Subsets*	*Secret Recovered or Not*
1	{B1 & B2}, {B2 & B3},{B3 & B4}, {B1 & B4}	Yes
2	{B1 & B2.C1}, {B2 & B3.C2},{B3.C1 & B4}, {B1 & B4.C4}	No
3	{B1 & (B2.C1 &B3.C2) }, {B1 & (B2.C1 & B4.C3)}, {B1 &(B2.C2 & B3.C4)},	No
4	{B1 & (B2.C1.D1 & B2.C1.D2 & B2.C2.D1 & B2.C2.D2)}, {B1 & (B2.C1.D1 & B2.C1.D2 & B2.C2.D1 & B2.C2.D2)}	Yes

The above table shows the accuracy results as authorised shareholders accurately reconstructed original secret value. Unauthorised group of shareholders could not get the original secret back.

5. CONCLUSION

Access structure kind of secret sharing schemes are very useful where specific subsets of people are needed to assign to take important decision. The proposed scheme can be very effectively utilised for delegation without affecting hierarchy of employees in the organisations. The implemented result proves the accuracy of the proposed scheme, as forbidden set of users can't get access to the secret data. Only authorised set of users are allowed to get the access to the secret data. It provides the flexibility as easily new levels can be added. Also the scalability can be obtained at any level. This will help in expediting the important tasks with high security and trust.

REFERENCES

[1] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] Chih-Ching Thien, Ja-Chen Lin,"Secret image sharing", Volume 26, Issue 5, October 2002, Pages 765–770.

[3] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012

[4] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "An Explication of Secret Sharing Sch emes with General Access Structure" , International Journal of Advances in Engineering and Technology(IJAET) Vol 6,Issue 2, ISSN 2231 – 1963, April 2013.

[5] Kapil Tajane, Sonali Patil, Janhavi Sirdeshpande, "An Explication of Secret Sharing Schemes with General Access Structure" , International Journal of Advances in Engineering and Technology(IJAET) Vol 6,Issue 2, ISSN 2231 – 1963, April 2013.

[6] Mitsuru Ito, Akira Saito, Takao Nishizeki, "Secret Sharing Scheme: Realizing General Access Structure", GLOBECOM IEEE 1987.

[7] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan, "Non-perfect secret sharing over general access structures," in INDOCRYPT, 2002, pp. 409–421

[8] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27-35.

[9] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.

[10] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press,1996, pp. 524-528

[11] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp.207–216.

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

[13] Atanu Basu, Indranil Sengupta, "Cryptosystem for Secret Sharing Scheme with Hierarchical Groups", International Journal of Network Security, Vol.15, No.6, PP.455-464, Nov. 2013.

[14] Arcangelo Castiglione, Alfredo De Santis, "Hierarchical and Shared Access Control", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016.

[15] Oriol Farràs and Carles Padró, "Ideal Hierarchical Secret Sharing Schemes", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 58, NO. 5, MAY 2012.