ANONYMOUS ACCESS STRUCTURES FOR A SHARED SECRET IN A MULTI USER ENVIRONMENT USING BOOLEAN ALGEBRA

P Devaki[#1], Dr. Raghavendra Rao[*2],Kumara swamy[#3]

[#1]*Department of Information Science and Engg,*
The National Institute of Engineering, Mysore, Karnataka, India
[3*2]Department of Computer Science and Engineering,
The National Institute of Engineering, Mysore, Karnataka, India

Abstract
Secret sharing has been a practice to protect a secret key or password in a multi user environment. The secret sharing mechanism allows only the authorized users to participate in the reconstruction of the key and accessing the information. In some situations we need to define the access structures indicating which group of users can collect the shares and reconstruct the secret. The priority can be specified for the users based on various factors to distribute the shares among the users. This paper is about the different access structures which can be defined depending on the positions of the users for an application/organization.

Keywords : Access structure , Boolean algebra , Black box , hierarchical secret sharing , Multi user , Secret sharing

1. Introduction

Secret sharing is a technique to maintain the secrecy of the secret through out the communication, with out letting the unauthorized users know about the secret. Where the secret can be encryption/decryption key, or password or any other secret information. Sharing of secret has been done using different techniques. Secret sharing is very important in a multi user system, where more than one user is authorized to use the system. It may be a key to encrypt or decrypt the information, or it may be a password required to get in to the system, or it may be a sensitive data to be transmitted/stored in a network. So here the key, password and sensitive information is considered to be secret information which needs much attention in maintaining its secrecy. It is necessary to have a good technique to control the access and maintain the secrecy of the secret information. Where at no point of time any user will have information about the full secret, instead each user will have a share of the secret. Secret sharing method avoids the unauthorized access to the information by a single or a group of users with out the knowledge of the other users. But the access structure is defined with out the users knowledge so that there will be some hierarchy maintained while reconstructing the key. The dealer defines the hierarchy which is unknown to the users. This provides another level of confidentiality among the users. Based on the hierarchy the different users will get different number of shares.

Why we need secret sharing?
Example 1: if a set of users of an organization is authorized to encrypt or decrypt the messages that are sent or received in the organization, then the set of users must have the key to encrypt or

decrypt the message. This requires that each user in that set must know the key. This poses a threat, because if any one of the users is a disgruntled or compromised then the key may be given to an unauthorized user, or the user may manipulate the data according to his benefits. This is an unexpected event which must be prevented all the time as long as the key is being used by all the users of that set.

Example 2: if a system where the sensitive information is stored is allowed to be used by a set of authorized users, it requires a password. If all the users know about the password, then there may be a threat as mentioned in example 1. This must be prevented.

Example 3: if sensitive information is stored in a system and a set of users are allowed to access the information or modify the information, any disgruntled user may try to misuse the information or damage information or modify the information in such a way that there may be huge loss for the organization. So, even this must be prevented.

Example 4: if sensitive information needs to be transmitted over the network if the information is a big text file or image / audio/image then it requires large bandwidth. Another problem is while transmitting over the public network like internet, it is likely that the information gets hacked, or modified or destroyed etc.

There can be lots of examples which deal with the integrity and trustiness of the users.
Even though the organization authorizes a set of trusted users some times any of the users may become untrusted due to various reasons under various circumstances.
So the objective is to maintain the secrecy of the key/password/information from all the trusted users and untrusted users also, so that no user will have the knowledge about the complete key/password/information.
This is where the secret sharing plays an important role in maintaining the secrecy of the key/password/information.
In this paper we discuss the various access structures which are based on hierarchical and flat secret sharing.
The remaining part of the paper is organized as follows. Section 2 has the concept of secret sharing. Section 3 explains the meaning of hierarchical and flat secret sharing. Section 4 explains access structures.
Section 5 gives proposed design. Section 6 gives conclusions.

2. Secret Sharing

Instead of giving the complete key/password/information to all the authorized users, it is better to divide the secret among the users so that at any point of time all the users will have the partial information about the key/password/information. When the key/password/information is required by a user, that user can send a request to all the users in that group. Once all the users send their shares, the user reconstructs the key/password/ information with out coming to know about the shares of the other users. This ensures that which user has requested for the key/password/information.
One important point we can note here is, even if a user compromises his share to an unauthorized user due to some reason it is of no use for the unauthorized user, as he requires the other shares also to reconstruct the key/password/ information. This ensures the integrity of the users with

respect to key. Shamir [1] first proposed this secret sharing later on many people have worked in the same field. In general the key/password/information can be text, image, audio or video. He proposed a threshold secret sharing where in instead of collecting all the shares to reconstruct the key, a user can collect only the threshold number m (m,n) of shares out of n number of shares to reconstruct the key. This reduces the waiting time and also the traffic in the network.

The trusted dealer will prepare the shares and distribute among the users of a group. The dealer is not the user who involves in any communication. His job is to just divide the secret based on the number of users for a group and distribute the shares to all the authorized users of that group.

Many people have recommended several methods to divide and reconstruct the key based on threshold value. Threshold secret sharing has been defined by [1] [2] [3] which are of different approaches.

Normally the shares will be distributed to the users equally. Some times the dealer may specify the hierarchy for users while distributing the shares. That is based on the hierarchy number of shares may be given to users. So this is referred to as access structure. If all the users are having the same hierarchy then it is referred to as flat secret sharing. Other wise it is referred to as hierarchical secret sharing.

3. Hierarchical and flat Secret Sharing

The users may be categorized in to various levels based on their position and power in the organization [4]. This information must be known to the dealer.

3.1 hierarchical secret sharing:

Example: in a bank, manager has more power than any other employee, then the assistant manager, then the other employees. Similarly in the other organizations there will be hierarchy among the employees.

This hierarchy can be considered while distributing the shares to users. More the level and power, more number of shares can be provided.

Example: manager can get 3 shares, assistant manager 2 shares and other users can get 1 share each. While reconstructing the key, the required number of shares will be collected based on the threshold value. For this various access structures can be defined. The advantage of hierarchical secret sharing is , number of users may be reduced and so the number of shares need to be collected from the users will be reduced.

The flat secret sharing is dividing the secret in to n number of shares based on the n number of users. Each user will get a single share. Based on the threshold defined (m,n) , the reconstruction of the key can start immediately after collecting m number shares instead of waiting to collect all the shares. Here, there is no priority among users.

One of the limitations of flat secret sharing is that, minimum n number of users need to submit their shares. Even if n-1 number of users send their shares also, it is not at all possible to reconstruct the key. This indicates that no user will have more than one share, and reconstruction requires any of the n number of users to submit the shares.

4. Access structure

Here we are considering an organization where the president, vice president and members are the users of the system. Since president has more powers he can get more number of shares, the vice president can get more than one but lesser than the presidents number of shares, and the members can get one each. P1 is the president, P2 is the vice president, m1, m2, m3, and m4 are the members[4] [5].

If the secret sharing is based on the following threshold, then the different access structures can be defined.

The threshold is (3, 6) where 3 is the minimum number of shares required to construct the key and 6 is the total number of shares. There are 6 users where 1 president,1 vice president and 4 members.

Access structure 1: president will be given 3 shares out of 6 shares. Vice president with 2 shares and remaining one share will be given to all the other members in the group. This indicates 3 levels among the users.

President is the level 1 member. Vice president is the level 2 member. And the remaining users are the level 3 members.

So the access structure can be as follows

{P1}

{P2 and (m3 or m4 or m5 or m6)} is the access structure. This indicates that president alone can reconstruct the key by using his 3 shares or 1 vice president and any one member can construct the key.

This access structure theoretically looks good, but practically there will be an issue. The president alone can reconstruct the key, but the objective is to see that no single user can get in to the system. Also there is no guarantee that he will not compromise the key.

But the other 2 groups do not have any problem because more than 1 user is involved, hence if one user gets compromised, it's of no use. Because with one share , it is not possible to construct the key.

But this access structure has got another issue, in case if both the president and vice president are not available, then there is no way that the secret can be reconstructed. This is because all the level 3 members have the same share.

Instead of giving 3 shares to president 2 shares can be given to president and 2 for vice president and one each for the members. Then the access structure can be as follows

Access structure 2:
{P1 and P2 }
{P1 and m3 or m4 }
{P1 and m5 or m6}
{P2 and m3 or m4 }
{P2 and m5 or m6}

This will ensure that at no point of time a single user is able to reconstruct the key.

This also gives the flexibility of having 3 levels of users to access the system by providing different number of shares. This requires at least 2 levels of the users to participate in the reconstruction of the key.

Here the president and the vice president are given with 2 mutually exclusive shares each. The remaining 2 shares are given to the 4 members which is repeated. 2 members get 1 share.

Access structure 3:
P1 and P2 share 3 shares, and remaining 3 shares are distributed to the 4 members.
{P1 and P2}
{P1 and {m1 or m2 or (m3 or m4)}}
{P2 and {m1 or m2 or (m3 or m4)}}
{m1 and m2 and (m3 or m4)}

In this access structure, it is possible to reconstruct the key with out the participation of the president or the vice president. The 3 members out of 4 can reconstruct the key with 3 shares.

Here we have defined 3 access structures. Each access structure has several groups of users who can reconstruct the key/password/information.

3.2 Flat secret sharing:
In this all the users get 1 share each. Here there are no levels among the users. All the users are in the same level. Any user can reconstruct the key by obtaining at least 2 more shares from any of the 2 users from the group.
{(m1 and m2 and m3) or (m1 and m2 and m5) (m1 and m2 and m6) or (…….)…….}

Organization can decide whether to follow hierarchical or flat sharing based on the application.

5. Proposed work

We have used shamir's threshold secret sharing method to divide the secret. (3,6) is being used , where 3 is the threshold value which indicates the minimum 3 shares is required to reconstruct the secret out of 6 shares of the secret. The shares will be distributed according to the access structures defined. A black box is used to collect the shares, where the black box defines the various groups who can reconstruct the secret, which is unknown to the users.
The reconstruction of the shares is performed by using Lagrange's interpolation method.

In this method a polynomial of order m-1 will be used. For (m,n) threshold secret sharing.

The polynomial is used to share the secret by considering the coefficients.

$F(x) = S + C1x + C2x^2 \ldots\ldots\ldots + Cmx^m$

Where S is the secret to be shared, C1, C2 … Cm are coefficients. The coefficients can be any random integer values.

$$F(x)= \frac{(x-x1)(x-x2)}{(x0-x1)(x0-x2)} y0 + \frac{(x-x0)(x-x2)}{(x1-x0)(x1-x2)} y1 + \frac{(x-x0)(x-x1)}{(x2-x0)(x2-x1)} y2 + \ldots\ldots\ldots\ldots$$

is the interpolation formula using which it is possible to reconstruct the secret.

EX: [6]

The polynomial is

$F(x) = 222 + 3x + 2x^2$

We can select 5 values for x and calculate F(x).

Y1= F(x1) = 227

Y2=F(x2)= 236

Y3 = F(x3) = 249

Y4 = f(x4) = 266

Y5 = F(x5) = 287

Y6 = F(x6) = 312

After obtaining the shares y1 to y5, the shares along with the values of x for each user can be given to the users as follows.

U1 = (x1, F(x1)) = (1, 227)

U2 = (x2, F(x2)) = (2, 236)

U3 = (x3, F(x3)) = (3, 249)

U4 = (x4, F(x4)) = (4,266)

U5 = (x5, F(x5)) = (5, 287)

U6 = (x5, F(x6)) = (6, 312)

The shares will be distributed to the users based on the access structures.

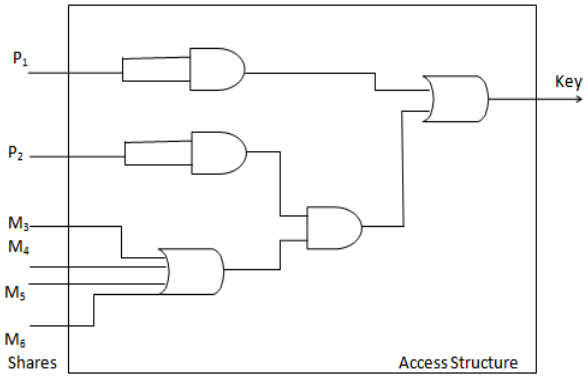

Fig-1 Access structure 1

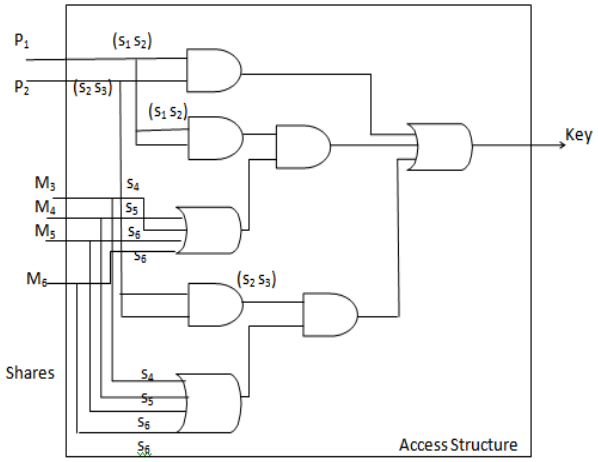

Fig-2 Access structure 2

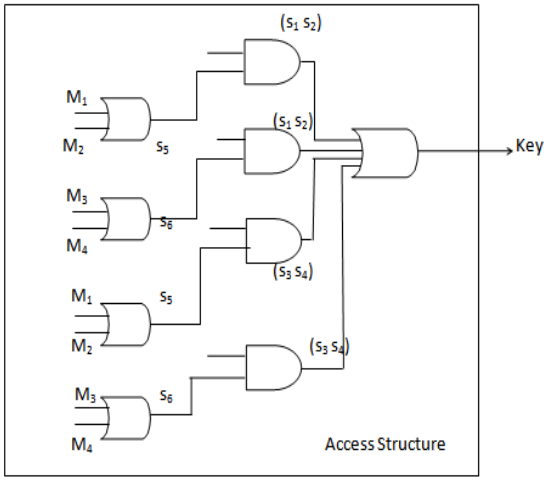

Fig-3 Access structure 3

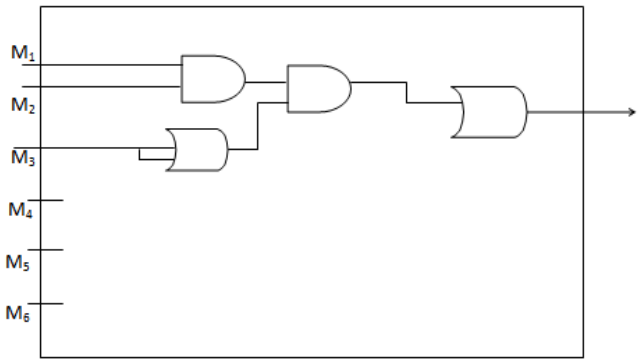

Fig-4 Access structure 4

6. Conclusions

In this work we have shown 3 access structures which are based on hierarchical secret sharing. This proves that the levels among the authorized users of the system can be maintained and tracked in case of any untoward incidents. We have also shown the flat secret sharing, which doesn't have any levels. The levels can be maintained based on the severity of the secret. The hierarchical secret sharing ensures that more than one level of users are involved in the reconstruction of the key.

References

[1] A. Shamir, "How to share a secret," *Comn.ACM.*, **22**(1979), 612-613.

[2] G. Blakley, "Safeguarding Cryptographic Keys," *AFIPS Conference Proceedings*, **48**, 1979.

[3] C.C. Thien, J.C. Lin, Secret image sharing , Comput. raphics 6 (5) (2002) 765–770.

[4] Tamir Tassa, "Hierarchical Threshold Secret Sharing ", Journal of Cryptology , Online Publication ,Feb 07-2007.

[5] Vidyasagar M. potdar , Song Hon, " fingerprinted secret sharing stegnography for robustness against image cropping attacks" , 3rd IEEE international conference on Industrial informationics (INDIN) , 2005

[6] P Devaki , Dr G Raghavendra Rao , "A novel way of providing Confidentiality to shared secret key and authenticate the shares during reconstruction " , International conference on Information technology and control automation, Chennai , july 14-15 ,2012.