IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.

www.ijiset.com

ISSN 2348 – 7968

Hybrid Key Sharing

Sahana H R, Chaithra S, Pavana K E, Poornima P

Department of Information Science and Engineering

The National Institute Of Engineering, Mysore-8 Karnataka, India

ABSTRACT

Let us consider the problem of secret sharing with Hierarchical structure. Here the secret will be shared among group of m members, i.e, divided into different levels. Members are said to be authorized if they have atleast m0 members form the highest levels, as well as atleast m1>m0 members from two highest levels and so on. Members will differ in their authority and the presence of higher level member is essential in order to recover the secret. None of the existing system address the setting where a bank transfers should be signed by three employees, where in atleast one of them must be a Department Manager. For this problem we are considering secret sharing scheme which is suitable for the Hierarchical structure. The secret is represented in Shamir's scheme as free co-efficient of some polynomial.

Keywords-- *Pre-shared key; Cipher text; Access server; Admin server; Encryption.*

1. INTRODUCTION

A (n,m) Hierarchical secret sharing is a method of sharing a secret among a set of m members, such that every n of those members(n less than or equal to m) are needed to recover the secret by providing their share together, while secret could not be recovered if its less than m members. Generalized secret sharing refers to collection of U-users with N-keys. This generalized secret sharing is a method of sharing secret among the U users, such that only subsets in pre-shared may recover the secret, while remaining subsets cannot. There are many real time examples of hierarchical secret sharing. Some examples are sharing a key to control locker in a bank, triggering mechanism for nuclear weapons etc., Here we have taken the example of bank secret sharing scenario, it is natural to expect that the members are not equal in their authorities. For example the shares of locker key may be distributed among bank employees, some of whom are tellers and some are Department Managers. The could require the presence of say 3 employees in opening the locker but atleast one of them must be a department manager.

2. PROPOSED SYSTEM

In our project we have taken example of bank. Initially the user has to open an account in a bank and has to ask for the locker in order to keep all his document in the locker. For this purpose we have maintained two servers, one is Admin server

ISSN 2348 – 7968

and the other is access server. Admin server will keep track of entire user details, he acts as the key generation agent, maintains user accounts, provides resources for creating and managing user accounts and assign resources to the users. It also creates pre-shared keys and distributes those keys among the users.

Access server is mainly used to provide access to the lockers by the valid user. In order to access the locker, initially user has to enter his account number, locker number and his pre-shared keys. As soon as the user enters his pre-shared key, the manager and the clerk will get a message saying that this user needs to access his locker, so provide your respective pre-shared keys. When both of them receives this message they will provide their pre-shared keys. These pre-shared keys of manager, clerk and user are needed for generating the cipher text. This cipher text will be generated by the access server using pre-shared keys. Using cipher text user account number and locker number will be encrypted. The original encrypted data will be sent to the Admin server, there Admin server will decrypt the data using cipher text, then the decrypted locker number and account number will be matched with the locker number and account number entered by the user initially[for encryption and decryption of data we are using symmetric algorithm, for generation of pre-shared key and reconstruction of cipher text Shamir's algorithm has been used.]. If it is matched , signal will be sent to the access server saying that he is a valid user and allow him to access his locker otherwise he is not a valid user and he will be blocked to access the locker.

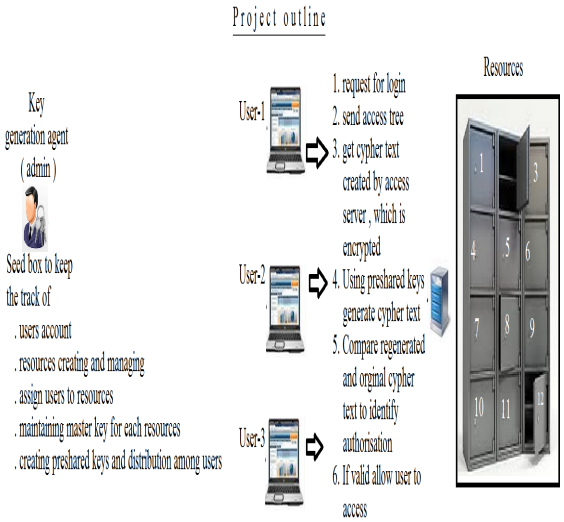

Fig 1. Locker System Design

1. *Shamir's Secret Sharing*

Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

2. *Mathematical definition*

Formally, our goal is to divide some data D (e.g., the safe combination) into n pieces D1,…,Dn such a way that:

1. Knowledge of any k or more Di pieces makes D easily computable.

2. Knowledge of any k-1 or fewer Di pieces leaves D completely undetermined (in the

ISSN 2348 – 7968

sense that all its possible values are equally likely).

This scheme is called (k,n) threshold scheme. If k=n then all participants are required to reconstruct the secret. Choose at random k-1coefficients a1,…,ak-1 in F, and let a0=S. Build the polynomial f(x)=a0+a1x+a2x2+a3x3+…+ak-1xk-1. Let us construct any n points out of it, for instance set i=1,…,n. The result of the polynomial with different instance which is generated are distributed to the participant.

REFERENCES

1] Aho,A.,Hopcroft,J.,and Ullman,J. The Design and Analysis of Computer Algorithms. Addison-Wesley, Reading, Mass.,1974.

2] Blakley, G.R.Safeguarding Cryptographic Keys. Proc.AFIPS 1979 NCC, Vol.48,Arlington,Va.,June 1979 pp.313-317.

3] Knuth,D. The Art of Computer Programming,Vol.2:Seminumerical Algorithms. Addison-Wesley, Reading ,Mass.,1969.

4] Liu,C.L. Introduction to Combinatoria Mathmatics. McGraw-Hill,Newyork,1968.

5] Rivest,R.Shamir.A. and Adleman,L. A method for obtaining Digital Signatures and Public Cryptosystems. Comm.ACM 21,2 Feb.1978, 120-126.

6] Shamir,Adi(1979),” How to share a Secret”, Communications of the ACM 22(11):612-613.

7] Dawson,E.;Donovan,D(1994),” The breadth of Shamir’s Secret-Sharing Scheme”, Computers and Security 13:69-78.