ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Data Security in Proactive Network using Secret Sharing Mechanism

Himanshu Gupta[1], Vasudha Arora[2]

M. Tech Scholar, Dept. of CSE, Manav Rachna International University, Faridabad, India[1]

Assistant Professor, Dept. of CSE, Manav Rachna International University, Faridabad, India[2]

ABSTRACT: For most of the cryptosystems, using a single master key system is not enough to protect important documents, there is a need of many encryption and decryption keys for this purpose. A Secret Sharing Scheme is the method which divides the secret into several parts and distributes them among the specific communicating entities in such a way that only these participants can reconstruct the secret by poling there share. Hence, unauthorised entity cannot reconstruct the secret. The best way to implement such a system is in cloud environment.
Shamir's(t, n) threshold scheme is one of the most well-known and widely used example of secret sharing systems.

KEYWORDS: Secret Sharing; Shamir's secret sharing scheme; shared key; secret key;

I. INTRODUCTION

Security is concerned with the ability of a system to prevent it from unauthorized access to information and services. Confidentiality, Integrity and Authenticity are fundamental objectives of security. Many group-oriented applications require communication confidentiality, means that the information of a group should not be exposed to any outsider, but the question is whom to trust. There are many examples when even well-established trusted entities also become malicious. One solution to such a problem is instead of placing trust in just one party to distribute the trust among a group of trusted entities.

There are several known cryptographic concepts that address the question for distribution of secret. Some of them are secret sharing schemes, verifiable secret sharing schemes, and multiparty computation [1].

Although a well-known term within the cryptographic community, secret sharing might be a bit misleading for an outsider [2]. It does not mean two or more people sharing one secret. It means two or more people are having shares of the secret. One secret is split into n different shares. Ideally, it should be impossible to gain any information about the secret with less than n shares.

To provide fundamental objectives of security one-time session keys need to be shared among communication entities to encrypt and authenticate secrets. Thus, before exchanging communication messages, a key establishment protocol needs to issue a one-time secret session keys to all participating entities. The key establishment protocol also needs to provide confidentiality and authentication for session keys. There are two types of key establishment protocols: key transfer protocols and key agreement protocols. Key transfer protocols rely on a mutually trusted key generation centre (KGC) to select session keys. KGC sends the session keys to all other shareholders of the original secret. In key agreement protocols, all communication entities are involved to determine session keys [5].

To explain secret sharing consider the example: Suppose you and your friendhave a joint account in which you have deposited your money. If both have passwords for that account or anyone have password for that account then you are worried about the integrity of your friend that he might withdraw all the money and cheat you and so as your friend. Now who is going to keep the password? Now, we need a scheme such that the password is shared between both of you in such a way that both shares of password are required in order to open that account. Individual shares will be useless. Now, you and your friend can be assured that the other will not take all the money without the consent of both. This illustrates the concept of secret sharing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

In cryptography, secret sharing refers to any method for distributing a secret among a group of participants, eachparticipant will have a share of that. The secret can be reconstructed only when the shares are combined together; individual shares are of no use. To implement such a scheme the most simple and commonly used technique is Shamir's secret sharing scheme.

Secret sharing schemes can be used in equivalent situations, or perhaps to safely increase data availability, just to name two examples. Secret sharing is not only an interesting information-theoretical concept, but it also has several practical applications.

II. RELATED WORK

In [13], author conclude that in multi cloud data is replicated so the data is available even if the cloud is fail, they also conclude that the Shamir's secret sharing mechanism has a variety of advantages such as security and client side aggregation etc.

In [14] the author proposed a very important concept in cloud computing is Self-Destructing data. In shared data an item if they are available for a long time it will considerably decrease the security and also increases the complexity of managing the files. Hence, in this Self –Destructing system the data files are automatically be deleted if they are not needed any more.

In [8] the author introduces a method to increase the efficiency of DES. In this scheme the data is encrypted using DES used with secret key and this data is send only to a group of trusted entities and KGC is shared between sender and receiver. This data can only be decrypted with KGC.

In [10] the authors have discussed about various secret sharing mechanisms.

In [15] it is shown that owing to the distributed nature of cloud, information dispersal is more secure and optimal approach for data outsourcing.

III. SHAMIR'S SECRET SHARING

Shamir's Secret Sharing is a scheme in which a secret is divided into several parts giving each part to corresponding trusted participants in a group where some of the parts or all the parts are needed to reconstruct the secret. A threshold scheme is used in order to reconstruct the secret where K is any number of sufficient parts needed to reconstruct the secret as it may be impractical to have all the parts at the time of reconstruction. This threshold scheme is based on Lagrange Polynomial Interpolation method.

A. Sharing Protocol

Goal: To share a secret S among $E_1, E_2, \ldots\ldots\ldots\ldots, E_{n,}$ number of trusted entities.

1. Suppose we want to use a (K, n) threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < K \leq n < P; S < P$ 0 and P is a prime number.
2. Choose at random K - 1positive integers $a_1, \ldots\ldots\ldots a_{K-1}$with $a_i <$ P, and let a_0 = S. Build the polynomial
$$f(x) = a_0 + a_1 x + a2_2 x^2 + a_3 x^3 \ldots\ldots\ldots + a_{K-1} x^{K-1}$$
3. Construct n random distinct evaluation points $= 1 \ldots\ldots\ldots n : X_j \neq 0$ and secretly distributes the shares to corresponding trusted entityE_j.
$$share_j(s) = (X_j, f(X_j)); \; j = 1 \ldots\ldots n$$

B. Reconstruction Protocol

Goal:to reconstruct the secret from K out of n shares:

1. Use Lagrange Interpolation to find unique polynomial $f(x)$ such that $degree\ f(x) < K$ and $f(j) = share_j(S)$ for $j = 1,2 \ldots\ldots t$.
2. Calculate $f(0)$ = the reconstructed secret.

Lagrange interpolation: $f(x) = \sum_{t=1}^{t} f(i) * L_i(x); where\ L_{i(x)} = \frac{\prod_{j \neq 1}(x - x_j)}{\prod_{j \neq 1}(x_i - x_j)}$ is the Lagrange polynomial which has value 1 at x_i, and 0 at every other x_j.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

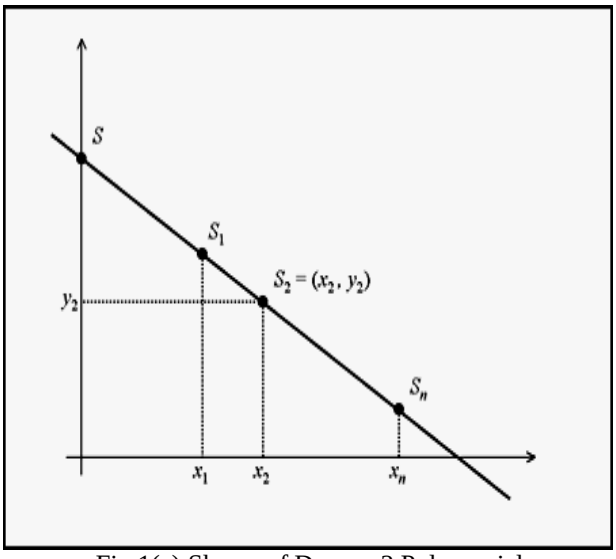

Fig 1(a):Shares of Degree-2 Polynomial

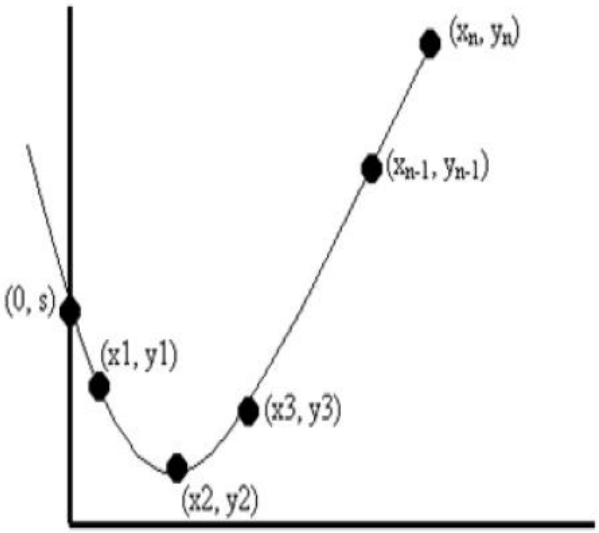

Fig 1(b): A Degree-2 Ploynomial

IV. PROACTIVE SECRET SHARING

Proactive Secret Sharing (PSS) is a scheme that allows the servers to regenerate a new set of shares from the old ones periodically without reconstruct the secret. This protocol will allow servers to recover from possible undetected attacks. It will provide the servers with new shares of secret without actually modifying the actual secret. The information (shares) gathered by an attacker before the refreshment period will become useless after the refreshment to detect the secret. Before executing the next PSS, every server checks the integrity of its state and code with no PSS, using an (t, n) secret sharing scheme, a service can tolerate up to t-1 compromised servers, because if any more servers are compromised the secret is exposed. In case of PSS, we know that it refreshes all its shares at some time interval,so as to make old shares useless. Now an adversary needs to gather at least *t* shares between two executions of the PSS,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

which will make it more difficult for attacker to get the secret. The secret remains confidential if less than *t* servers are compromised from the start of one PSS to the end of the next PSS.

The basic methodology used to renew shares is given below:

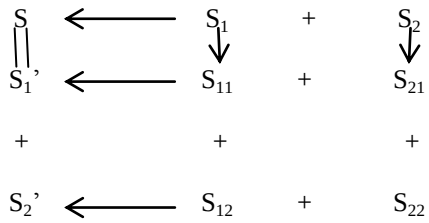

Fig 2: Method used to Renew Shares

A. Basic Share Renewal Protocol

The goal here is to renew the shares without changing the secret. The shareholders should agree on a new polynomial with the same secret *S*. At the end, each shareholder/entity will have a new share on the newpolynomial of degree $t-1$. Every share holder/entity must remember its original share.

The protocol at the beginning is as follows:

1. Everyi^{th}entity$i \in [1 \ldots . n]$randomly picks $t-1$numbers from a finite field. These numbers define a polynomial *Pi(X)* of degree $t-1$whose free coefficient is zero$P_i(0)=0$.
2. Using VSS Each i^{th}entity distributes the shares of *Pi(X)* among the participating entities.
3. Everyi^{th}entity receives the following shares:$P_1(i), \ldots \ldots, P_n(i)$ including his own made share $P_i(i)$and calculates its new share by adding its old share- $f(i)$to the sum of the new *n* shares. Mathematically speaking:$h(i)=f(i)+\sum_{c=1}^{n} P_c(i)$.
4. Everyi^{th}entity erases his/her old share $-f(i)$.

B. Detection of Corrupted Shares

In this secret sharing scheme each participating entity wants to be sure that shares of other entities is not corrupted or revealed. There are many reasons that shares are not available such as disk crash, server crash, any hacker attacked one of the shares, now the question is how we would know that the share is attacked by a hacker. One solution to this problem is periodical secure broadcast to compare shares. One should save some traces of shares for this purpose.

This can be done as follows:

1. Do Verifiable Secret Sharing (VSS), so the encryption of each share is saved at each entity site.
2. Each i^{th} entity updates his shares using homomorphic property for every j as:$E\big(h(i)\big)=E(f(i))\times \prod_{m=1}^{n} E(P_m(j))$.

C. Reconstruction of Corrupted Share

Reconstruction is the most important phase of this scheme. The algorithm for reconstructing the corrupted share is given below:

1. Everyi^{th}entity$i \in [1 \ldots . r-1],[r+1 \ldots \ldots n])$ randomly chooses a polynomial $P_i(X)$ of degree $t-1$ where $P_i(r)=0$ and $P_i(0)\neq 0$.
2. Everyi^{th}entity distributes shares of $P_i(X)$: $P_i(1) \ldots \ldots P_i(n)$ using VSS among the shareholders.
3. Now, every i^{th} entity has $P_i, \ldots \ldots, P_{r-1}(i), P_{r+1}(i), \ldots \ldots, P_n(i)$ and calculates its updated new share for *r*: $h(i)=f(i)+\sum_{c=1}^{r-1} P_c(i)+\sum_{K=r+1}^{n} P_k(i)$ and sent it to *r*.
4. Now, the r^{th}entity decrypts all these shares and recovers$f(r)$ by using interpolating property of Lagrange's theorem. Here it has a new polynomial which has value equal to the old corrupted share i.e. $h(r)=f(r)$.

V. SIMULATION AND RESULTS

To simulate our work we have used CloudSim simulator along with Amazon Web Services and Net beans IDE.CloudSim is a web app that runs in a virtual machine on the Amazon Web Services (AWS) cloud. It allows users to launch, terminate and monitor virtual machines in the AWS cloud. Different configurations can be launched,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

depending on the requirements, and available machines on the cloud. Each CloudSim configuration maps to a constellation, which are collections of multiple virtual machines running together. The key provided from AWS is the token that allow CloudSim to access AWS on behalf of the AWS user. Figure 3 below shows how the key first is divided into several shares and then it is recombined to regenerate the secret.

```
run:
Prime Number: 137
a1: 92
a2: 118
a3: 129
a4: 119
a5: 78
a6: 89
a7: 127
a8: 123
a9: 54
Share n.1: 93
Share n.2: 30
Share n.3: 74
Share n.4: 98
Share n.5: 78
Share n.6: 40
Share n.7: 13
Share n.8: 99
Share n.9: 41
Share n.10: 90
Share n.11: 64
Share n.12: 103
Share n.13: 72
Share n.14: 106
Share n.15: 89
Share n.16: 131
Share n.17: 103
Share n.18: 129
Share n.19: 48
Share n.20: 94
The secret is: 123
```

Fig 3: Snapshot of Key Division and Regeneration

Below the Figure 4 and Figure 5 shows the graph for Key Division and Key Regeneration from shares for a 128 bit key with n = 10.

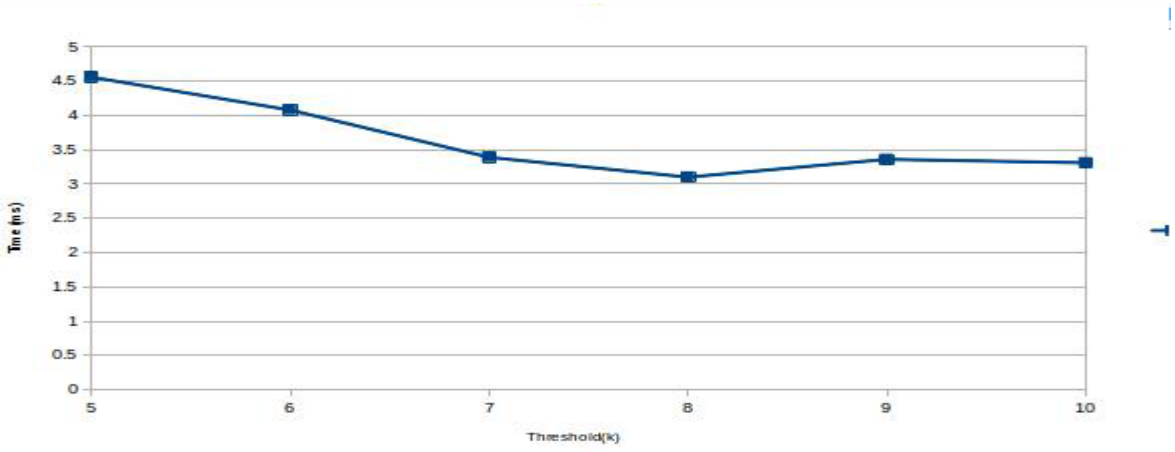

Fig 4: Key Division for 128 bit key with n= 10

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

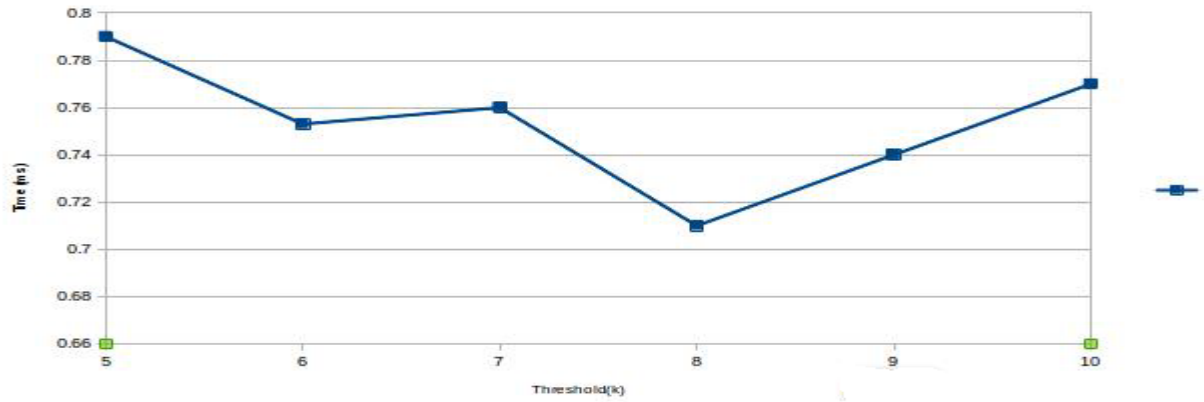

Fig 5: Key Regeneration from Shares for 128 bit key with n= 10

VI. CONCLUSION

This research showed a very important cryptographic concept – Secret Sharing Scheme which is given by Adi Shamir. In a Secret Sharing Scheme generally we have a secret which is divided among several trusted entities. The secret shared can only be recovered by these trusted entities. This scheme is very useful and efficient in safeguarding cryptographic keys. It is based on Lagrange Polynomial Interpolation Theorem to design several groups or classes of secret sharing. This scheme also has some useful properties such as homomorphic and a multiplicative property which makes it suitable for threshold based cryptography. So, we conclude that it is an efficient scheme where the secret is shared in a group because the unauthorised or outside entity cannot get the access to the information shared in a group without having at least threshold number of shares of the decryption key used to encrypt the information.

REFERENCES

1. Fredrik Olsson, "A Lab System for Secret Sharing", 2004.
2. N. Ferguson & B. Schneier, "Practical Cryptography", 2003, pp. 358-360
3. A.Shamir," How to share a Secret",Comm ACM, Vol.22, no.11, pp.612-613, 1979.
4. LeinHarn and Changlu Lin, "Authenticated Group Key Transfer Protocol Based on Secret Sharing" IEEE transactions on computers, vol, 59,No.6, June 2010 IEEE.
5. W.G.Tzeng. " A Secure Fault-Tolerant Conference Key Agreement Protocol," IEEE Trans.Computer, Vol.51,no.4,pp.373-379,Apr.2002
6. LeinHarn and Changlu Lin, " Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEE Trans. Computers, Vol .59, No.6,pp.842-846, June2010.
7. Saria Islam, A. S. M MahmudulHasan, "Implementation of Shamir's Secret Sharing on Proactive Network", International Journal of Applied Information Systems(AJAIS) , Foundation of Computer Science FCS, New York, USA, Vol.06, No. 02, pp. 17-22, September 2013.
8. YaminiIndla, M. Sampat Kumar, "Extended Group Key Transfer Protocol for Authentication Using DES based on Secret Sharing in Cloud" International Journal of Emerging Technology and Advanced Engineering(IJETAE), Vol. 02, Issue 11, pp.541-551, November 2012.
9. Mrs.Komal Ate, Prof. S. D Potdukhe, "Data Sharing in Cloud Storage with Key-Aggregate Cryptosystem", International Journal of Engineering Research and General Science(IJERGS), Vol. 02, Issue 06, pp. 882-886, October-November 2014.
10. DnyaneshewarSupe, AmitSrivastav, Dr. Rajesh S. Prasad, "Review of Methods for Secret Sharing in Cloud Computing", International Journal of Advanced Research in Computer Engineering and Technology(IJARCET), Vol. 02, Issue 1, pp. 11-17, January 2013.
11. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
12. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in *IEEE Cloud*, June 2012, pp. 295–302.
13. Swapnila S. Mirajkar, Santosh Kumar Biradar, "Using Ssecret Sharing Algorithm for Improving Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Technology(IJARCST), Vol 02, Issue 02, Ver. 03, pp. 395-398, April-June 2014.
14. Ranjith. K, P.G. Kathiravan, "A Self-Destructing System for Dynamic Group Data Sharing in Cloud", International Journal of Research in Engineering and Technology(IJRET), Vol. 03, Special Issue 07,pp. 265-270, May 2014.
15. S. Jaya Nirmala, S. Mary SairaBhanu, AhteshamAkhtar Patel, "A Comparative Study of Secret Sharing Algorithms for Secure Data in the Cloud", International Journal of Cloud Computing: Services and Architecture(IJCCSA), Vol. 02, No. 04,pp. 63-71, August 2012.