Aggrandized Authenticated Secret Sharing

Sachin Sonawane
Professor of Computer Engineering
Atharva College of Engineering
Mumbai, India

Chetana Pawaskar
Computer Engineering
Atharva College of Engineering
Mumbai, India

Vishwajit Gupta
Computer Engineering
Atharva College of Engineering
Mumbai, India

Shubham Gawai
Computer Engineering
Atharva College of Engineering
Mumbai, India

***Abstract*- Shamir algorithm is used to divide passwords between N number of users in such a way that minimum k number of users are required to regenerate the original password .but Shamir algorithm is vulnerable to as it uses Lagrange interpolation formula to regenerate original password if one of the N user is able to find one or more passwords using trial and error. The more key he finds the faster he can get k number of keys. In order to avoid this we add hash bytes to the generated passwords thereby making it impossible to use trial and error to get the keys also the user will be notified about the person who may be trying to find a new key. Because if the key is altered the hash bytes won't match.**

Keywords—Secret sharing, cheater detection.

I . INTRODUCTION

As the name implies, Shamir's secret sharing is created by Adi Shamir, a famous Israeli cryptographer, who also contributed to the invention of RSA algorithm. Shamir's secret sharing is an algorithm in which the secret key is divided into equal number of shares.

Imagine a case where you have to encrypt a data from the system. Using any encryption method, you must store the secret key used in the encryption in order to decrypt later. The key has to be much secured. If the key is stolen by intruder, your data will be easily decrypted. However, storing a key is always a difficult problem.

This problem of storing and sharing secret key is always difficult for administrators. However, if you use Shamir's secret sharing algorithm with the hash algorithm you can solve the two problems to greater extent. You can divide your secret key into parts and distribute them to other administrators. Each administrator will have a part of secret key, but knowing a part of a key is not enough to recover the original secret. Because attacker must compromise multiple administrators' key parts, secret generated by Shamir's secret sharing is very difficult to be compromised. Even if the attacker known the share of the secret key it will be difficult to decrypt the key because the Shamir key is converted into the hash byte using hash algorithm. So it provides more security to the system.

II. LITERATURE REVIEW

ZhenWang, Mark Karpovsky, Life Fellow, IEEE, and Lake Bu[1] have proposed a robust Shamir's secret sharing using error detection codes to detect cheating and malicious attacks .Adi Shamir[2] has present a method for sharing the Shamir secret key into the equivalent administrators.

Amos Beimel[3] had done a survey on secret-sharing schemes, In that paper they have discussed the most important constructions of secret-sharing schemes in particulate they explained the connections between secret-sharingschemes.

Lein Harn[4] has introduce a proposed system used the shares generated by the dealer to reconstruct the secret and, at the same time, to detect and identify cheaters.

T.-C. Wu1and T.-S[5] has present a method to enforce the security of any threshold method with the ability to detect cheating and identify cheaters.

P. Luo, A.-L. Lin, Z. Wang, and M. Karpovsky[6] has present a hardware implementation of reliable and secure

Shamir's secret sharing scheme.

Toshinori Araki[7] have proposed a (k, n) threshold secret sharing scheme that is capable of detecting the fact of cheating in the system from n - 1 or less colluding participants.

III. NEED OF THE PROJECT

Due to the increasing reliance on computer systems and the Internet in most societies, wireless networks such as Bluetooth and Wi-Fi and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things computer security is becoming more and more important. Shamir Algorithm provides excellent security but it has a security flaw. It cannot detect which key was entered incorrectly. This provides attackers a way to exploit and find new partial keys. We needed a way to fix this exploit.

IV. EXISTING SYSTEM

In the existing system the author used the concept of Shamir secret sharing created by Adi Shamir . It is a form

of secret sharing, where a secret key is divided into parts, giving each member its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all member to combine together the secret might be impractical, and therefore sometimes the threshold method is used where any k of the parts are sufficient to reconstruct the original secret key.

Due to this system there are many possible keys and hence brute-force attack using nominal calculations can lead to generating keys that can work.

V. PROBLEM STATEMENT

For mutually authenticating two parties to each other, we want a protocol that will also output session key that can be used to encrypt and protect the integrity of future communications between those two parties.

Some times as per Shamir algorithm a normal modification in key can give another correct key. If a traitor modifies the partial key in order to derive a new key a warning message should be displayed.

VI. SYSTEM OVERVIEW

The proposed system has following stages:
1. Input stage
2. Encryption
3. Decryption
4. Final stage

1. INPUT STAGE:

Input credentials and upload file.

2. ENCRYPTION:

File is encrypted using the password. Shamir Algorithm segregates the password. Hash algorithm creates hash bytes for the segregated password. Hash bytes are appended to the secret keys and display the keys to the user.

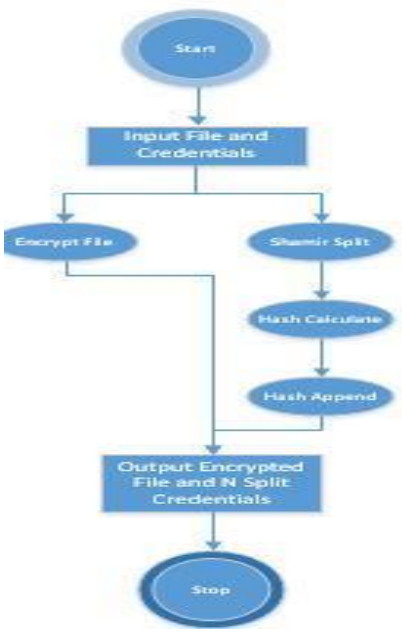

Fig.1 Encryption

3. DECRYPTION:

When there is a need to decrypt the file, K number of the passwords and encrypted file is uploaded. Each password is split to separate hash bytes and the hash for each password is calculated. If the hash equals the hash which is calculated again for their respective password, the password is not tampered.

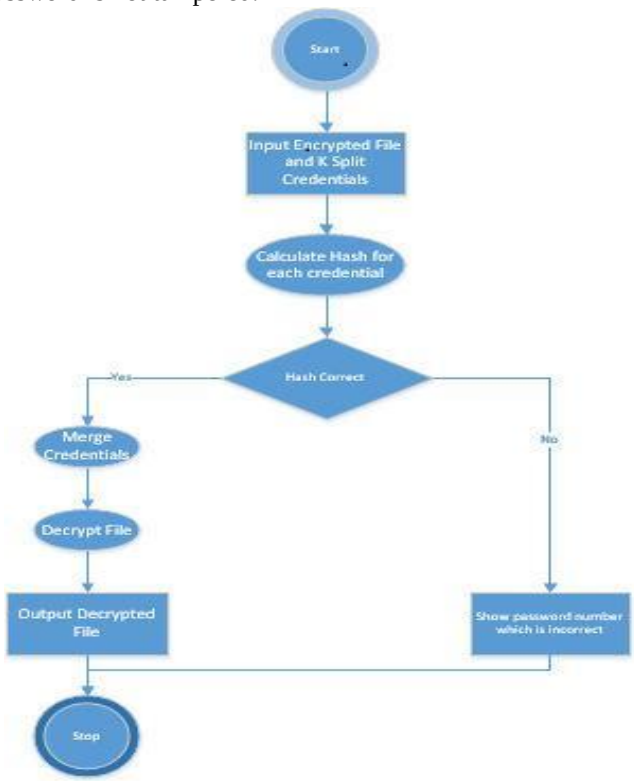

Fig. 2 Decryption

FINAL STAGE:

Shamir algorithm is then used to regenerate the original password which can be used to decrypt the file. If even one of the passwords does not match its respective hash, error message is displayed with the password number which has been tampered.

VII .MATHEMATICAL DEFINITION

The goal is to divide secret (e.g., safe combination) into pieces of data in such a way that

1. Knowledge of any k or more S_i pieces makes S easily computable.
2. Knowledge of any k-1 or fewer S_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

Shamir's secret-sharing scheme

The essential idea of Adi Shamir's threshold method is that 2 points are sufficient to define a line, 3 points are sufficient to define parabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynomial of degree k-1.Suppose we want to use a (k,n) threshold method to share our secret S, without loss of generality assumed to be an element in finite field F of size P where 0<k<=n<P;S<P and P is a prime number.

- Choose at random k-1 positive integers $a_1,...,a_{k-1}$ with $a_i<P$, and let $a_0=S$. Build the polynomial $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\mathbf{\ldots+a}_{k-1}x^{k-1}$.
- Let us construct any n points out of it, for instance set **i=1,…,n** to retrieve (i,f(i)). Every participant is given a point (an integer input to the polynomial, and the corresponding integer output).
- Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

VIII. CONCLUSION

In this paper, we described a cheater detection and identification methodology for Shamir's secret sharing scheme using Hash algorithm. The combination of hash and modified Shamir provides higher levels of security to the information being transmitted. We analyzed the security level of the proposed schemes under different cheating models to test the security level of the proposed schemes. Results shows that the proposed method can increase the security level of the system and protect the system against strong cheaters.

REFERENCES

[1] ZhenWang, Mark Karpovsky, Life Fellow, IEEE, and Lake Bu "Design of Reliable and Secure Devices Realizing Shamir's Secret Sharing" IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 8, AUGUST 2016 2443

[2] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[3] A. Beimel, "Secret-sharing schemes: A survey," in Proc. 3rd Int.Workshop Coding Cryptol., 2011, vol. 6639, pp. 11–46.

[4] Y.-X. Liu, L. Harn, C.-N. Yang, and Y.-Q. Zhang, "Efficient (n, t, n) secret sharing schemes," J. Syst. Softw., vol. 85, no. 6, pp. 1325– 1332, 2012.

[5] T.-C. Wu and T.-S. Wu, "Cheating detection and cheater identification in secret sharing schemes," IEE Proc. Comput. Digital Techn.,vol. 142, no. 5, pp. 367–369, Sep. 1995

[6] P. Luo, A.-L. Lin, Z. Wang, and M. Karpovsky, "Hardware imple-mentation of reliable and secure Shamir's secret sharing scheme," in Proc. 15th IEEE Int. Symp. High Assurance Syst. Eng., 2014, pp.193–200.

[7] T. Araki, "Efficient (k, n) threshold secret sharing schemes secure against cheating from n - 1 cheaters," in Proc. 12th AustralasianConf. Inf. Security Privacy, 2007, pp. 133–142.