IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

POLYGRAM SUBSTITUTION IN DETECTION AND IDENTIFICATION OF CHEATERS IN SECREATE SHARING SCHEME

[1]Prof Poonam Yadav, [2]Prof Priyanshi Mulwani
[1]Assistant Professor, [2]Assistant Professor
[1]Scool of Applied Science, computer Science Department,
[1]REVA University, Bangalore, India

ABSTRACT

In the Polygram substitution technique, one block of alphabets is replaced by another block. The model is proposed for computationally secure online secret sharing, which allows dynamic modification of the secret and addition of participants without the need to secretly distribute the new shares to the current participants. The security of the method is based on the intractability of factoring. This can be achieved by a simple graphical masking method that includes two phases: Encryption of the individual secrets and sharing of the data. The generation of the shares is done by a simple masking technique using Polygram substitution, and the reconstruction can be done by a simple unmasking of the qualified shares. The generated shares are encrypted and each encrypted share contains partial secret information, which leads to additional protection of secret data on the Internet. Moreover, we achieve efficient recovery of the original secret data.

KEYWORDS

Polygram substitution, security, secret sharing, polynomial equation.

I.INTRODUCTION

Although the need for computer security has always existed, the paradigm itself has shifted in recent years with the dramatic changes in computer technology itself. The concern for data security shifted from protecting system resources to protecting access to files and data. Technologies such as user authentication, data encryption, and security policies have been introduced. Secret sharing is a fundamental notion of secure cryptographic design. An unqualified subset of participants is unable to recover the secret even if all their shares are used. In perfect secret sharing systems, participants should have no advantage over outsiders. In secret sharing, secret sharing refers to a method of distributing a secret among a group of participants, each of whom is assigned a share of the secret. The secret can be reconstructed only if a sufficient number of shares are combined; individual shares are of no use by themselves. Such a scheme is called a (k, n)-threshold method (sometimes also called a (k-n-threshold-method). The proposed scheme introduces Polygram substitution for data so that the safety bound is more stringent. In the Polygram substitution technique, one block of letters is replaced by another block. The new model is proposed for computationally secure online secret sharing, which allows dynamic modification of the secret and addition of participants without the need to secretly distribute the new shares to the current participants. The security of the method is based on the insolvability of the factorization. This can be achieved by a simple graphical masking method that includes two phases: Encryption of the individual secrets and sharing of the data. The generation of the shares is done by a simple masking technique using Polygram substitution, and the reconstruction can be done by simple unmasking of the qualified shares. The generated shares are encrypted and each encrypted share contains partial secret information, which leads to additional protection of secret data on the Internet. Moreover, we achieve efficient recovery of the original secret data.

II. LITERATURE REVIEW

In a (t, n) secret sharing scheme, a secret s is divided into n shares and shared by a trusted trader to a group of n shareholders, such that t or more than t shares are able to reconstruct this secret; however, less than t shares cannot learn any information about the secret. When shareholders present their shares at the stage of reconstructing the secret, dishonest shareholders (i.e., fraudsters) can always derive the secret solely by presenting fake shares, so the other honest shareholders receive nothing but a fake secret. Detection and identification of fraudsters is very important to achieve fair reconstruction of a secret. Suppose there are more than t shareholders involved in the reconstruction of the secret. Since there are more than t shares (i.e., only t shares are needed) to reconstruct the secret, the redundant shares can be used for fraudster detection and identification. The proposed method uses the trader-generated shares to reconstruct the secret and simultaneously detect and identify impostors. The method is based on sharing secrets with thresholds. It is an extension of Shamir's scheme. In Shamir's scheme, one can create shares but at the time of combination, it is not guaranteed that one can reconstruct the original secret because one cannot find out the cheater in the secret sharing scheme but in the proposed scheme, one can find out the cheater using a single algorithm. In CRT (Chinese reminder method), this method uses threshold secret sharing. The cheater can be detected, but the limitation of this algorithm is when the situation in which (c > t). This means that the cheaters are larger than the threshold so that one cannot find the cheater, but in the proposed scheme, the redundant portion (j) which is used to identify and detect the cheater, and the condition of the proposed scheme is (t <j<n).

In linear secrecy, the impostor is also determined using a threshold. But in this method, the share is divided into two parts, one of which is used for verification and the other for sharing the secret. Linear secret sharing has the limitation that one cannot construct multiple secrets simultaneously. This scheme is more complicated and the time complexity of this algorithm is 0(n2). But the scheme proposed in this paper provides a single share used for sharing and the time complexity of the algorithm is 0(j!). One of the best performing methods is the one-way hash function. This creates in some integer value. Set the sharing using the hash function. It requires MD5. It provides good security but this scheme is complicated because it requires many mathematical operations, this scheme is also costly. The detection and identification under three attacks shows that the detectability of our proposed scheme gradually decreases from type 1 to type 3 for j = 5 participants. Similarly, it shows that the identification of fraudsters in the proposed scheme gradually decreases from type 1 to type 3 for participant's j = 9. The decrease in the detectability and identification of impostors from type 1 to type 3 is caused by the increase in the attackers' capabilities from type 1 to type 3. The figure illustrates that the detectability of the proposed system is proportional to the number of participants. Similarly, the figure illustrates that the identification of fraudsters in our proposed system is proportional to the number of participants. The proposed model is for computationally secure online secret sharing, which allows the secret to be dynamically changed and participants to be added without the need to secretly distribute new shares to the current participants. The security of the method is based on the insolvability of the factorization. This can be achieved by a simple graphical masking method that involves two phases: Encryption of individual secrets and generation of shares and exchange over the Internet. The generation of shares is done by a simple masking technique using Polygram substitution, and the reconstruction can be done by a simple unmasking of the qualified share set. The generated shares are encrypted and each encrypted share contains partial secret information, which results in additional protection of secret data on the Internet. Moreover, we achieve efficient recovery of the original secret data.

III. PROBLEM DEFINITION

From the literature survey, there is much room for improvement in secret sharing. Designing a more secure secret sharing scheme is a challenging task. The computational complexity of the given scheme is extremely low because it uses a simple masking method, replaces PolyGram with a simple algorithm in generating the clearance, and the reconstruction can be performed by a simple unmasking technique. This makes it effective for security as it is also a great challenge. In our scheme, we proposed to divide each information into several shares. These different shares are to be transmitted over multiple disjoint paths between the communicating pairs of nodes. We proposed to transmit these shares at different times, if possible. At the receiving end, the original information is reconstructed by combining the received shares. Since the method is an extension of Shamir's (t, n)- SS method, the detection and identification of impostors is very important to achieve a fair reconstruction of the secret. Assuming that there are more than t shares (i.e., only t shares are needed) to reconstruct the secret, the redundant shares (j shares) can be used to detect and identify impostors. With this in mind, this paper describes the approach and proposal for cheater detection and identification. A unique feature of the proposed scheme is that the same share that is used to reconstruct the secret is also used to detect and identify the fraudsters. The scheme uses the trader-generated shares to reconstruct the secret while detecting and identifying the fraudsters.

IV. ARCHITECTURE OF PROPOSED SYSTEM

In this scheme, we aim to develop an Internet-based messaging application that implements a novel secret sharing scheme that uses a simple masking method with a simple substitution of Polygram for generating shares, and the reconstruction can be done by unmasking the predefined minimum number of shares. Although this work is not related to the traditional client-server model, the role of the server here is simply to store data in a secure manner. As in the system architecture diagram, client-side operations consist of sender-side and receiver-side operations, but since both operations require a common graphical user interface, they are combined in the system. Therefore, they are combined in the system architecture diagram.

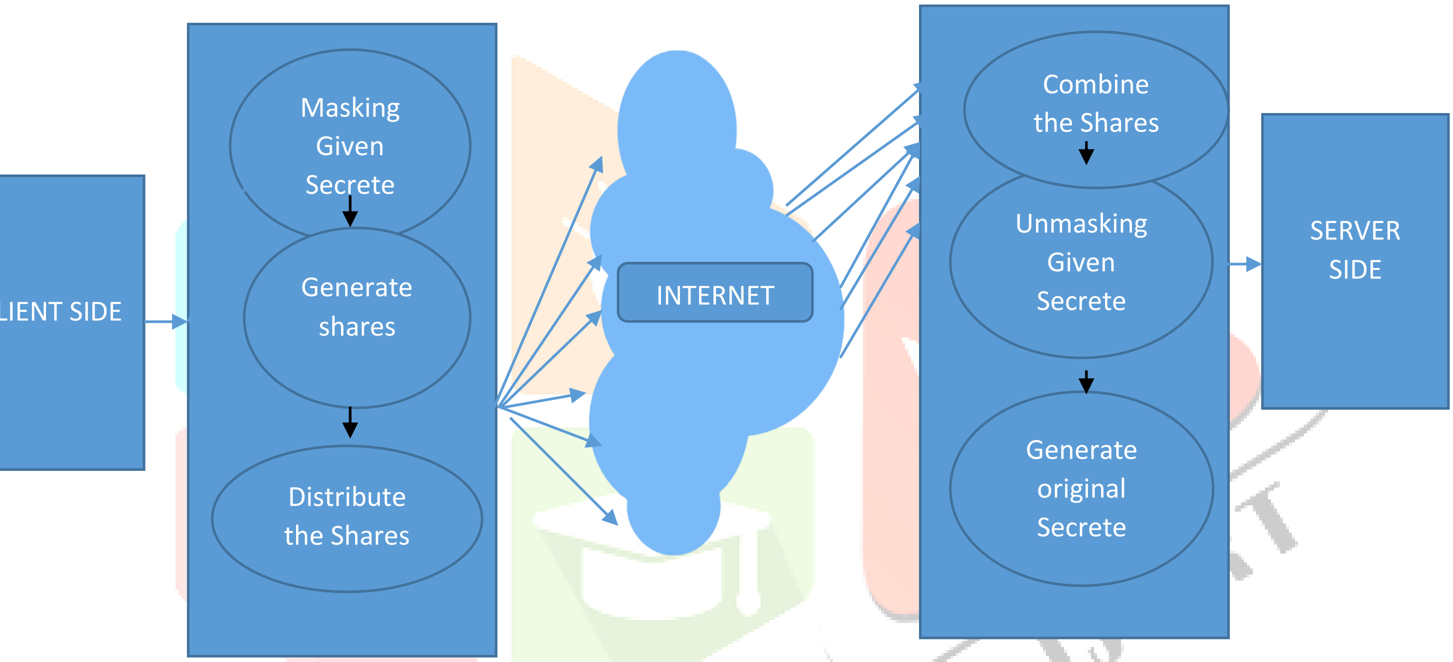

Fig: System Architecture

The Proposed System architecture shown above basically consist of three major blocks: (1) Client side Operations, (2) Internet, and (3) Server Side Operations.

A. Client Side Operations

The client can be both sender and receiver. In either case, both sender and receiver use the graphical user interface to access the application according to their requirements. The block diagram shown in Fig: System Architecture applies only to operations on the sender side. 1. Each ellipsoid shows the function and operation on the sender side. 2. They work from top to bottom, from masking to release. 3. Multiple arrows pointing outward mean that data from the sender side is sent over different channels to ensure secure transmission.

The block diagram in Fig: System Architecture shows the application for the operations on the receiver side, which works almost opposite to the sender side, as the received message goes through these operations to regenerate the original message, and multiple incoming arrows denote incoming data from multiple channels.

B. Internet

The Internet block in the system architecture indicates that all data is transmitted over a wide area network to reach the destination, and therefore all operations are performed to safely transmit the data over multiple channels throughout the journey.

C. Server-side operations

The server, in our case multiple servers, simulates multiple channels because the data arriving from the clients is randomly stored on the servers, which makes it difficult to track the flow. Also, the server serves as a repository for all records, history, transfer, and access to old data.

V. WORKING OF THE PROPOSED SYSTEM

The operation of our proposed system is mainly divided into two phases: (I) Secret Sharing Phase, (II) Secret Data Reconstruction or Recovery Phase.

I. Secret Sharing Phase

In these two phases, we need to generate a mask by replacing Polygram with the following algorithm

POLYGRAM SUBSTITUTION METHOD

a. MASKING Process

1) Take the sample text.

2) Reverse the characters in the given text.

3) Replace the reversed character according to the key generation algorithm. The difference of the key to the character "a" is calculated and then added to the reversed character.

4) The ASCII value of the key's character is added to the corresponding replaced character.

5) The ASCII value of the algorithm is added.

6) After adding the ASCII value of all values of the given text, the resulting text is an encrypted message.

7) Convert the corresponding ASCII value to its equivalent binary value.

8) Transposition takes place in each character after the entire process is complete, i.e., one bit is either MSB shifted or changed, increasing security. As the MSB is taken, the alternate sign is changed.

9) Finally, the decimal values of each updated character in the given text are determined

b. Creation of a Shares

In this phase, a trusted entity, usually the share creator, is provided with the necessary input to create a share for each shareholder. It requires the poultry information: The secret can be as small as an encryption key or vault combination, or as large as a database. Without losing generality, the secret information is usually represented as integers.

c. Distribution of shares

In the share distribution phase, the shares produced in the first phase are delivered to the shareholders, but there are methods to distribute the shares through the public Internet.

II. secret data reconstruction or recovery phase.

a. Combine shares

Steps in combining shares

- Enter the qualified threshold (t).
- Enter the number of participants (n).
- Select the required qualified quantity.

Proper selection of the qualified quantity results in a secret

b. Detection and identification of cheaters

Method for detecting cheaters in Shamir's (t, n)- SS scheme, an interpolating polynomial of degree t - 1 can be uniquely reconstructed based on t shares. Thus, if there are more than t shares and there is no impostor share, a consistent polynomial should be reconstructed for all combinations of t shares. Cheater detection is done by discovering inconsistent polynomials (or secrets) among all reconstructed secrets. However, fraudsters can work together to determine their fake shares to deceive honest shareholders into believing that a fake secret is a real secret

c. Unmasking process

1) The ASCII values of each updated character in the given text are converted into binary format.

2) After the process is completed, each character is transposed, i.e., shifted or changed by one bit MSB. The sign bit is changed when the MSB changes its value.

3) Subtract the value ASCII from all values of the given text, the resulting text is a decrypted message.

4) Subtract the corresponding ASCII value of the character of the key from the corresponding character of the transposed plaintext.

5) Transposition takes place in each character after the whole process is completed, i.e. one bit is shifted or changed either LSB or MSB, the final result is a binary value.

6) Finally, the decimal values of each updated binary value in the given text are taken and printed.

7) Then the character value generated by the values of ASCII is reversed again.

8) The decrypted message is generated.

VI. CONCLUSION

With the implementation of the secret sharing algorithm based on the extension of the Shamir scheme, the encrypted secret can be broken into shares and sent to the recipient. With this level of security, the original data can be recovered even if some shares are lost during transmission, sin ce the data is scattered over each share and can be recovered at the receiver. An advantage of this scheme is that even if an intruder gains access to one or more shares (less than the threshold), he is not able to regenerate the original message. We have presented an efficient approach to secret sharing with minimal computational overhead. Security is enhanced by introducing masking and unmasking techniques using the Polygram substitution technique. In our future efforts, the mean value of each share can be computed and added to each share so that the identification and detection of intruders in each share can be performed more effectively.

REFERENCES:

1. Josef Pieprzyk and Xian-Mo Zhang, Cheating Prevention in Linear Secret Sharing, 1983 2. Ehud d. Karnin, jonathan w. Greene, martin e. Hellman, "On secret sharing systems" IEEE transactions on information theory, vol. It-29, no. 1, January 1983.

3. TalalAlkharobi, "Sharing secrets A better protection even from shareholders."

4. Donald Davies, "A brief history of cryptography," Information Security Technical Report. Vol. 2, No. 2 (1997) 14-17.

5. Martin Tompa, "How to share secrets with others," Springer Verlag, 1998.

6. E.F. Brickell, D.R. Stinson, "The detection of impostors in threshold schemes," Springer-Verlag, 1998.

7. K.-J. Tan, H.-W. Zhu, S.-J. Gu, "Cheater identification in (t,n) threshold scheme," Computer Communications 22 (1999) 762-765.

8. Ren-Junn Hwang, Wei-Bin Lee, Chin-Chen Chang, "A concept of designing cheater identification methods for secret Sharing" The Journal of Systems and Software 46 (1999) 7 - 11.M. Frei, "Secure Sharing", available: http://www.cs.cornell.edu/Courses/cs513/2000SP/SecretSharing.html,accessed September 2003.

9. PKI Security, Data Interchange Plc, September 2005.

10. Wakaha Ogata, Kaoru Kurosawa, Douglas R. Stinson, "Optimum Secret Sharing Scheme Secure against Cheating," July 2005.

11. Michael Ganley, "Introduction - Cryptography," Information Security Technical Report II (2006) 67.

12. David Andrew Schultz, "Mobile proactive secret sharing," PhD dissertation, Massachusetts Institute of Technology, January 2007

13. Rong Zhao, Jian-jie Zhao, Fang Dai, Feng-qun Zhao, "A new image secret sharing scheme to identify cheaters," Computer Standards & Interfaces 31 (2009) 252-257.

14. LeinHarn, Changlu Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme", Des. Codes Cryptogaphy. DOI 10.1007/s10623-008-9265-8, 2009.

15. Chor B, Goldwasser S, Micali S, Awerbuch B, "Verifiable secret sharing and achieving simultaneity in the presence of

faults", Proceeding of 26th IEEE Symposium on Foundations of Computer Science, 1985, pp.383-395

16. Feldman A, "A practical scheme for non interactive verifiable secret sharing", Proceedings of 28th IEEE symposium on Foundations of Computer Science, 1987, pp.427-437

17. Pedersen T P, "Non-interactive and information theoretic secure verifiable secret sharing", CRYPTO'91, 1991, pp.129-139.
9. W.-A,Jackson, K.M.Martin, C.M.O'keefe, "On sharing many secrets", Asiacrypt'94, 1994, pp.42- 54

18 J. He, E. Dawson, "Multistage secret sharing based on one-way function," Electronics Letters, 1994, 30(19), pp. 1591-1592

19 J. He, E. Dawson, "Multi-secret sharing scheme based on one-way function," Electronics Letters, 1995, 31(2), pp.93-95
20 L. Harn. "Commentary: multistage secret sharing based on one-way function." Electronics Letters, 31(4):262, 1995

21 H.-Y.Chien, J.-K.Jan, Y.-M.Tseng, "A practical (t,n) multi-secret sharing scheme," IEICE Transactions on Fundamentals, 2000, E83-(12), pp.2672-2675

22 Chou-Chen Yang, Ting-Yi Chang, Min-Shiang Hwang, "A (t,n) multi-secret sharing scheme", Applied Mathematics and Computation, 2004, 151, pp. 483-490

23 Liao-jun Pang,Yu-Min Wang, "A new (t,n) multisecret sharing scheme based on Shamir's secret sharing", Applied Mathematics and Computation, 2005, 167, pp. 840-848
24 T.ElGama, "A public-key cryptosystem and a signature scheme based on discrete alogarithms", IEEE Transactions on Information Theory, 1985, IF -31(July), pp.469-472
25. Ultra Secured and Authentic Key Distribution Protocol using a Novel Secret Sharing Technique, International Journal of Computer Applications (0975 - 8887) Volume 19- No.7, April 2011.
26. C.-C. Chen and W.-Y. Fu, -A geometry-based secret image sharing approach,‖ Journal of Information Science and Engineering, vol. 24, no. 5, pp. 1567-1577, 2008
27. Khobragade, P. V., and Nilesh Uke. "Cogent Sharing of Covert File Using Audio Cryptographic Scheme.", IJAIS, Volume 1- No.8, April 2012.