



SECRET SHARING FOR DIGITAL DATA SECURITY USING SHARED KEY CRYPTOGRAPHY: REVIEW

Neha Yadav¹, Chander Diwaker²
Department of Computer Engineering
U.I.E.T., Kurukshetra University Kurukshetra
Kurukshetra, Haryana
INDIA

Abstract: Information is one among the most necessary assets for any organization to protect against any sort of harm or theft. Cryptography proposes that the art of encoding and decoding digital information using mathematical techniques. The ciphered information will solely be deciphered by someone who has the mechanism for that. However if the initial ciphered information or ciphering key gets broken then the initial information will never be recovered. Presently, the Secret sharing scheme for digital information based on Shamir's threshold cryptography method to share the information among various users acts the hero in such conditions. The idea is developed in the form of a web application where one user presents the information and breaks it into shares after ciphering it through the proposed bit conversion method. The shares are disseminated among various users relying upon who can collectively view the initial information. Now these users group can view information only if they have the minimum required no. of shares.

Keywords: Cryptography, Secret sharing, Masking, Cipher, Decipher

I. Introduction

With the rise in use of Internet and different types of digital data communication, security of digital data is changing into more and more vital. The science of securing information by changing it (encoding it) into a not justifiable format and later changing over it back (decoding) to initial form is termed cryptography [1]. Just the individuals who have the decoding algorithm can decipher the encoded data. But sometimes the messages secured by some form of encryption can be deciphered by cryptanalysis. This is also termed as code-breaking, but most modern cryptography mechanisms are unbreakable. Cryptography is used in various applications to protect e-mail messages, network data during transmission, credit card information, and other important information etc.

A. Cryptography: Cryptography implies the specialty of encoding and decoding digital data utilizing scientific strategies. The ciphered information must be deciphered by someone who has the framework for that [2]. Cryptography permits us to store delicate information or transmit it crosswise over in secure networks (like the Internet) with the goal that it can't be perused by any interloper. Cryptanalysis implies examining and breaking secure communication. Traditional cryptanalysis incorporates a fascinating mix of pattern discovering, tolerance, application of mathematical mentioned concisely here.

A.1. Symmetric Key Cryptography: This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Because only single key is used at both ends so it is called symmetric encryption. This mechanism has a problem that a single key is used for encryption and decryption both, so if the intruder somehow gets the key then security is compromised. Some common symmetric cryptography mechanisms are :

a) DES (Data encryption standard): DES inputs a fixed-length string of plain text in the form of bits and converts it into another cipher text bit-string of the same length using a series of complicated operations.

b) AES (Advanced encryption standard): AES is based on a principle mechanism which is a combination of both substitution and permutation, and works very fast in both software and hardware. AES does not use a Feistel network like its predecessor DES. This technique is a variant of Rijndael algorithm, which has a fixed block size of 128 bits, and works with a key of 128, 192, or 256 bits size.

c) SKC (Shared Key Cryptography):

SKC is a technique in which a mask generated through a masking algorithm to form the shares and then the same mask used to regenerate the original data. So it comes under the symmetric class of encryption scheme.

A.2. Asymmetric Key Cryptography: This technique allows a secure communication to take place between receiver and sender over insecure communication channel. This technique involves two key cryptosystem in which the sender and receiver use different keys to encrypt and decrypt respectively. This technique is termed as symmetric encryption as a pair of keys is applied here at both ends. In this method, both sender and receiver have a private key and a public key. The private key is kept secret while the public key is shared with all those whom

you are interacting with. If X is sender for a message to Y, then X will encrypt the message with Y's public key and Y can easily decrypt the message using the private key that he has. The RSA asymmetric cryptography mechanism is detailed below.

a) **RSA**(Ron Rivest, Adi Shamir and Leonard Adleman) : A user of RSA creates a public key based on two large prime numbers and then publishes the key along with an auxiliary value. The secrecy of prime numbers has to be maintained. Anyone who gets the public key can decrypt the message. But if the public key is comparatively large enough, then only someone who knows the related prime numbers can possibly decode the message. This breaching of RSA encryption is termed as RSA problem.

B. Limitations of Traditional Cryptography:

However, a common weakness of this technique is that an entire secret data is kept in single medium. The secret data cannot be revealed if the medium or key is lost or corrupted. This is termed as single point failure. The sender encrypts a secret image using the key and then transmits to the receiver. At the receiver end, receiver may receive correct data or data may be corrupted during transmission. In this situation, using correct key reconstruction will be lossless for correct received data otherwise reconstruction will not be possible. So the main challenges which could not be overcome by previous researchers were- preventing a single point failure on loss of encryption key, flexibility to work with all types of digital data, preferential user key distribution and efficiency (low complexity).

II. Shared Key Cryptography

SKC is a technique in which a mask generated through a masking algorithm to form the shares and then the same mask used to regenerate the original data. The steps used for SKC are defined below:

Secret hiding Algorithm (SHA)

SHA is a novel secret sharing scheme which splits the ciphered data into shares. The two main secret sharing algorithms used are Shamir's[3] and Blakley's[4] secret sharing algorithms. They are discussed below:

1. The first scheme was Threshold Secret sharing scheme proposed by Shamir [3]. This method is based on a polynomial of degree (k-1) and has a set of k points that lied on the polynomial.

$$f(x)=d_0+d_1x_1+d_2x_2+d_3x_3 + \dots + d_{k-1}x_{k-1} \pmod{p}$$

where, d_0 is the secret and p is a prime number and the remaining coefficients picked at random.

This method first creates a polynomial of degree (k-1). Next it finds n points on the curve and allocates a point to each of the participants. There is sufficient information to fit an $(k-1)^{th}$ degree polynomial after at least k out of the n participants have revealed their points. Then Lagrange Interpolation can easily be applied to find the secret value d_0 .

2. In Blakley's scheme, two non parallel lines in the same plane intersect at a single point. This means n non parallel lines in $n-1$ dimensional hyperplanes have intersect at 1 point. One of the coordinate of the point of intersection of the two non parallel lines is used to encode the secret. If we use all the coordinates to encode the secret then there is a risk involved that the insider can get information about the secret since he knows that the point of intersection to decode the secret lies is on the same plane as it is. But now, the insider has no more information than the outsider. Each client knows about a single hyperplane and the full information can only be recovered by finding planes' point of intersection.

In 2014, Yeshvanta rao[5] presented a secret sharing mechanism based on Shamir's scheme. The author presented it as a client server application. But the research mainly worked for audio files and had a single point failure in the form of encryption key lost. In the same year, Apoorva [1] implemented secret sharing on all types of digital data but failed to provide any security to the shares by any form of encryption method. Again the method used encryption key to encrypt data, so any damage or loss of encryption key resulted in single point failure. YouliangTian [6] implemented secret sharing based on fairness of secret distribution among all users. The method was based on polynomial interpolation and verification of the polynomial solution to detect cheaters in each round. The complexity was high which impacted efficiency of method.

III. Review of Literature

The two main schemes which form the basis of almost every secret sharing technique – Shamir's secret sharing and Blakley secret sharing scheme [5]. Many other secret sharing techniques developed since then have used these as their principle and formulated new methods or applications.

Shamir [3] created a threshold cryptographic method where a data D was divided into n pieces in such a way that it could easily be reconstructed from any k pieces where $k \leq n$. The knowledge of less than k pieces revealed absolutely no information about D . This technique brought into existence some robust key management schemes to be used in cryptographic systems that could function securely without failure even when half the pieces somehow got destroyed and any form of theft or security breach exposed all but one of the remaining pieces. *Blakley* [4] proposed the importance of cryptographic keys in DES or RSA encryption schemes. The author commented on schemes like DES cryptosystem and stated that certain cryptographic keys, for e.g a number which computed the secret decoding exponent in an RSA public key cryptography technique or the system master key and certain other keys in it, actually presented a dilemma. There were chances that one might go astray if a

relatively large number of copies were distributed. On the contrary, creating too few copies had the risk that they might all be destroyed. He discussed about what the non-volatile copies of the keys, or non-volatile pieces of information from which the keys were reconstructed, be guarded against. *Hai et al.* [7] presented two matrices that could be used for the scheme proposed by Blakley's system. The elements in these matrices increased in a rather slower way as compared to the Vandermonde matrix which was employed in Shamir's scheme. Furthermore, the authors formulated the problem of optimal matrix. They traced the lower bound and upper bounds of the minimal maximized element for $k=2$ and for given k respectively. The author implemented the Blakley's secret sharing scheme and proposed two new matrices for its implementation. The computation of inverse matrix over the field $GF(p)$ was easier because the corresponding square matrix had the determinant value 1. The multiplication operation under mod p field was also not required for the generation of these matrices. These matrices required lesser resources like computation and storage capacity as compared to the Vandermonde matrix. *Ssulami* [8] emphasized the importance of secret sharing schemes as they were employed in some very critical applications like e-voting, secure online auctions, sharing and distribution of cryptographic key, information hiding and secure multiparty computation. The research explained some secret sharing popular algorithms like threshold, graphical and visual schemes along with their access structures. Besides, the limitations of the available schemes were also discussed. Additionally, the author proposed the use of Fast Fourier Transform (FFT) algorithm to form a novel threshold secret sharing scheme, to be used for the first time in the field of secret sharing through the proposed research. So, the authors exploited the inherent characteristics of FFT like reversibility, linearity and efficiency. The FFT had time complexity of $O(n \log n)$, and it provided a wider field of complex numbers. The presented scheme was perfect in many senses. The share's size was considerably smaller as compared to the secret and also secure because it depended on providing a solution for the linear system of equations that it has from FFT. So the proposed mechanism combined the merits of the schemes from Shamir and Blakley. *Wankhade and Soni* [2] emphasized the importance of information security in diplomatic and military matters. It was often required that the Information had to be stored or transferred from one place with the risk of being exposed to an opponent or intruder. The proposed method used Rijndael Algorithm to encrypt any data. The main aspect under consideration in this paper was Data security and the need for Data security. Key management was very important for confidentiality. This dealt with the generation, storage and distribution of key. *Kumar and Das* [9] proposed technique using a secure mask generation technique and the masking of original data repeatedly generate shares. The purpose of steganography was to covert communication to hide the existence of a message from an intermediate attacker. This paper discussed about pure steganographic technique, which did not require prior exchange of data like shared-keys. This proposed algorithm had advantages like minimal change was permitted in Stego image and the naked eyes could not catch any difference due to high rate of imperceptibility achieved. The proposed algorithm did not need any secret key. The proposed security technique used both shared cryptographic technique and steganographic technique, provides high security to exchange of confidential text data over public channel in a safe way. *Ghule and Deshmukh* [10] implemented a scheme for images using essentially two techniques: Shamir's scheme and the Matrix Method. The method allowed the colored secret image to be reconstructed from the threshold K shares. But the knowledge of any $(k-1)$ or fewer image shares did not reveal the secret image. The size of image shares and the size of secret image were same. The implemented scheme was at par with any other secret sharing scheme according to the security and accuracy conditions. *Rao et al.* [11] used Pell's equation with Jacobi symbol and proposed a dynamic threshold multi-secret sharing scheme which was verifiable. Some secret was converted into shares and the secret was protected by distributing the shares among many participants. The system ensures that only an authorized group of participants had the capacity to reconstruct the secret back. The scheme allowed the dealer to periodically publish some of the information, so the secret changed periodically. The participants could also verify the information which they had received. Each participant held only one permanent, private secret, and some of them used it during different time periods to reconstruct the corresponding shared secrets without revealing their own private information. This scheme renewed some public information, so the old information was irrelevant now for the next secret. This paper used Pell's equation with Jacobi symbol in algorithms for key generation, encryption and decryption. *Tian et al.* [6] evaluated the efficiency of secret reconstruction in a (t, n) secret sharing scheme. The author initially defined the fair notion of secret sharing in a probabilistic way. The proposed scheme was a fair (t, n) secret sharing scheme. The security and fairness of proposed scheme was tested against three different attack types. The basic model of secret sharing (Shamir's scheme) and the Dov Gordon's approach for fairness formed the basis of proposed scheme. The efficiency of the proposed scheme was confirmed using theoretical analysis. The creation of new distribution and then reconstruction protocols confirmed achieving the fairness in a secret sharing. In this scheme, the cheaters could be detected in any round by the polynomial interpolation and its verification in each round. The performance was evaluated experimentally and the results confirmed that the proposed method was more efficient than the basic schemes employed. *Yeshwantrao et al.* [5] presented scenario where many audio files were needed to be transmitted over internet for various important purposes. Most of the available cryptographic methods lead to chance of key compromise and single point failure. To overcome this problem shared cryptography scheme became best solution. In shared cryptography scheme, a shared secret was a small piece of secret data, known

only to the parties involved in a secure communication channel. A new model was proposed for computationally secure online secret sharing, which allowed dynamically changing the secret and adding participants, without having to redistribute new shares secretly to the current participants. The security of the scheme could be achieved by using simple graphical masking method, which included two phases Sharing data and Encryption of each share. Share generation was performed by logical AND and reconstruction can be done by performing logical OR operation on the qualified set of qualified shares. Not only the generated shares were compressed but also got encrypted and each encrypted share contained partial secret information that lead to added protection to the secret data and reduced bandwidth requirement for transmission over internet. In addition to these, efficient recovery of original secret audio data achieved. *Apoorva et al.* [1] presented a thoroughly new idea to protect very crucial information from any kind of theft or piracy. The idea of breaking the information into shares and storing the shares separately, then doing the same to the cryptography key also provides a never before level of security. The information could be retrieved from any minimum specified no. of shares and individual share is not of any use. So piracy could be prevented and theft of information made almost impossible.

IV. Conclusion

Secrecy of data is a requirement for almost every single enterprise who is managing its data digitally. The matter becomes even more important when it relates to some intelligence agency. It is quite common that some data should be accessible to a user or a group of users. Here a web interface conceptualized to provide a platform where a secret is accessible only if a particular minimum no. of keys is available. A person may have all the required keys or the keys might be shared between a group. This methodology will certainly provide immense security and global availability of any such secret data to the intended users. In future, the researchers can work on the masking scheme to reduce the size of shares created after masking. Also the proposed bit conversion scheme can be used for encrypting the source data in many military and public network applications.

REFERENCES

- [1] Arya Apoorva, Parikshit Singla, "A Review of Information Sharing Through Shared Key Cryptography", International Journal of Research in Engineering Technology and Management, pp: 1-6, June-2014.
- [2] Mukund S. Wankhade and Pravin D. Soni, "Advanced Cryptanalytic Algorithm for Data Security", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 3, pp: 321-324, March 2013.
- [3] Adi Shamir, "How to Share a Secret?", International Journal of Communications of the Association for Computing Machinery (ACM), Vol. 22, 1979, pp: 612-613, 1979.
- [4] G.R. Blakley, "Safeguarding cryptographic keys", in the proceedings of National Computer Conference, Vol. 48, pp: 313-317, June 1979.
- [5] Sagar A. Yeshwantrao, Prof. Vilas J. Jadhav, Prof. Pravin S. Rahate, "Shared Cryptographic Scheme with Efficient data Recovery and Compression for Audio Secret Sharing", IJETAE, Vol.4, pp: 408-414, Issue 2, Feb 2014.
- [6] Youliang Tian, Jianfeng Ma, Changgen Peng and Qi Jiang, "Fair (t, n) threshold secret sharing scheme", International Journal of Information Security, Vol. 7, Issue 2, pp: 106-112, June 2013.
- [7] XialiHei, Xiaojiang Du and Binheng Song, "Two Matrices for Blakley's Secret Sharing Scheme", in the proceedings of International Conference on Communication (ICC), pp: 810-814, 2012.
- [8] Abdulraheeb M. Al-Ssulami, "A Novel Threshold Secret Sharing Scheme Using FFT Algorithm", International Journal of Information Security Science, Vol. 2, pp: 19-27, 2013.
- [9] Boina Avinash Kumar, Madhusmita Das, "A Relevant Technique of Hiding Information in an Image Using Shared Cryptography", International Journal of Computer Applications, Vol. 69, pp: 12-19, May 2013.
- [10] Arti G. Ghule, Prashant R. Deshmukh, "Secret Sharing an Effective Approach for Sharing Images", International Journal of Innovative Research and Studies, Vol. 2, Issue 6, pp: 698-709, June 2013.
- [11] M K Rao, K V S R S S Sarma and P S Avadhani, "A Model on Dynamic Threshold Multi-secret Sharing Scheme Using Pell's Equation with Jacobi symbol", in the proceedings of 10th International Conference on Information Technology New Generations (ITNG), pp: 773-776, April 2013.

Acknowledgements

I would like to take the chance of expressing my sincere gratitude to a number of people who accompanied me in the course of my studies and helped shaping this thesis. First and foremost I would like to express my deep sense of gratitude and indebtedness to Mr. Chander Diwaker, Assistant Professor, University Institute of Engineering and Technology (U.I.E.T), Kurukshetra University, Kurukshetra for introducing the present topic and for his inspiring guidance, valuable suggestions and support throughout the work. I am also thankful to Dr. Kulvinder Singh, Head of the department, Computer Engineering, University Institute of Engineering and Technology (U.I.E.T), Kurukshetra University, Kurukshetra for their generous help in various ways for the completion of my dissertation work.