IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Secret Sharing Scheme using Cryptographic Techniques

Pratiksha Patil[1], Nilesh Javre[2], Priyanka Patil[3], Sarang Deshpande[4]

UG Students, Department of Computer Engineering, SSBT's College of Engineering and Technology,

North Maharashtra University, Jalgaon, Maharashtra, India[1, 2, 3, 4]

Abstract: From many years, people were concerned about the secure transmission of data. Among the various cryptography techniques, the Adi Shamir's secret sharing scheme based on La-grange's polynomial is considered as the most secured one. But, it faces the man in middle attack in which an adversary can retrieve the secret even without any valid share. To over-come this drawback, the token generation mechanism is proposed in which each valid share is binded with the public information of all the nodes. The proposed system consists of Adi Shamir's secret sharing scheme based on Lagrange's polynomial along with the concept of Token Generation. Token Generation mechanism involves binding of shares with their respective shareholders. Due to this the intruder will not be able to retrieve the secret if he does not have a valid share. Thus, one can conclude that the proposed system provides better security than the traditional one.

Keywords: Security, secret sharing scheme, public information, token.

I. INTRODUCTION

Secure transmission of data plays a very vital role in today's era. There are various cryptography techniques for such secure transmission. Among the various algorithms and concepts, the Adi Shamir's secret sharing scheme, is the securest one. The Adi Shamir's secret sharing scheme depends on Lagrange's polynomial for dividing the secret into number of shares. There are n shareholders, and a dealer D. The scheme consists of two algorithms:

- With knowledge of any't' or more than't' shares can reconstruct the master secret 's'.
- With knowledge of fewer than't' shares cannot get any information about the master secret's'[1].

People have failed to notice, however, an adversary or intruder may obtain the secret without any valid share. This creates man in middle attack in the existing system. In the Man in Middle Attack, an adversary without any valid share may obtain the secret if there are over't' participants in the secret reconstruction. Therefore to overcome this drawback, the concept of token generation is proposed. Token generation mechanism involves binding of shares with their respective shareholders. Because of this, only the authenticated shareholders can obtain the secret whereas, the intruder will not be able to retrieve the secret, without any valid share.

A. Motivation

The existing Adi Shamir's Secret Sharing Scheme is prone to the Man in Middle Attack, due to which the security of secret or message transmission is not ensured.

The security of transmission of the secret can be ensured by the introduction of a token generation mechanism. Token binds the shares with their valid shareholders. Hence, each shareholder or authenticated node of the group has a token attached with it. Due to this, even if an intruder tries to recover the secret without having a valid share, the intruder will not be able to retrieve the secret. The proposed system involves the traditional Adi Shamir's Secret Sharing Scheme along with the concept of token generation. The token generation mechanism enhances the security of the traditional secret sharing scheme.

II. LITERATURE SURVEY

The content of the paper focuses on the research and contributions of various sources. These include:

[1]The paper describes the basic (t, n) secret sharing scheme and the attack to which it is prone. The share generation and share reconstruction concepts are discussed in detail. The existing secret sharing scheme faces a drawback if an adversary is able to retrieve the secret, even without a valid share. The paper proposed the concept of randomized component which binds the shares with their particular shareholders. Due to this, the adversary is not able to recover the secret as it is not having a valid share and is not binded with the share.

[2]The paper discusses the Adi Shamir's secret sharing scheme in detail. The paper describes how the shares are split at the distributor end and how they are reconstructed at the receiver end. Various cryptographic encryption algorithms are also described in the paper. The concept of Lagrange's polynomial and its use in the Adi Shamir's secret sharing scheme is also discussed in detail.

[3]The paper describes the basic concept of group authentication and secure transmission of secret in a group. It includes a review of Shamir's (t, n) Secret Sharing Scheme. The concept of token generation is discussed in the paper. The paper also describes the share

DOI 10.17148/IJARCCE.2016.54148

generation, token generation, secret reconstruction and group authentication in detail along with the concept of Lagrange's polynomial.

TABLE I Literature Survey

Authors	Description	Limitation
Miao Fuyou, Xiong Yan, Wang Xingfu, and Moaman Badawy	The paper describes the basic (t,n) secret sharing scheme and the attack to which it is prone. The share generation and share reconstruction concepts are discussed in detail. The existing secret sharing scheme faces a drawback if an adversary is able to retrieve the secret, even without a valid share. The paper proposed the concept of randomized component which binds the shares with their particular shareholders. Due to this, the adversary is not able to recover the secret.	The randomized component method makes the scheme more complicated as each participant needs to be authenticated by another one.
Siyaram Gupta and Madhu Sharma	The paper discusses the Adi Shamir's secret sharing scheme in detail. The paper describes how the shares are split at the distributor end and how they are reconstructed at the receiver end. Various cryptographic encryption algorithms are also described in the paper.	The paper involves only the analysis of various encryption algorithms.
Lein Harn	The paper describes the basic concept of group authentication and secure transmission of secret in a group. It includes a review of Shamir's (t,n) Secret Sharing Scheme. The concept of token generation is discussed in the paper. The paper also describes the share generation, token generation, secret reconstruction and group authentication in detail along with the concept of Lagrange's polynomial.	The scheme should be able to work properly for various size m (i.e., t<m<n) of users participating in the authentication.

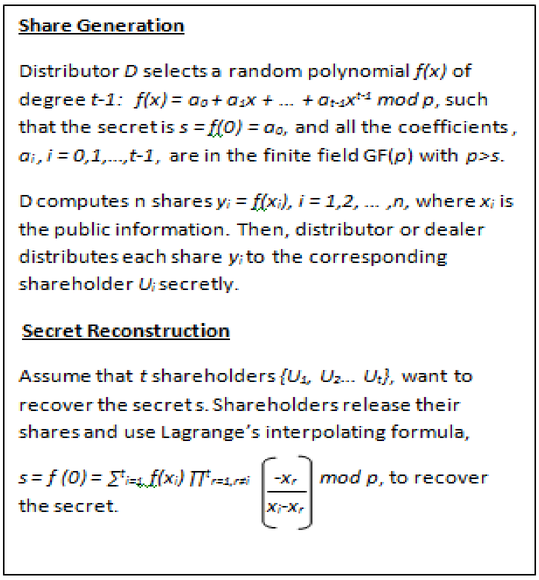
III. PROPOSED SYSTEM

The proposed system is a solution to the Man in the Middle Attack. Man in the Middle Attack can be resolved by introducing the concept of token generation into the existing Secret Sharing Scheme. Due to token generation for each shareholder, the intruder will not get the token from the distributor, thus the secret cannot be retrieved by the intruder.

A. Problem Definition

Secure transmission of data across a network is a necessity in today's era. Among the various cryptography mechanisms, the Adi Shamir's Secret Sharing Scheme (SS Scheme) is the most secured one and hence is widely used. The Adi Shamir's secret sharing scheme depends on Lagrange's polynomial for dividing the secret into number of shares. However, an adversary or intruder may obtain the secret even without any valid share. This creates Man in Middle Attack in the existing system. Therefore, to overcome this drawback, the concept of token generation is proposed. Token generation mechanism involves binding of shares with the respective shareholders. Because of this, the intruder will not be able to retrieve the secret, without possessing a valid share. The main objective of the proposed system is to provide a more secure transmission of data in a network consisting of a group of nodes. Along with secure transmission of data, the proposed system also focuses to tackle the Man in the Middle Attack, so that an intruder will not be able to retrieve the secret without any valid share.

The existing system involves the division of secret into a number of shares equal to the number of nodes in the group. Among all the nodes, a fewer i.e. t of them can recover the secret. But less than t nodes are unable to recover the secret.



Share Generation

Distributor D selects a random polynomial $f(x)$ of degree t-1: $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1} \bmod p$, such that the secret is $s = f(0) = a_0$, and all the coefficients, a_i, $i = 0,1,\dots,t-1$, are in the finite field GF(p) with $p>s$.

D computes n shares $y_i = f(x_i)$, $i = 1,2, \dots ,n$, where x_i is the public information. Then, distributor or dealer distributes each share y_i to the corresponding shareholder U_i secretly.

Secret Reconstruction

Assume that t shareholders $\{U_1, U_2 \dots U_t\}$, want to recover the secret s. Shareholders release their shares and use Lagrange's interpolating formula,

$s = f(0) = \Sigma^t_{i=1} f(x_i) \Pi^t_{r=1,r\neq i} \left(\frac{-x_r}{x_i - x_r}\right) \bmod p$, to recover the secret.

Fig1: Adi Shamir's Secret Sharing Scheme

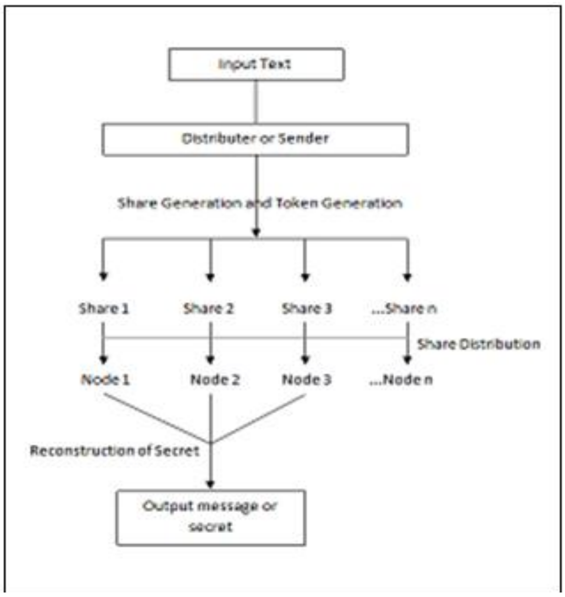


Fig2: Proposed System Architecture

However, more than t participants can recover the secret. Due to this, an intruder can attack and intervene as a participant to reconstruct the secret. Thus, it is prone to the Man in Middle Attack. To solve such an attack, the concept of token generation is proposed. All the shares are attached with the tokens generated by the distributor. Hence, each share is binded with the shareholder with the help of token. Thus, an intruder will not receive the token and hence is unable to reconstruct the secret. The token binds the share with its shareholder as well as helps in secret reconstruction. Therefore, the proposed system provides better security as compared to the traditional secret sharing scheme.

DOI 10.17148/IJARCCE.2016.54148

IV. IMPLEMENTATION

Implementation of the proposed system involves the environment in which the system is implemented and the overall system development. The overall development of the proposed system requires suitable environment and proper resources for its successful completion. The proposed system is developed for a client-server communication. At the server, the secret is divided into a number of shares. These shares are then distributed to the clients along with the public information. At the client, the received encrypted string is decrypted and again the shares are generated. These shares are then combined in order to reconstruct the secret.

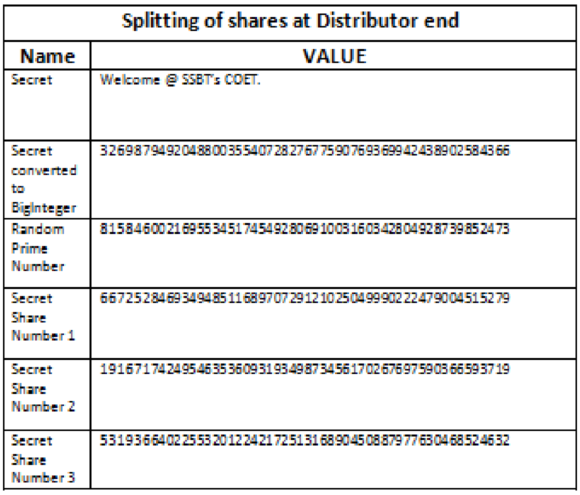
A. Flow of system development

The proposed system involves the transmission of secret or message from a server to multiple valid clients. Fewer of the clients can sit together in order to reconstruct the secret. At the server, a random prime number, which is larger than the secret is chosen and the Lagrange's polynomial for the secret is formed. The secret is then divided into number of shares, equal to the number of shareholders. The shares are then encrypted using the public information and hence resulting into the tokens. These tokens are then sent to the multiple clients or shareholders over a network through UDP. At the client side, the encrypted token is received. This token is then decrypted by using Lagrange's polynomial and a random prime number. The evaluation of the polynomial then generates the shares. The generated shares are the combined to reconstruct the secret.

V. RESULTS

At the distributor end, the secret in the form of number, string, special character or a combination of these is converted into a BigInteger. A random prime number is then chosen which is greater than the secret. The prime number along with the BigInteger secret is used to form the Lagrange’s polynomial. The polynomial is then used to generate the shares, equal to the number of participants in the network.

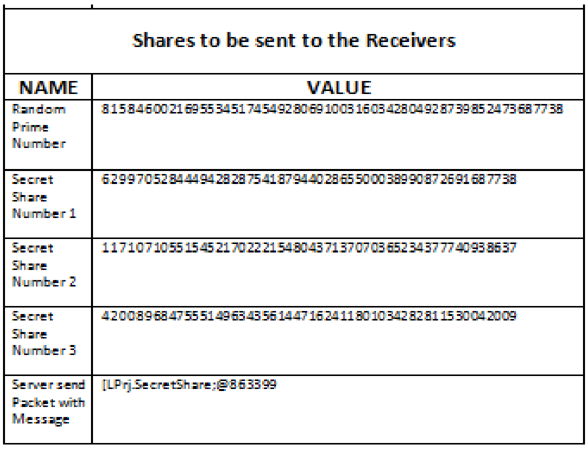
TABLE II RESULT FOR DISTRIBUTOR OR SENDER



Splitting of shares at Distributor end	
Name	**VALUE**
Secret	Welcome @ SSBT's COET.
Secret converted to BigInteger	32698794920488003554072827677590769369942438902584366
Random Prime Number	81584600216955345174549280691003160342804928739852473
Secret Share Number 1	66725284693494851168970729121025049990222479004515279
Secret Share Number 2	19167174249546353609319349873456170267697590366593719
Secret Share Number 3	53193664022553201224217251316890450887977630468524632

At the time of distribution of shares, the secret is again split in order to regenerate the shares so as to send it to the receiver. Along with the shares, the public information, also called as token is also sent through the User Datagram Protocol.

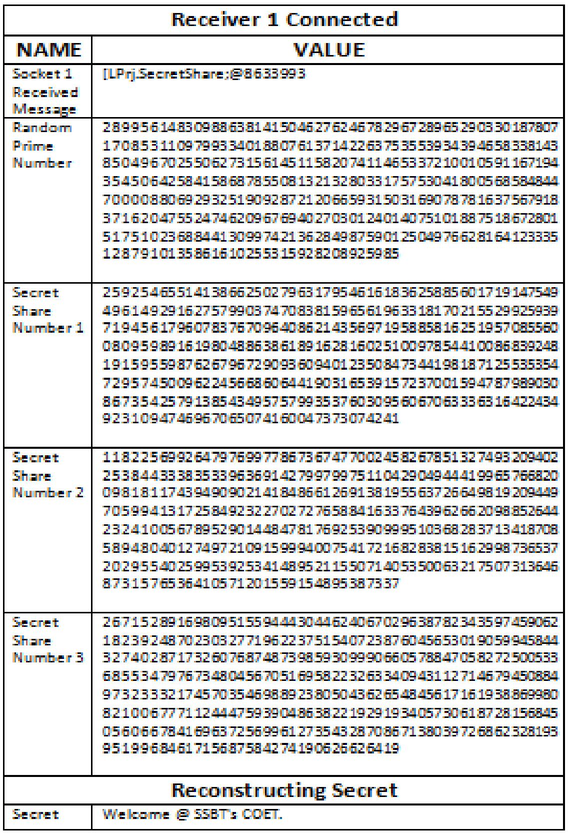
TABLE III RESULT FOR DISTRIBUTION OF SHARES TO SHAREHOLDERS



Shares to be sent to the Receivers	
NAME	**VALUE**
Random Prime Number	81584600216955345174549280691003160342804928739852473687738
Secret Share Number 1	62997052844494282875418794402865500038990872691687738
Secret Share Number 2	11710710551545217022215480437137070365234377740938637
Secret Share Number 3	42008968475551496343561447162411801034282811530042009
Server send Packet with Message	[LPrj.SecretShare;@863399

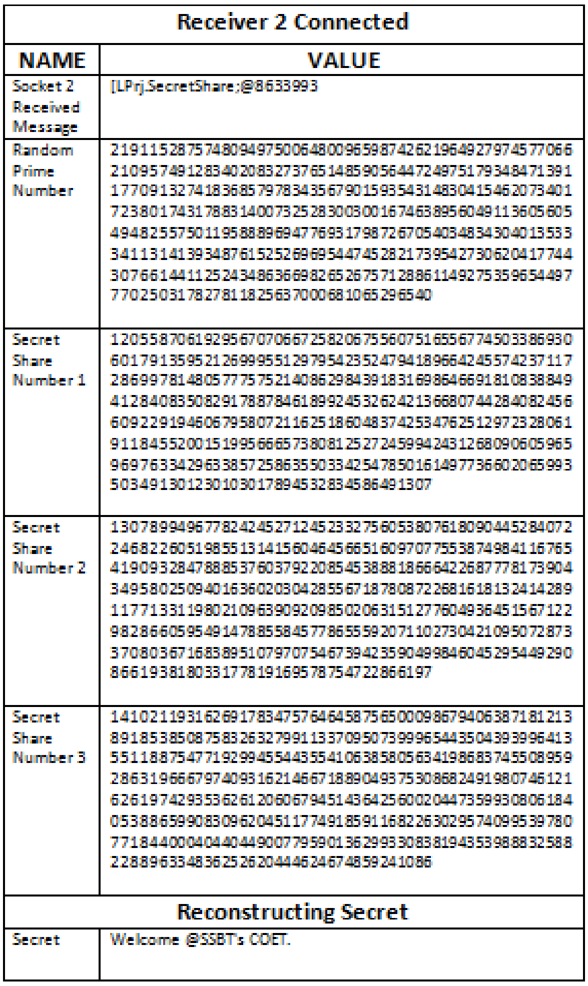
At the receiver end, the encrypted message containing the token and shares is received. This received string is then used along with a new random prime number to generate the Lagrange’s polynomial. The shares are then regenerated. By combining fewer of the shares (i.e. t shares), the secret message is reconstructed. The results for receivers 1 and 2 are shown in the following tables.

TABLE IV RESULT FOR SHAREHOLDER OR RECEIVER 1



Receiver 1 Connected	
NAME	**VALUE**
Socket 1 Received Message	[LPrj.SecretShare;@8633993
Random Prime Number	289956148309886381415046276246782967289652903301878071708531109799334018807613714226375355393439465833814385049670255062731561451158207411465337210010591167194354506425841586878550813213280331757530418005685848447000088069293251909287212066593150316907878163756791837162047552474620967694027030124014075101887518672801517510236884413099742136284987590125049766281641233351287910135861610255315928208925985
Secret Share Number 1	25925465514138662502796317954616183625885601719147549496149291627579903747083815965619633181702155299259397194561796078376709640862143569719588581625195708556008095989161980488638618916281602510097854410086839248191595598762679672909360940123508473441981871255353547295745009622456686064419031653915723700159478798903086735425791385434957579935376030956067063336316422434923109474696706507416004737307424 1
Secret Share Number 2	118225699264797699778673674770024582678513274932094022538443338353396369142799799751104290494441996576682009818117439490902141848661269138195563726649819209449705994131725849232270272765884163376439626620988526442324100567895290144847817692539099951036828371341870858948040127497210915999400754172168283815162998736537202955402599539253414895211550714053500632175073136468731576536410571201559154895387337
Secret Share Number 3	267152891698095155944430446240670296387823435974590621823924870230327719622375154072387604565301905994584432740287173260768748739859309990660578847058272500533685534797673480456705169582232633409431127146794508849732333217457035469889238050436265484561716193886998082100677711244475939048638221929193405730618728156845056066678416963725699612735432870867138039726862328193951996846171568758427419062662641 9
Reconstructing Secret	
Secret	Welcome @ SSBT's COET.

TABLE V RESULT FOR SHAREHOLDER OR RECEIVER 2



Receiver 2 Connected	
NAME	**VALUE**
Socket 2 Received Message	[LPrj.SecretShare;@8633993

Random Prime Number	21911528757480949750064800965987426219649279745770666
	21095749128340208327376514859056447249751793484713911
	17709132741836857978343567901593543148304154620734011
	72380174317883140073252830030016746389560491136056055
	49482557501195888969477693179872670540348343040135333
	34113141393487615252696954474528217395427306204177444
	30766144112524348636698265267571288611492753596544977
	7702503178278118256370006810652965 40

Secret Share Number 1	12055870619295670706672582067556075165567745033869300 60179135952126999551297954235247941896642455742371177 28699781480577757521408629843918316986466918108388499 41284083508291788784618992453262421366807442840824566 60922919460679580721162518604837425347625129723280611 91184552001519956665738081252724599424312680906059655 96976334296338572586355033425478501614977366020659933 503491301230103017894532834586491307
Secret Share Number 2	13078994967782424527124523327560538076180904452840722 24682260519855131415604645665160970775538749841167655 41909328478885376037922085453888186664226877781739044 34958025094016360203042855671878087226816181324142899 11771331198021096390920985020631512776049364515671222 98286605954914788558457786555920711027304210950728733 37080367168389510797075467394235904998460452954492900 866193818033177819169578754722866197
Secret Share Number 3	14102119316269178347576464587565000986794063871812133 89185385087583263279911337095073999654435043939964133 55118875477192994554435541063858056341986837455089599 28631966679740931621466718890493753086824919807461211 62619742935362612060679451436425600204473599308061844 05388659908309620451177491859116822630295740995397800 77184400040440449007795901362993308381943539888325888 228896334836252620444624674859241086
Reconstructing Secret	
Secret	Welcome @SSBT's COET.

The proposed system provides better reliability, integrity and security as compared to the existing system.

VI. CONCLUSION

Secure transmission of data is a necessity in the networks. The existing secret sharing scheme is prone to the Man in Middle attack, thus the proposed system is developed to overcome the drawback. Therefore the proposed system involving token generation mechanism provides better reliability, integrity and security than the existing one.

The system can be further extended for the secure transmission of image, audio and video data through various image processing techniques.

REFERENCES

[1] Miao Fuyou, Xiong Yan, Wang Xingfu, and Moaman Badawy. “Randomized component and its application to (,)-group oriented secret sharing". “Information Forensics and Security, IEEE Transactions", 10(5):889-899, 2015. (Research Paper)

[2] Siyaram Gupta and Madhu Sharma. “A python based enhanced secret sharing scheme to secure information using cryptography techniques”. “International Journal of Advanced Science and Technology", 71:15-30, 2014. (Research Paper)

[3] Lein Harn. “Group authentication". “Computers, IEEE Transactions", 62(9):1893- 1898, 2013. (Research Paper)

[4] Liu, Yining, and et al. "An improved authenticated group key transfer protocol based on secret sharing." Computers, IEEE Transactions on 62.11 (2013): 2335-2336.

[5] Rivest, Ronald L., Adi Shamir, and Yael Tauman. "How to share a secret."Communications of the ACM. 1979.

[6] Yang, Chou-Chen, Ting-Yi Chang, and Min-Shiang Hwang. "A (t, n) multi-secret sharing scheme." Applied Mathematics and Computation 151.2 (2004): 483-490.

DOI 10.17148/IJARCCE.2016.54148