Privileged authenticity in reconstruction of digital encrypted shares

Joydeep Dey[1], Anirban Bhowmik[2], Arindam Sarkar[3], Sunil Karforma[4]
[1]Department of Computer Science, M.U.C. Women's College, Burdwan, WB, India
[2]Department of Computer Application, Cyber Research & Training Institute, Burdwan, WB, India
[3]Department of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math, Howrah, WB, India
[4]Department of Computer Science, The University of Burdwan, Burdwan, 713104, WB, India

Article Info

Article history:

Received Jan 28, 2019
Revised Mar 30, 2019
Accepted May 10, 2019

Keywords:

Authentication
Entropy
Floating frequency
Privileged recipient
Threshold

ABSTRACT

Efficient message reconstruction mechanism depends on the entire partial shares received in random manner. This paper proposed a technique to ensure the authenticated accumulation of shares based on the privileged share. Threshold number of received shares inclusive of the privileged share, were being accumulated together to validate the original message. Although attaining threshold number of shares or more excluding the privileged share, it would not be possible to reconstruct the original message. Encryptional procedure has been put into the desired partial shares to confuse the evaesdroppers. Decisive parameter termed as hash tag has been extracted from the cumulative shares and bitwise checking procedure has been carried out. In appearance of first mismatch, rests of the checking bits were ignored, as test case put under failure transaction. Different statistical tests namely floating frequency, entropy value have proved the robustness of the proposed technique. Thus, extensive experiments were conducted to evaluate the security and efficiency with better productivity.

Corresponding Author:

Joydeep Dey,
Department of Computer Science,
B.C. Road, Uttar Fatak, Post- Rajbati,
Burdwan, West Bengal, India- 713104.
Email: joydeepmcabu@gmail.com

1. INTRODUCTION

Digital communication system is the backbone of technological data exchange protocols throughout the world. With the emergence of the Internet, the need of secured and trusted delivery of message evolves at greater dimensions. Cryptography [1-3] is one of the intermediate solution approaches for such abstract level of message communication. There are so many malware attackers present in the network, whose main task is to sniff the confidential data during communications. Once they succeed, they do synchronize with the recipients for rest of the session. Attackers willingly do distort or damage the messages which were supposed to be procured in between the two parties only. Validation of the regenerated message by the receiver is an essential feature in any format of digital communications. The proposed technique addresses the said area of concern through hiding the delegation of privilege to a recipient from the intruders. The organization of this paper is as: Section 1.1 deals with the brief literature survey, Section 1.2 contains the problem domain, Section 1.3 reveals the proposed solution in short, Section 2 and Section 3 illustrate the proposed technique and its brief explanation respectively. Results are discussed in the Section 4 and Section 5 has the conclusion.

1.1. Literature survey

A pattern of value is a key which is used for encryption by the sender and it is used for decryption by the receiver in case of symmetric key cryptography. The exchange of that particular key is the basic criteria in cryptography. The most challenging fact is that an intruder silently intercepting all the cipher text in the network to decode the message. The key exchange problem [4] was coined by two scientists Whitfield Diffie and Martin Hellman in 1976. They have proposed a system to exchange a key from X to Yeven if I observs the entire communication, where X, Y, and I represents sender, receiver, and intruder on the global view. Another technique to transmit a message with more security is secret sharing of data [5]. A transmittable data would be splitted into multiple fragments with the criteria that threshold fragments can only reassemble the entire data. Blakey's Secret Sharing Scheme [6] has applied geometry to solve secret sharing of data. The secret data is a point value in a k- dimensional space and corresponding n shares are treated as the point of intersection on an affine hyper plane. The solution set $y = (y_1, y_2, \dots, y_k)$ and the equation $p_1 y^1 + p_2 y^2 + \cdots + p_k y^k = b$ forms an affine hyper plane. The point of intersection can be found by determing the intersection on the hyper planes.

1.2. Problem domain

Leakage of the information without the consent of the admimistrator is possible in existing system of secret sharing. Controlling the personal information and not to accessible to the external hands on the network is a big challenge. Thus, in a group sharing of partial shares, some malpractioners may do misuse the sender's confidential data in wrong direction.

1.3. Proposed solution

If a grant of privilege is issued to a delegated sender/recipient, then it may be assured that without the involvement of that recipient, the original message cannot be regenerated. Authentication at the recipient's terminal is badly needed due to the fact that messages can be duplicated, manipulated, damaged, reverted, etc by the intruders. To make the communication system more reliable [7-8], this proposed technique provides a better optimal answer.

2. PROPOSED TECHNIQUE

The key idea is to include the privileged share at the recipient's end. Thus, to create one additional protection level, so that without the privileged share the original message cannot be regenerated. The foremost task is to accumulate the privileged share and other partial shares which constitute the threshold value. It is followed by the filtering of specified fields help to achieve the proposed technique. The specified fields are extracted accordingly followed by the authenticity verification. In case of genuine authentication, further deciphering of the shares is being carried out.

```
$Proposed\ Algorithm: Privilege\ Based\ Authentication$
$Requirement(s): Sender's\ ID\ No.(PID), Master\ Key\ of\ Sender(Mk), Source\ File\ (S1.PDF\ )$
$Input(s): n, k\ :\ number\ of\ recipients\ \&\ threshold\ number\ respectively$
$Output(s): Regenerated\ authenticated\ message$
$\{/*\ Merge\ of\ Privilege\ Share\ with\ threshold\ */\}$
$Threshold\_MSG\ [\ ] \leftarrow Call\ Merge\_Shares\ ((k-1)\ number\ of\ shares\ [\ ], Privileged\_Share\ [\ ])$
$\{/*\ Validation\ of\ Shares\ */\}$
$Field[0 \dots 3] \leftarrow Call\ ExtractionFields\ (Threshold\_MSG)$
$\{/*\ Authentication\ Verification\ */\}$
$TEMP \leftarrow Call\ Authentication\ (Field[2], Field[3])$
$If\ (TEMP)\ Then$
    $Success$
$Else$
    $Report\ Failure\ in\ data\ transmission$
$End\ if$
```

2.1. Proposed merging of digital secret shares

The proposed technique deals with that the threshold number of shares are minimum needed to be combined together to regenerate the original share. The novelty of our proposed technique is that a grant of privilege has to be assigned to a pre-defined recipient. This recipient is delegated as privileged recipient. Unless and until the share of the privileged recipient is merged into the threshold shares, the original data can not be revealed. Bitwise ORing operations were carried on those threshold digital shares.

```
Proposed Algorithm: Merge_Shares
Requirement(s): $(k-1)$ Threshold Shares, $TSH[1], \dots. TSH[k-1]$, (1) Privileged_Share, $PSH[\,]$
Input(s): $n$: Number of Recipients, $k$: Threshold Value
Output(s): Merged Matrix$[k][\,]$: Merged matrix obtained from threshold
{/* Operations on threshold digital shares */}
$MAT1[\,] \leftarrow$ Call Merge ( $TSH[1], TSH[2], \dots, TSH[k-2]$ )
{ /* Merging of Privileged Share */ }
$MAT1[\,] \leftarrow$ Call Merge ( $MAT1, PSH[\,]$ )
```

The Merge ( ) function called as above is a dynamic function which can receive multiple parameters as shares. Since the partial received shares are of same length. The principal work done by this is to determine the resultant of bitwise OR operations carried out between the multiple digital shares.

2.2. Proposed extraction of fields

The orientation of the bits while transferring the secret message as follows according to our proposed technique. The first attribute is header of four bits length, out of which two denotes the size of the encrypted file and remaining two denotes the length of the digest. The second attribute denotes the entire encrypted message. The third attribute denotes the contents of the message digest. And the last attribute denotes the encrypted key of the sender's master key.

```
Proposed Algorithm: Authentication of Fields
Requirement(s): Master key of sender, Header structure, Matrix of privileged shares.
Input(s): MST_KEY, Header, MAT1
Output(s): Required fields
{ /* Extraction of Fields */ }
Size = Call ValueAt( Header , 1,2 )
DigestSize = Call ValueAt( Header , 3,4 )
EK = Call RSA ( MST_KEY )
EncSize = Call SizeOf ( Ek)
EF ← Call SubString( MAT1 , 5, Size)
DK ← Call SubString( MAT1 , EF + 5 , DigestSize)
PAD ← Call SubString ( MAT1, 4 + EF + DK + 1, EncSize )
```

2.3. Proposed authentication verification

Proposed algorithm authenticates the threshold number of shares received and processed henceforth. The fourth field of the accumulated share would be extracted at the recipient's end, which in turn would be fed into the MD5 algorithm to generate the hash code of 128 bits. A bitwise XOR operation would be done between the generated hash code and received hash code through secured channel. The sensitivity parameter is that if any conflict observed even in a single bit determines the bit distortion/damage while message communication, and decides the invalid merging of shares. So the sensitivity test is on the entire sequence of bits. Following algorithm determines the authenticity based on checking.

```
Proposed Algorithm: Authentication Verification
Requirement(s): Temp [128]: Integer Array
Input(s): Pad field (summation of thsersold shares) ($P_{AD}$), digest key ($D_K$)
Output(s): verified or not (yes or not)
{ /* Retrieval of Message Digest */ }
DK' ← Call MD5 ( PAD )
for i = 0 to 127 do
Temp [i] ← (DK[i □ DK'[ i ] ) // Equality Checking done here
end for
Set flag = 0
for i = 0 to 127 do
if ( Temp[i] ! = 0 ) then
flag = 1
break
end if
end for
if (flag ) then
Verification Failed
else
Verification Success
end if
```

3. ILLUSTRATION OF PROPOSED TECHNIQUE

To illustrate the proposed technique in brief, $\{n, k\}$ can be assumed as $\{5, 3\}$ where n and k denotes the number of recipients and threshold respectively. Let $8A24C34AG7SK25$ be the master key (MK) of the sender and a message saved as p1.pdf is to be shared using this proposed technique. The sender's public key pair may be $(137, 83)$ which are prime numbers. The public key pair of the following desired recipients show in Table 1.

Table 1. Public key pairs of recipients

Sl.No.	Recipient ID	Known Key Pair
1	R#1	public (97, 73)
2	R#2	public (197, 41)
3	R#3	public (103, 173)
4	R#4	public (173, 41)
5	R#5	public (97, 23)

The corresponding master key (M_K) of the sender has been fed into RSA algorithm to obtain the encrypted key (E_K) de94f81bfe83f7eed728. Similarly, the source file (p1.pdf) has also been encrypted using RSA algorithm to generate the following hexadecimal string $260d8f2f \ldots e7$. Now using a hash algorithm, the digest of the encrypted key is $c7c52f2bbab358795947dfbd27e5d63b$. Shown in Figure 1 structure has been proposed.

Header	Encrypted data	Digest key (D_K)	Padding
MSG: 0A14	260d8f2f…e7	c7c52f2bbab358795947	dfbd27e5d63bde94f81bfe83f7eed728

Figure 1. Proposed structure under authentication

Following are the n (=5) number of shares which are produced from MSG using mask generation algorithm.as for example, here we use a mask matrix[9] of order $5x10$ and using this mask matrix we generate 5 shares. Three previlaged shares can generate plain text out of five shares.

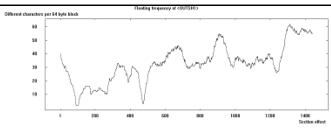
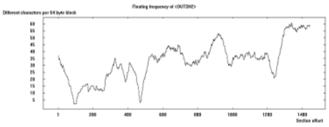
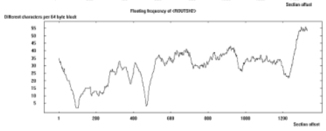
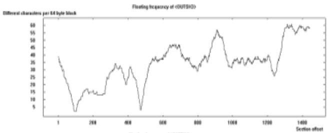
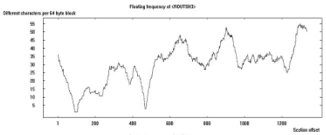
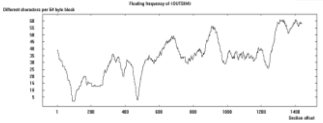
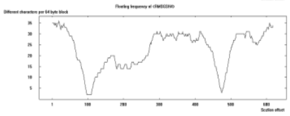
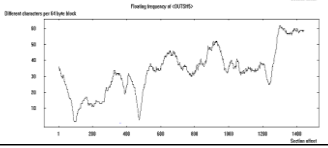
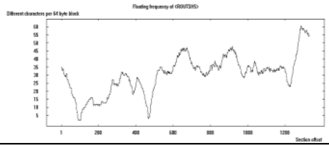
$$1st\ share: 0A00060d0f2f0707050f2b0a03080959070f0d07e5060b\ 0e04f80b0e0307ee0708$$
$$2nd\ share: 0A202600000fe7c7c0000bbab350000947dfb00005d63b\ d000081bfe80000ed72$$
$$3rd\ share: 0A20200d8f0fe0c0052f0bb0b008790940d00d2705d0300e94f81bf003f70ed020$$
$$4th\ share: 0000000d800fe0c0052f0bb0b008790940d00d2705d030\ de90f00b0083f0e00700$$
$$5th\ share: 002026008f20e0c7c02f20b0b350795040dfb027e0d03b\ d094f010fe80f7e0d028$$

Next the above shares are encrypted by the corresponding individual public key of the recipient and send them. Now each recipient decrypts the message using their private keys. Now the message can get back from ORing any three decrypted shares including the privileged share. Thus two bytes header field is separated to recognize the size of encrypted data and padding (encrypted key). Now the padding string is fed into the RSA algorithm to generate master key and using the same hash algorithm to generate an output, which is being checked with digest key (D_k).On successful checking, the original secret data can be reconstructed by decrypting the encrypted data using sender's public key, else, on hit and trial method the said procedure is repeatedly done over another k number of shares.

4. RESULTS SECTION

Shown in the Table 2 floating point frequency represents the number of repeated characters in a block of text. If the repeated characters are much more in a text then intruders can predict the plain text. Floating frequency analysis and entropy value analysis show that comparison to existing protocol for encryption and secret sharing are at par for the proposed model. Floating point frequency represents the number of repeated characters in a block. Our technique provides extra authentication of messages by using MD5 algorithm, in both receiver and sender sides.If we compare the entropy values between the cipher text by RSA with the cipher text by our proposed scheme the in all share our technique provides good result.

Table 2. Floating point frequency of proposed technique compared to standard technique

Share No.	Plain Text	Cipher Text by RSA	Cipher Text by Proposed Algorithm
Share 1			
Share 2			
Share 3			
Share 4			
Share 5			

4.1. Analysis based on entropy value

Entropy is the measure of unpredictability of information in cipher text. Entropic security in encryption means it is very hard to predict the nominal information about plain text. Show in Table 3 the entropy value of our technique and this value is better than existing technique. So the table and Figure 2 graph indicates that the technique is robust than any existing technique. If one looks at the shares in the above example it is cleared that the shares are all different from the actual key and there is no one to one relation between the shares and the actual key. Here longer key length denotes better security.The key is first encrypted by the sender’s private key and finally opened by sender’s public key, which confirms both authenticity and non-repudiation.The shares are encrypted by individual receiver’s public key before transmission and opened by individual receiver’s private key at the receiving end, which ensures confidentiality. Each share contains the share of the signature along with the share of the key. After reconstruction, the signature is compared with the digest of the key thus generated to ensure integrity.It can also be noticed that the n shares are generated only by ANDing n different masks with the secret message (how) and reconstructed simply by ORing the predefined minimal k number of shares where n and k can be anything $k \leq n$ and $n›2$.

Table 3. Entropy value of our proposed technique and standard technique

Source	Plain Text	Cipher text by RSA	Cipher text by proposed technique
Share 1	6.29	2.34	5.42
Share 2	6.27	3.28	5.42
Share 3	6.3	3.59	5.49
Share 4	6.29	3.67	5.39
Share 5	6.29	3.5	5.57

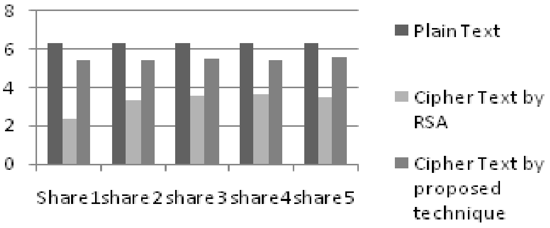


Figure 2. Graph for entropy value

5. CONCLUSION

Message regenation without the consent of the admimistrator can not be done in the proposed methodology. Now the sender can transmit data without being accessible to the unauthorized nodes by keeping his/her privilege. Thus, in a group sharing of partial shares, it provides more reliability in terms of encryption alanysis. This proposed technique provides a better optimal answer and is best suited for any financial transaction because of its two layer security and authentication under priviged scheme.

REFERENCES

[1] C.Asmuth and J.Bloom, “A modular to key safeguarding”, *IEEE Transaction on Information Theory*, vol.29, no. 2, pp. 208-210, 1983.

[2] G.R. Blakley, “*Safeguarding Cryptographic Keys*,” in Proceedings of AFIPS International Worhshop on Managing Requirements Knowledge, pp. 313, 1979.

[3] Sarkar A., Dey J., Bhowmik A., Mandal J.K., Karforma S. (2018), Energy Efficient Secured Sharing of Intraoral Gingival Information in Digital Way (EESS-IGI), In: Mandal J., Sinha D. (eds) Social Transformation – Digital Way. CSI 2018. *Communications in Computer and Information Science*, vol 836. Springer, Singapore.

[4] Shamir: “How to share a secret?” Comm ACM 22(11):612-613, 1979.

[5] Y. Desmedt “*Some recent research aspects of threshold cryptography*” Proc of ISW’97 1st International Information Security Workshop vol.1196 of LNCS paper 158-173 Springer-Verlag 1997.

[6] De Santis, Y. Desmedt, Y. Frankel and Y. Yung “*How to share a function securely*?” In proc of STOC 94, paper 522-533, 1994.

[7] Sarkar A., Dey J., Bhowmik A., Mandal J.K., Karforma S. (2019) Computational Intelligence Based Neural Session Key Generation on E-Health System for Ischemic Heart Disease Information Sharing. In: Mandal J., Sinha D., Bandopadhyay J. (eds) Contemporary Advances in Innovative and Applicable Information Technology. *Advances in Intelligent Systems and Computing*, vol 812. Springer, Singapore.

[8] Sarkar A, Dey J, Chatterjee M.,Bhowmik A.,Karforma S., “Neural soft computing based secured transmission of intraoral gingivitis image in e-health care”, *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 14(1), pp. 186-192, April-2019.

[9] Prabir Kr. Naskar, Hari Narayan Khan, Ayan Chaudhuri, Atal Chaudhuri “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.

BIOGRAPHIES OF AUTHORS

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and Master of Computer Application from the University of Burdwan in year 2011 and he secured University First Class First Rank. He is working as a Lecturer in Department of Computer Sciences at M.U.C. Women’s College, Burdwan, West Bengal, India since 2011. He has published two journal papers (SCOPUS Indexed) and five international conferences papers. His main research work focuses on Cryptography and Computational Intelligence. He has 8 years and 0.5 years of teaching experience at UG and PG level respectively.

Anirban Bhowmik completed Bachelor of Science (Mathematics Honours) from Bolpur College, Bolpur, West Bengal, India and Master of Computer Application from the University of Burdwan in year 2008. He is working as an Assistant Professor in Department of Computer Applications at Cyber Research & Training Institute, Burdwan West Bengal, India since 2008. He has published five conference papers and two journal papers at reputed international journals, which are available online. His main research work focuses on Cryptography, Mathematical Modelling, and Soft Computing. He has 11 years of teaching experience at UG level.

Dr. ARINDAM SARKAR is currently serving the Deparment of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math-711202, Howrah as an Astt. Professor. He has completed his Master of Computer Application (M.C.A) degree in the year of 2008 from VISVA BHARATI, Santiniketan, WB, India and he secured University First Class First Rank. In the year of 2011, Dr. Sarkar has completed his M.Tech in Comuter Science & Enggineering degree from University of Kalyani, WB, India and also secured University First Class First Rank. Dr. Sarkar has completed his Doctor of Philosophy in Engineering in the year of 2015 from University of Kalyani under the INSPIRE Fellowship Scheme of Department of Science & Technology (DST), New Delhi, India. In the year of 2016 he has secured 2nd Rank in the West Bengal College Service Commission Examination. He has more than 50 International Journal and Conference publications.

Sunil Karforma has completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He received his Ph.D. in Computer Science, and is presently Professor & Head of the Dept. of Computer Science at the University of Burdwan, India. His research interests include Network Security, E-Commerce, and Bioinformatics. He has published numerous papers in both national as well as international reputed journals and conferences.