IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

A Symmetric Key based Secret Data Sharing Scheme

Anirban Bhowmik[1*], Arindam Sarkar[2], Sunil Karforma[3], Joydeep Dey[4]

[1]Department of Computer Application, C.R.T.I., Tinkonia, Goodshed Road, Burdwan, India
[2]Department of Computer Science and Electronics, R.K.M. Vidyamandira, Belur Math, Belur, India
[3]Department of Computer Science, The University of Burdwan, Burdwan, India
[4]Department of Computer Science, M.U.C Women's College, B.C. Road, Burdwan, India

**Corresponding Author: animca2008@gmail.com, Tel.: +91-9732383024*

Available online at: www.ijcseonline.org

***Abstract*— ** Data security over the Internet communication is the prime concern in this technological fast era. One of the major and fruitful security techniques is data encryption with keys. The efficiency of the encryption depends on the resistance ability of the encryption key. This paper presents an attack resistant symmetric key encryption model. In this paper, the threshold cryptographic technique provides a reliable and robust key and cipher text management system. The novelty of this system is it reconstructs the key and cipher text even in the case of destruction of difference between total shares and threshold shares on the contrary end. Thus secret sharing with symmetric key provides a robust encryption technique. The implemented symmetric key is the unique group symmetric key. The existing techniques available in world lead to high computational complexity during both sharing and reconstructing of plain text. A proposed masking method, share generation using that mask and transmission has been deployed. The symmetric key is used to impose proposed authenticity of data by implementation of the proposed key expansion technique. A secret sharing technique along with conventional cryptography technique for symmetric key validation and management make this methodology more robust. Statistical type of test results proves the robustness of our technique.

***Keywords*—**Secret Sharing, Key Expansion, Symmetric key encryption

I. INTRODUCTION

The field of network security is driven by the influence of cryptography [1-3]. Threshold cryptography [1-3] is a part of cryptographic tool. Contemporarily more sensitive data and information are stored on computers and transmitted over the Internet. We need to ensure security and safety of information. Cryptography [1-3] is the study of data and information hiding and retrieval from the unauthorized access. It is the art of protecting the information and data by transforming it into an unintelligible format in which a message can be hidden from attacker and only the intended recipient will be able to convert it into original message. All intruders can only see twaddle. The effective and secure protection of the information using symmetric key is a significant tool in modern era. There are many cryptography techniques such as DES [1], Triple DES [1], RC6[1], TWOFISH[1] etc. Symmetric key based encryption algorithms play a primary role in information security. The proposed technique works on secret sharing using symmetric key. A unique group key has been constructed which has been expanded to forty eight bytes length to achieve the encryption and authentication procedure. Here, the different shares are provided to different individuals and forcing them to co-operate to find the plain text on specified condition. Before the share generation phase, a compact structure has been designed in here with three components. One of that component facilates to achieve the authentication of the message.

II. RELATED WORK

Symmetric encryption algorithms provide extremely effective means for transmitting a lot of data and information through internet and computationally less strong than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers. There are different symmetric key algorithms, for example, DES, AES, RC6, TWOFISH, etc. The brief descriptions of a few are given below.

A. Data Encryption Standard (DES): The most widely used symmetric block cipher method. It was designed by IBM's Lucifer Cipher. DES encrypts data in blocks of size 64 bit each, which in turn generates sixty four bits of cipher text. In DES, the Feistel block cipher [3] technique is used. The two different inputs are: the plaintext to be encrypted and the secret key. It consists of a number of several rounds where each round consists of bit-shifting, S-boxes [1] and XOR operations.

B. Advanced Encryption Standard (AES): The Advanced Encryption Standard (AES) [1-2] is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology in 2001. AES is based on the Rijndael cipher. Here, encryption consists of ten rounds of processing for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys. Every round of processing contains S-Box, shift rows, mix column and add round keys. The order in which these four steps are executed is different for encryption and decryption**.**

C. Rivest Cipher 6: RC6 is a symmetric key block cipher technique developed from RC5 [1]. It was developed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. It is a proprietary algorithm, patented by RSA Security. RC6 and RC5 are same in structure and contain data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as implicating two parallel RC5 encryption method, however, RC6 uses an extra multiplication operation in order to make the rotation dependent on every bit in a word which are not present in RC5.

Now using secret sharing [4-5] technique we can decompose the whole message by different shares by using some algorithm. Some secret sharing schemes are as follows.

i) Shamir's Secret Sharing Scheme: - Shamir's Secret Sharing Scheme is implemented on $\{k, n\}$ threshold based cryptography. In this scheme a $(k-1)$ degree polynomial is necessary. The polynomial function of order $(k-1)$ is constructed as follows.

$$f(x) = (p_0 + p_1 x^1 + p_2 x^2 + p_3 x^3 + \cdots + p_{k-1} x^{k-1}) \bmod m \quad ,$$

where p_0 is the secret and m is a prime number and all other coefficients are selected randomly from secret. Each of the n shares is a pair (x_i, z_i) of numbers satisfying $f(x_i) = z_i$ and $x_i > 0, 1 \le i \le n \; and \; 0 \le x_1 \le x_2 \le x_3 \le \; \ldots \; \le x_k \le m - 1$. Given any k shares, the polynomials are uniquely determined and hence the secret p_0 can be computed via Lagrange's interpolation [5].

ii) Blakey's Secret Sharing Scheme: Blakey used geometry to solve secret sharing problem [6]. The secret message is a point in a k- dimensional space and n shares are the intersection point on affine hyper planes .The solution set $y = (y_1, y_2, y_3, \ldots, y_k)$ an equation

$$p_1 y^1 + p_2 y^2 + p_3 y^3 + \cdots + p_k y^k = b$$

forms an affine hyper plane. The intersection point is obtained by finding the intersection on the hyper planes.

Above stated secret sharing schemes are regarded as a perfect secret sharing scheme because accumulation of (k-1) shares doesn't expose any information about the secret.

III. PROBLEM DOMAIN

In symmetric encryption algorithms we effectively transmit a huge amount of data with less time complexity as compared to asymmetric encryption algorithms. But the main problem is the matter that how does nodes exchanges the symmetric key in between them. By sniffing, attackers can easily access the encryption key, and if once revealed then the overall communication will be under threat. Such algorithm does not change their keys with respect to time frames. Hence, the authentication proof is not feasible within the domain.

IV. SOLUTION DOMAIN

The proposed technique provides an extra part of message authentication along with this symmetric encryption. This proves the robustness of our technique. The tailer part of the expanded key is used to impose the authentication purpose. Thus, the authentication cum encryption technique is the added flavour of our proposed technique. The proposed methodology has been described at section V.

V. METHODOLOGY

The proposed technique has been composed of three following parts, (i) symmetric key expansion (ii) encryption with symmetric key (iii) share generation. The summary of our scheme is described by a compact algorithm, given below.

```
Algorithm 1: Proposed_ Encryption_Authentication
Input(s):  key (Skey), Plain text (file), n, k.
Output(s): Encrypted Shares.
Requirement(s): fp: File pointer.
/* Expansion of Symmetric Key */
    $ExKEY[ExSize] \leftarrow Call\ KeyExpand(\ Skey[Size]\ )$
/* Masking Creation */
Mask[n][$^{n}C_{k-1}$] ← $Call\ MaskCreate(\ n\ , k\ )$
/* Message File Encryption */
  fp←get_pointer(file)
  while ($fp\ != \ eof$) do
     Cipher_file[n] = $Equivalence\_Operation$ (fp, ExKEY)
   end while.
/* Compact Structure (CS) Generation */
fs ← Call $fileSize$ (file )
while ( $fp\ != \ eof$ ) do
    for i = 0 to 3 do
          $CS1[i] \leftarrow BitCopy(toHex(fs, 32))$
    end for
   for i = 4 to (fs+4) do
          $CS2[\ i] \leftarrow BitCopy(Cipher\_file[fs])$
    end for
    for i = fs+4 to (fs+ 36) do
        $CS3[\,i] \leftarrow BitCopy(Exp[32])$
    end for
end while
            $CS \leftarrow Concat(CS1, CS2, CS3)$
/*Secret Share Generation */
for i = 0 to n do
    EncSh[i][$^nC_{k-1}$]← Call $ShareGeneration$(CS,
    Mask[i][$^nC_{k-1}$] )
end for
```

At the recipient side, the k number of recipients separates authentication message part of compact structure and check whether file is hacked by intruders. The decryption process will be done in the reverse order of the proposed methodology.

1.PROPOSED KEY EXPANSION TECHNIQUE

The proposed key expansion technique involves sixteen bytes of symmetric key[1] as an input. This key has been expanded into three arrays; each array contains four rows and four columns according to the proposed algorithm.

Algorithm 2 : Symmetric Key Expansion

Input: - Skey [16], w [12]: Integer Array

Output: - ExKEY[48] :expanded key, Exp[32]:expanded part of key.

```
Set x, y as integer.
Set tmp as word
for x=0 to 3 do
    w[x] ← Skey [4*x], Skey [4*x+1], Skey [4*x+2],
                              Skey [4*x+3];
end for
for y= 4 to 11 do
    tmp ← w[y-1];
    if ($y \bmod 4 = 0$) then
        tmp= rotate (tmp) XOR( $Dec2Hex\_Convert$(y*2))
        w[y] = w[y-4] XOR tmp;
    end if
end for
```

Thus, forty eight bytes obtained as expanded key (ExKEY) which is used to encrypt the given file for transmission over the public transmission channel.

2. PROPOSED MASK CREATION ALGORITHM

The proposed technique of creation of mask matrix[7-8] is to determine a double dimensional matrix with order n*$^nC_{k-1}$. The purpose is to confuse the attackers in case of shares compromization. The pseudo code of the proposed mask matrix creation is given below.

Algorithm 3 : Proposed Mask_Creation

Input: n and k: Integer

Output: $Mask[n][nCk-1]$.

```
void Mask_Creation (int n , int k ){
    Set p=$^nC_k$ , num_1 = 3, k1=0, k2=0
    BIN[n], Indx[p], Indx2 [p]   : Integer Array
    Set Mid= Floor ((0+ ( p-1) /2 ), $x = 2^n - 1$;
      For i= x to 1 do
        BIN[n] ← Call $toBinary$ (i);
        if ($CountOne$ ($BIN$ [$n$] ) $=$ $num\_1$) then
            Indx [k1++] ← i ;
        end if
      end for
Indx [p] ← Call $ASC\_SORT$ (Indx [0, Mid] ||
    $ASC\_SORT$ (Indx [Mid + 1] , p - 1 );
 Set i =0 ;
Set U=Mid + 1;
While ($i <= Mid$ && $u <= p - 1$ ) do
    $Indx2\,[k2++] \leftarrow Indx[i]$;
    $Indx2\,[k2++] \leftarrow Indx\,[j]$;
    $Increment\ i$;
    $Increment\ j$;
End while
For $S = 0\ to\ (p - 1)$ do
    Mask[S][ ]← Call $toDecimal$ ($Indx$[ $Indx2$[ $S$] ]);
End for
Mask [n] [p] ← Call $Transpose(Mask[p][n])$
}
```

3. PROPOSED SECRET SHARES GENERATION

The proposed shares generations done by XORing each rows of the mask matrix upon the compact structures, CS1, CS2, and CS3. The following algorithm will illustrate the idea of secret share generation.

Algorithm 4: Secret Share Generation

Input:$Mask\ Matrix$: $Mask[n][n_{C_{k-1}}]$, Compact Structure (CS).

Output: $'n'$ number of Secret Shares.

Method:-

```
    Set gRow← get_Row (Mask[n] [$^nc_{k-1}$])
    for i= 0 to  (gRow - 1 ) do
        for j= 0 to  $^nC_{k-1}$ do
            EncSh[i][j] ← Call $BitwiseXOR$(
             CS , Mask[i][j])
        end for
    end for
```

VI. RESULTS AND DISCUSSION

A file with the extension (.txt, .doc etc) has been used as a secret data. Secret sharing algorithm should robust against all types of attacks. In secret sharing n shares with threshold value k size of each mask is ${}^{n}C_{k-1}$ where we have ${}^{n-1}C_{k-2}$ number of 0's and ${}^{n-1}C_{n-k}$ number of 1's [6]. If and only if numbers of collating shares are equal to k or more, then only the original secret file is reconstructed; otherwise file cannot be reconstructed. Because fewer shares cannot reconstruct the original header, thus we cannot have the information to construct the correct masking pattern. So the proposed technique can be categorized under a Perfect Secret Sharing (PSS) technique [9]. Here all generated shares are contains partial secret information in encrypted form, that provides additional protection to the secret message. Only when authenticated group of shares come together, then only the original secret message is reconstructed. Here histogram analysis and run test analysis addresses the strength of encryption and sensitivity of symmetric key.

KEY STRENGTH ANALYSIS OF PROPOSED PROTOCOL

In this proposed protocol shared data is very sensitive to the secret key value and. Here we have used the expanded part of symmetric key to convert the variable length to fixed length key. The expanded symmetric key is used for encryption and the expanded part is used as an authentication of message in recipient side. The beauty of our scheme is in the use of symmetric key (16 byte) and expanded part of symmetric key (32 byte) and total 48 byte key for encryption. Here we use the statistical test (poker test) for checking the randomness of key with respect to pseudo random key generation algorithm [10]. The following table of poker test provides the strength of the key.

Table1: Table for poker test

Key length (byte)	**Test result of proposed technique**	**Test result of our prng( ) key generation**
08	9.0213	12.0634
16	9.1245	12.1979
32	9.2565	12.0843
40	9.2443	12.6998
64	11.0027	12.6088

The above table of poker test shows comparison of result between our technique and a standard technique (pseudo random key generation) and which proves our technique is at per level of a standard technique and in some cases it shows good result. Lower values obtained by the proposed technique are always good characteristics of this methodology. Following figure 1 contains the graph analysis of table 1, which also proves our experimental results.

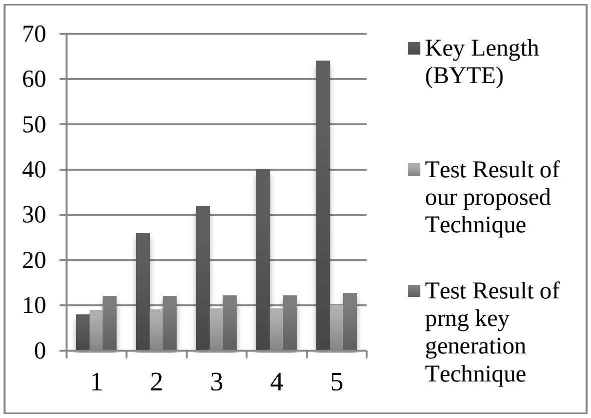


Fig1.Graph analysis of poker test

ANALYSIS OF HISTOGRAM

The binary histogram analysis describes how binary values of a file are distributed. It is a graphical representation of a frequency distribution. We examine the distribution of our data, including the peaks, spread and symmetry of the cipher text and shared cipher text. The peaks represent the most common values and spread represents how much our data varies. From the results in figure 2, it has been observed that the data are not skewed. The histogram of results data shows the distribution is normal and normal in shape. The comparative analysis of our algorithm and RC6 shows our technique at per level of RC6.

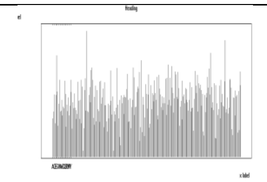
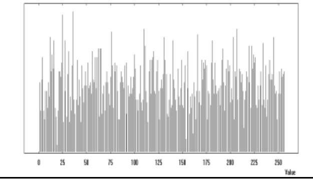
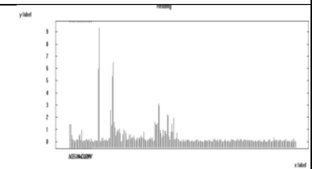
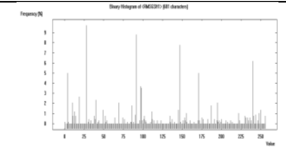
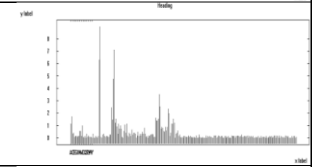
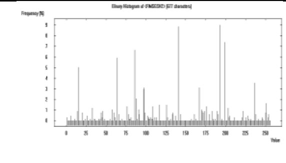
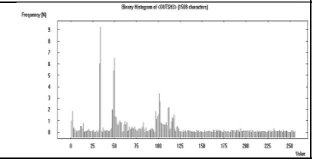
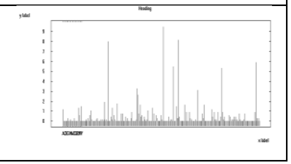
TO OLS	**CIPHER TEXT OF RC6**	**CIPHER TEXT OF PROPOSED TECHNIQUE**
HISTOGRAM		

Fig2.Histogram analysis

	Plain Text	**Cipher Text**
Sh1		
Sh 2		
Sh 3		

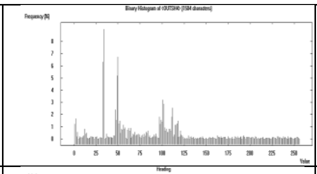
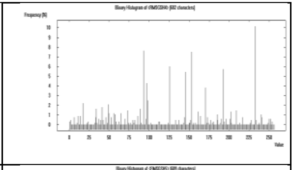
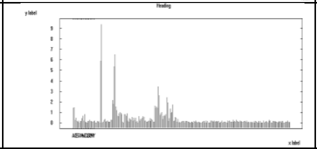
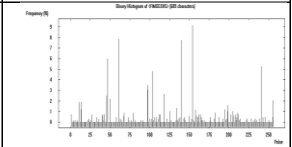
Sh 4		
Sh 5		

Fig3.Histogram analysis of shares of different shares

The above histograms of shares generated through the proposed methodology shows the distribution of data in shared file are equal which proves the encryption using symmetric key is good. Using any 'k' number of shares we get back the encrypted file and from encrypted file it is infeasible to get an idea about symmetric key. This proves strength of our scheme.

The use of secret sharing scheme in our technique protects man in the middle attack.

VII. CONCLUSION

We have presented a secured key based secret sharing approach with minimal computational overhead. Here symmetric key as well as secret data is shared among set of n number of participants and from n number of nodes, at least k number of participants are able to construct the original message. To enrich the robustness of encryption we include an authentication part. Comparative statistical test between proposed technique and pseudorandom key generation technique proves the robustness of our key. To the best of our knowledge our proposed technique is the simplest threshold secret sharing technique with symmetric key, and authentication. It is practically having minimal computational overhead during both share generation and reconstruction. The key strength analysis and histogram analysis proves the acceptability of our scheme.

REFERENCES

[1]. Stallings William ,"Cryptography and Network Security", Pearson India Education Service Pvt. Ltd., pp.111-155, 2015.

[2]. Preeti Singh et al, "Symmetric Key Cryptography: Current Trends", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, pp. 410-415, 2014.

[3]. G.R. Blakley, "Safeguarding cryptographic key", In Proceedings of AFIPS International Worhshop on Managing Requirements Knowledge, pp. 313, 1979.

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

[5]. A. De Santis, Y. Desmedt, Y. Frankel and Y. Yung "How to share a function securely?" ,In proceeding of STOC 94, pp. 522-533, 1994.

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

[7]. 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.

[8]. Y. Desmedt "Some recent research aspects of threshold Cryptography",In proceeding of ISW'97 1st International Information Security Workshop vol.1196 of LNCS pp. 158-173 Springer-Verlag 1997.

[9]. H. F. Hua ng and C.C. Chang A "novel efficient (t, n) threshold proxy signature scheme", Information Sciences 176(10): 1338-1349, 2006.

[10]. A. Peinado, J. Munilla, and A. F ´uster-Sabater. EPCGen2 Pseudorandom Number Generators: Analysis of J3Gen. Sensors, 14(4):6500-6515, 2014

[11]. F. Zheng, X. Tian, J. Song, and X. Li. "Pseudo-random sequence generator based on the generalized henon map", The Journal of China Universities of Posts and Telecommunications, 15(3):pp.64–68, 2008.

Authors Profile

Anirban Bhowmik completed Bachelor of Science (Mathematics) 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 Application at Cyber Research & Training Institute, Burdwan West Bengal, India since 2008. He has published two conferences papers and it's also available online. His main research work focuses on Cryptography and Soft Computing. He has 10 years of teaching experience at UG level.

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 Rand 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. His research interests include Network Security, E-Commerce, and Bioinformatics. He has published numerous papers in both national as well as international journals and conferences.

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 with first class first rank. He is working as Leturer in Department of Computer Sciences at M.U.C. Women's College, Burdwan West Bengal, India since 2011. He has published two conferences papers and it's also available online. His main research work focuses on Cryptography and Computational Intelligence.. He has 7.5 years and 0.5 years of teaching experience at UG and PG level respectively.