International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1785~1791
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.9674

Two Way Mechanism to Enhance Confidentiality and Accuracy of Shared Information

Manash Pratim Dutta, Subhasish Banerjee, Swarnendu Kumar Chakraborty, Chandan Tilak Bhunia
Department of Computer Science & Engineering, National Institute of Technology, Arunachal Pradesh, India

Article Info

Article history:

Received Dec 9, 2015
Revised Feb 18, 2016
Accepted Mar 2, 2016

Keyword:

Dynamic key
Error control
Randomness
Security

ABSTRACT

As such internet and information technology have influenced the human life significantly thus the current technology cannot solely assure the security of shared information. Hence, to fulfil such requirements mass amount of research have been undertaken by various researchers among which one of the mechanisms is the use of dynamic key rather than static one. In this regard, we have proposed a method of key generation to provide the dynamic keys. The scheme not only can change the key but also provide the error control mechanism. At the end of this paper, a comparison with the existing techniques has also been made to prove the efficiency of the proposed scheme.

Corresponding Author:

Manash Pratim Dutta,
Department of Computer Science & Engineering,
National Institute of Technology, Arunachal Pradesh,
Yupia, India 791110.
Email: manashpdutta@gmail.com

1. INTRODUCTION

With the rapid development of computer networks and micro electromechanical devices (smart phone, pad etc.), it becomes feasible to access the different services from different service provider servers at anytime and anywhere in the world within a fraction of second. Due to the large number of users, accessing the services at a time, it creates a huge traffic and load overhead in the communication networks. As a result, the chances of noises are growing exponentially. This may occur due to load overhead or interference by the unwanted users. Therefore, to improve the throughput and security of the shared information, mass amount of research in the field of advanced error control [1],[2] and security in shared information have been undertaken by many researchers. In 1981, Lamport [3] proposed first conventional authentication system to verify the legitimacy among the users in which the remote server maintained a password table. However, due to the system overhead, smart cards based authentication schemes [4]-[6] have been widely adopted. In addition, since the number of service provider servers for users are usually more than one, remote user authentication schemes used for multi-server architecture rather than single server circumstance is considered [7],[8].

To improve the security to next higher level, a biometric based recognization has also been incorporated as another parameter of authentication [9],[10]. But, main common factor in all those mechanisms is key must be secured enough. Meanwhile, assuring such necessity is not feasible any more with the same key; does not matter how long it is. Hence, one of the solutions is why not making the keys dynamic in nature those change in every fraction of time. But, to provide such option, either both the parties must have to agree upon a bunch of keys or they must have to share a new key by encrypting with the previous one. However, in first case, the cost of negotiating such bunch of keys and protecting the same will be too high similarly in the other case, if any one of the keys is compromised then the entire rest of the keys

can easily be decrypted by the attackers one after another. Therefore, in 2006, Bhunia et al. [11]-[13] introduced the idea of Automatic Variable Key (AVK) where neither bunch of the keys to be negotiated nor even need to be shared every time. In AVK, a new key is generated symmetrically by both the parties every time whenever a new data is exchanged. Afterwards, Chakraborty et al. [14] , Goswami et al. [15]-[19], Banerjee et al. [20]-[24], Sing et al. [25], Prajapat et al. [26] have also emphasized in this arena and proposed many new ideas to promote the security to next higher level.

Unfortunately, in all such mechanisms even though they are able to reduce the communication cost for sharing or negotiating the new keys, but still the requirements of maintaining key secrecy has not been waived completely. Because, if any how the attacker will succeed to get any one of the keys by ciphertext only attack then also he can easily compute the rest of the keys afterwards. Therefore, to overcome from the aforesaid drawback we have proposed a new mechanism to create the dynamic keys where keys can be generated based on two established initial keys. The rest of the paper is organized as follows: section 2 demonstrates the proposed scheme "Key Generation with Error Control (KGEC)" which not only generates the keys but also can provide the error control. The step wise illustration of the scheme with example is described in section 3. The experimental results have been furnished in section 4 where as comparison among the related schemes is mentioned in section 5. Finally, concluding remarks is given in section 6.

2. PROPOSED SCHEME

In this phase, we have proposed a Key Generation with Error Control (KGEC) mechanism to generate the automatic keys and provide an additional feature of error control. In this approach, the entire set of plaintext needs to be divided into equal sized blocks in the form of square matrices of order n/8, where n is the block length of encryption method (i.e. in DES, the length of n=64 bits or in AES the length of n =128 bits etc). If the length of the original plaintext is not multiple of n/8×n/8 bits then extra bits will be appended as parity bits and the blocks of matrices are encrypted one at a time. If we call such matrix as P then the matrix P can be defined as p_1, p_2, p_3, --------- where p_i is the i^{th} block of plain text.

Suppose, if the encryption method used is DES, then the order of the individual plain text matrix block is 64/8 (n = 64) i.e. 8 and every character of the plain text consists of 8 bits each. Therefore, the entire plain text blocks can be represented as per Figure 1 for the following plain text:

"if someone steals your password you can change it but if someone steals your thumb print you cannot get a new thumb the failure modes are very different".

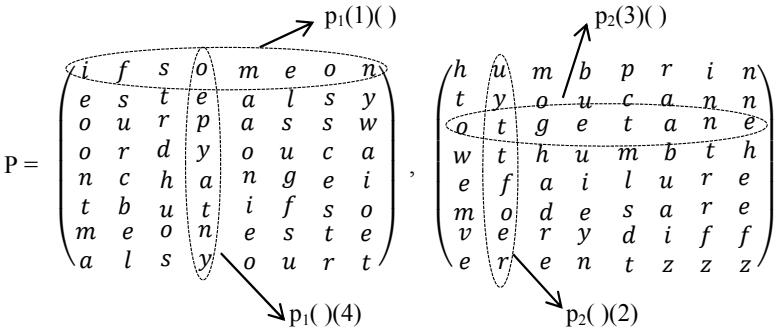

Figure 1. Representation of plain text in matrix form

After dividing the entire plain text into matrix form, each row and each column would be encrypted separately by the auto generated variable keys. Therefore, for each n/8 number of plaintext in the block, the number of ciphertext will be n/4 (i.e. n/8+n/8). Once all the n/8 row cipher as well as n/8 column cipher are received successfully, then the receiver will perform decryption separately and create two new set of matrices one for row decrypted cipher text and the other one is for column decrypted cipher text namely, p'_{row} and p'_{column} respectively. Now, if both the matrices produce the same values i.e. $p'_{row} = = (p'_{column})^T$, where M^T is transpose of the matrix M, then the received messages will be treated as error free otherwise discard the entire received messages of the corresponding blocks as noise has been detected.

The proposed scheme can generate the successive keys based on two initial keys i.e. K_{1row} and K_{1col}. At first, $p_1(1)(\ )^{th}$ row and $p_1(\ )(1)^{th}$ column of the 1^{st} plaintext matrix p_1 would be encrypted by using keys K_{1row} and K_{1col} respectively to produce the two ciphertexts $C_{1,1row}$ and $C_{1,1col}$. Therefore, for each n/8 × n/8 square matrices, the number of ciphertext will be n/4 with different auto generated keys. Now, the K_{irow}^{th} and

K_{icol}^{th} keys can simply be generated by computing $K_{irow} \leftarrow K_{(i-1)row} \oplus p_j(\,)(u-1)$ and $K_{icol} \leftarrow K_{(i-1)col} \oplus p_j(u-1)(\,)$ where u is the u^{th} row or column of the matrix block p_j. Eventually, by using these auto generated keys the encryption of the respective row or column of the matrix block can be defined as $C_{j,urow} \leftarrow E\{K_{irow}, p_j(u)(\,)\}$ and $C_{j,ucol} \leftarrow E\{K_{icol}, p_j(\,)(u)\}$ and so on.

The algorithm for key generation and encryption for the plain text blocks are described below:

$Key\_generation\_encryption(P, K_{1row}, K_{1col})$
{
$C_{1,1row} \leftarrow E\{K_{1row}, p_1(1)(\,)\}$
$C_{1,1col} \leftarrow E\{K_{1col}, p_1(\,)(1)\}$
$i \leftarrow 2, j \leftarrow 1, u \leftarrow 2$
$while(j < m)$
{
$if(j > 1 \;\&\&\; u == 1)$
{
$K_{irow} \leftarrow K_{(i-1)row} \oplus p_{j-1}(\,)(n/8)$
$K_{icol} \leftarrow K_{(i-1)col} \oplus p_{j-1}(n/8)(\,)$
}
$else$
{
$K_{irow} \leftarrow K_{(i-1)row} \oplus p_j(\,)(u-1)$
$K_{icol} \leftarrow K_{(i-1)col} \oplus p_j(u-1)(\,)$
}
$C_{i,urow} \leftarrow E\{K_{irow}, p_j(u)(\,)\}$
$C_{i,ucol} \leftarrow E\{K_{icol}, p_j(\,)(u)\}$
$if(u == n/8 + 1)$
{
$u \leftarrow 1$
$j \leftarrow j + 1$
}
$else$
{
$u \leftarrow u + 1$
}
$i \leftarrow i + 1$
}
}

3. STEP WISE ILLUSTRATION OF THE PROPOSED SCHEME

We now turn to a discussion of the stepwise operations to perform the encryption and key generation procedure of the proposed scheme. The hexadecimal equivalent of the previously mentioned 1st block of matrix p_1 of the given plain text is

$$p_1 = \begin{pmatrix} 69 & 66 & 73 & 6F & 6D & 65 & 6F & 6E \\ 65 & 73 & 74 & 65 & 61 & 6C & 73 & 79 \\ 6F & 75 & 72 & 70 & 61 & 73 & 73 & 77 \\ 6F & 72 & 64 & 79 & 6F & 75 & 63 & 61 \\ 6E & 63 & 68 & 61 & 6E & 67 & 65 & 69 \\ 74 & 62 & 75 & 74 & 69 & 66 & 73 & 6F \\ 6D & 65 & 6F & 6E & 65 & 73 & 74 & 65 \\ 61 & 6C & 73 & 79 & 6F & 73 & 72 & 74 \end{pmatrix}$$

Let the hexadecimal values of two initial keys K_{1row} and K_{1col} are "*A3EC0F172CA03BA9*" and "*CA31F06BCA352A5B*" respectively and the encryption method is DES. Therefore, the 1st encrypted row $C_{1,1row}$ is "*52E79BA985885D67*" and column $C_{1,1col}$ is "*560F60CB7061E95C*" for the matrix p_1. Therefore, to encrypt 2nd row and column of the matrix p_1, the keys K_{2row} and K_{2col} will be computed as $K_{2row} \leftarrow K_{1row} \oplus$

$p_1(\ )(1)$ and $K_{2col} \leftarrow K_{1col} \oplus p_1(1)(\ )$ and the hexadecimal equivalent of generated keys will be "*A3578304A7504535*" and "*CA89607842D456C8*" respectively. Hence, the entire row wise encrypted matrix C_{row1} and column wise encrypted matrix C_{col1} are:

$$C_{row1} = \begin{pmatrix} 52 & E7 & 9B & A9 & 85 & 88 & 5D & 67 \\ 93 & B9 & 90 & 33 & 85 & 1E & 38 & B3 \\ 8E & 56 & ED & 9B & 68 & 4F & 47 & 43 \\ 13 & 1F & 88 & 51 & F5 & 6B & 7E & EF \\ 04 & 66 & 12 & 65 & 76 & 43 & 98 & B6 \\ DE & 06 & D4 & 1A & DC & F8 & B9 & 93 \\ 2D & B8 & 33 & FD & DE & DD & 71 & 05 \\ 69 & A5 & B7 & F6 & F6 & 19 & 8A & 37 \end{pmatrix}$$

$$C_{col1} = \begin{pmatrix} 56 & 8E & 26 & A0 & 2D & 6F & C4 & AC \\ 0F & 87 & C9 & 50 & 3F & BE & ED & 78 \\ 60 & F9 & 10 & 4E & EF & FA & 00 & 52 \\ CB & 79 & 98 & DE & 5E & 61 & 9B & 26 \\ 70 & 92 & AD & 70 & 04 & 63 & 55 & CA \\ 61 & EC & F3 & C5 & 91 & C6 & 5F & C7 \\ E9 & CF & B1 & AC & 58 & 37 & 86 & 34 \\ 5C & 76 & 45 & C3 & 15 & EC & 02 & 71 \end{pmatrix}$$

Therefore, after receiving C_{row1} and C_{col1}, if the decryption forms of row wise C_{row1} completely overlaps with transpose decryption forms of column wise C_{col1} (i.e. $D\{C_{row1}\} == D\{C_{col1}\}^T$), then the receiver will take it grant that received message is noise free and kept the copy of the decrypted matrix block otherwise, simply discard the entire matrix as message been corrupted and apply the appropriate ARQ mechanism to generate resend request.

4. EXPERIMENTAL RESULTS

In this section, we will demonstrate some experimental results with various set of plain text. To express efficiency of the proposed mechanism, we have considered randomness as a parameter where randomness has been calculated based on hamming distance between the successive keys. For the illustration purpose and to prove the efficiency of our scheme to generate the successive keys, we have used the same initial keys "*673DE290F120A68C"* for row and "*5DA780E4812FCAC0*" for column in all the experiments.

Experiment 1: In this experiment, we have used "*An error detecting code can detect only the types of errors for which it is designed other type of errors may remain undetected*" as a data set. The computed values of randomness among the auto generated successive row keys and column keys are shown in Figure 2(a) and 2(b) respectively.

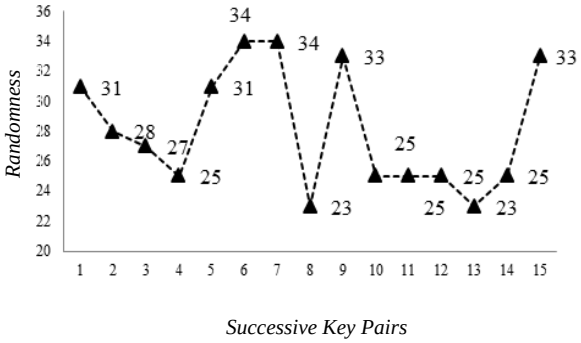

Figure 2(a). Randomness among the successive row wise keys for the experiment 1

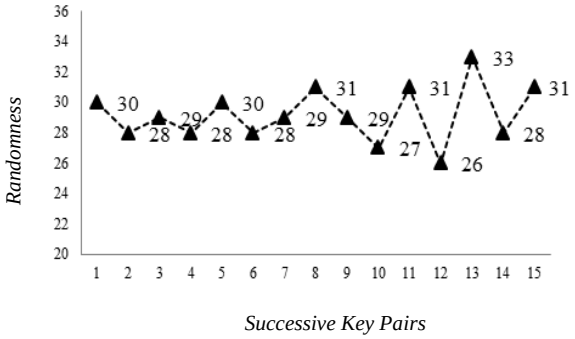

Figure 2(b). Randomness among the successive column wise keys for the experiment 1

Experiment 2: "*A burst error is more likely to occur than a single bit error. The duration of noise is normally longer than the duration of one bit which means when noise affects data it affects a set of bit*" is considered as the data set for this experiment. The experimental result for randomness are shown in Figure 3(a) and 3(b).

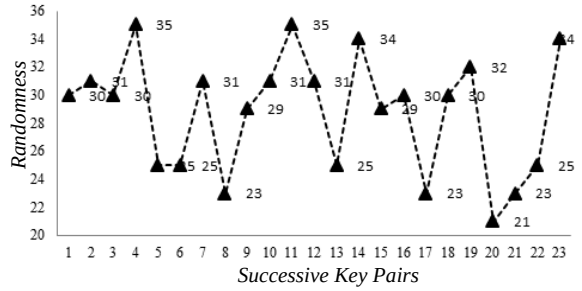

Figure 3(a). Randomness among the successive row wise keys for the experiment 2

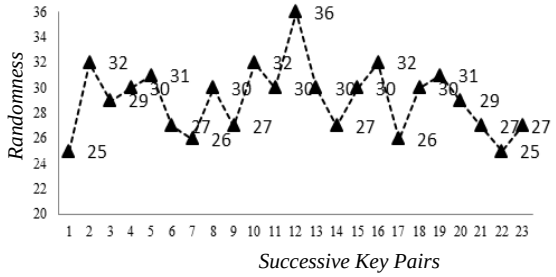

Figure 3(b). Randomness among the successive column wise keys for the experiment 2

Experiment 3: The following data set is considered for this experiment and the generated graphs are shown in Figure 4(a) and 4(b). "*Forward error correction is the process in which the receiver tries to get the message by using redundant bits where as in retransmission receiver asks the sender to resend the message*".

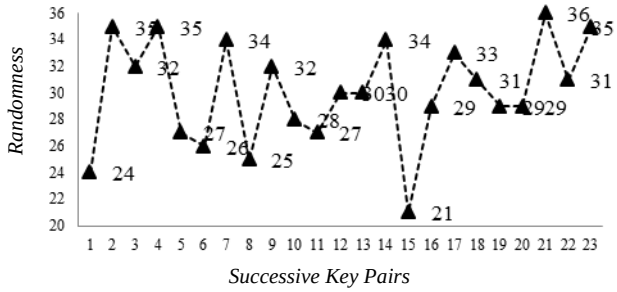

Figure 4(a). Randomness among the successive row wise keys for the experiment 3

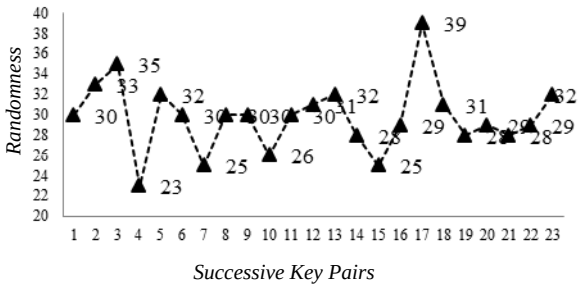

Figure 4(b). Randomness among the successive column wise keys for the experiment 3

5. COMPARISON

To justify our proposed scheme and to show the effectiveness, we have compared our proposed scheme with some existing schemes [11],[15]. Unlike the previous schemes, our scheme encrypts the messages in row and column wise and keys are also generated respectively for each block of plain text. As the plaintext has been arranged in row wise and for every row a new key is also used to generate hence, we have taken row wise auto keys only for the comparison purpose. All the three experiments from the previous section are taken for our comparison; standard deviation (Figure 5(a)) and the average randomness (Figure 5(b)) are used as the parameters where these are calculated as described in the compared schemes. In Figure 5(a) and 5(b), x-axis represents the list of experiments. In Figure 5(a), y- axis represents standard deviation whereas in 5(b), it represents average randomness.

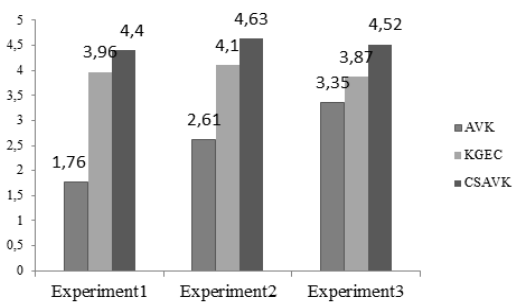

Figure 5(a). Standard Deviation comparison among the schemes

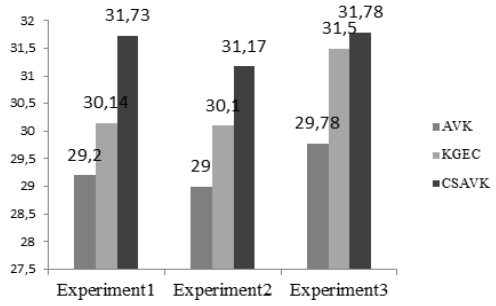

Figure 5(b). Average Randomness comparison among the schemes

6. CONCLUSION

In this paper, we have contributed a new dimension to information security where the security is not only enhanced but also defined the reliability and increased the throughput of shared information by adding error control mechanism as well. In the previous section, a comparison is also made with a set of existing schemes to prove the excellence of the proposed scheme. From Figure 5(a) and 5(b), it is cleared that randomness among the auto generated keys is far better than that of standard AVK but little bit weaker than the other one. As the scheme is based on two initial keys rather than a single one therefore, applying ciphertext only attack to find the keys is not feasible in linear polynomial time. Hence, the proposed scheme is far better and should be much preferable than existing ones for real world applications.

REFERENCES

[1] S. K. Chakraborty, *et al.*, "Investigation of Two New Protocols of Aggressive Packet Combining Scheme in Achieving Better Throughput," *Journal of the Institution of Engineers*, vol/issue: 96(2), pp. 141-145, 2014.

[2] S. K. Chakraborty, *et al.*, "Studies of several new modifications of Aggressive Packet Combining to achieve higher throughput, based on correction capability of disjoint error vectors," *Journal of the Institution of Engineers*, pp. 1-4, DOI 10.1007/s40031-014-0162-4.

[3] L. Lamport, "Password authentication with insecure communication," *Communication of the ACM*, vol/issue: 24(11), pp. 770-772, 1981.

[4] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol/issue: 46(1), pp. 28-30, 2000.

[5] C. W. Lin, *et al.*, "A new strong password authentication scheme using one-way Hash functions," *Journal of Computer and Systems Sciences International*, vol/issue: 45(4), pp. 623-626, 2006.

[6] M. Azizi, *et al.*, "Cryptanalysis and Improvement of the Zhu et al.'s Authentication Protocol," *International Journal of Informatics and Communication Technology*, vol/issue: 2(2), pp. 99-105, 2013.

[7] S. Banerjee, *et al.*, "Cryptanalysis and Security Enhancement of an Efficient and Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environments," in *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)*, March 6-7; Eluru, India, 2015. doi>10.1145/2743065.2743079.

[8] S. Banerjee, *et al.*, "An Improved Smart Card based Anonymous Multi-Server Remote User Authentication Scheme," *Internation Journal of Smart Home*, vol/issue: 9(5), pp. 11-22, 2015.

[9] K. C. Baruah, *et al.*, "An Improved Biometric-based Multi server Authentication Scheme using Smart Card," *International Journal of Security and Its Application*, vol/issue: 9(1), pp. 397-408, 2015.

[10] R. Parimala and C. Jayakumar, "Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing," *Indonesian Journal of Electrical Engineering*, vol/issue: 15(3), pp. 591-596, 2015.

[11] C. T. Bhunia, "New approaches for selective aes towards tackling error propagation effect of AES," *Asian Journal of Information Technology*, vol/issue: 5(9), pp. 1017-1022, 2006.

[12] C. T. Bhunia, "Application of AVK and selective encryption in improving performance of quantum cryptography and networks," *http://www.Ictp.it/~pub_off, IC/2006/045*.

[13] C. T. Bhunia, *et al.*, "Theory and application of time variant key in RSA and that with selective encryption in AES," in *Proceedings of EAIT (Elsevier Publications, Calcutta CSI)*, pp. 219-221, 2006.

[14] P. Chakarabarti, *et al.*, "A novel approach towards realizing optimum data transfer and automatic variable key (AVK) in cryptography," *International Journal of Computer Science and Network Security*, vol/issue: 8(5), pp. 241-250, 2008.

[15] C. T. Bhunia, *et al.*, "A new technique (CSAVK) of automatic variable key in achieving perfect security," *100th Indian Science Congress Association*, 2013.

[16] R. S. Goswami, *et al.*, "New techniques for generating of automatic variable key in achieving perfect security," *Journal of the Institution of Engineers (India): Series B,* vol/issue: 95(3), pp. 197-201, 2014.

[17] R. S. Goswami, *et al.*, "New approaches towards generation of automatic variable key to achieve perfect security," in *Proceedings of the 10th International Conference on Information Technology, IEEE Computer Society*, pp. 489-491, 2013.

[18] R. S. Goswami, *et al.*, "Generation of automatic variable key under various approaches in cryptography system," *Journal of the Institution of Engineers (India): Series B*, vol/issue: 94(4), pp. 215-220, 2014.

[19] R. S. Goswami, *et al.*, "Various new methods of implementing AVK," In *Proceedings of the 2nd International Conference Advanced Computer Science and Engineering*, pp. 149-152, 2013.

[20] S. Banerjee, *et al.*, "A novel approach to achieve the perfect security through avk over insecure communication channel," *Journal of the Institution of Engineers (India): Series B* (Communicated).

[21] S. Banerjee, *et al.*, "A New three dimensional based key generation technique in AVK," *Journal of the Institution of Engineers (India): Series B* (Communicated).

[22] B. K. Singh, *et al.*, "Generation of automatic variable key to make secure communication," in *Proceedings of the International Conference on Recent Cognizance Wireless Communication & Image Processing (ICRCWIP-2014)*, 2015.

[23] M. P. Dutta, *et al.*, "Two new schemes to generate automatic variable key (avk) to achieve the perfect security in insecure communication channel," in *Proceedings of the International Conference on Advanced Research in*

Computer Science Engineering & Technology (ICARCSET 2015), March 6-7; Eluru, India, 2015. DOI= http://dx.doi.org/10.1145/2743065.2743080.
[24] M. P. Dutta, *et al.*, "An Approach to Generate 2-Dimensional AVK to Enhance Security of Shared Information," *International Journal of Security and Its Applications*, vol/issue: 9(10), pp. 147-154, 2015.
[25] A. P. Singh and S. Kumar, "A New Method for Generation of Variable Session Keys," *International Journal of Scientific Research and Education*, vol/issue: 2(8), pp. 1578-1581, 2014.
[26] S. Prajapat, *et al.*, "A Novel Approach for Information Security with Automatic Variable Key using Fibonacci Q-Matrix," *International Journal of Computer & Communication Technology*, vol/issue: 3(3), pp. 54-57, 2012.

BIOGRAPHIES OF AUTHORS

Manash Pratim Dutta, he is an Assistent Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. He is currently working towards his Ph. D. degree in the field of cryptography and information security at the same Institute.

Subhasish Banerjee, he received his M.Tech degree in Computer Application from Indian School of Mines, Dhanbad, India in 2012. Currently he is persuing his Ph.D and also working as Assistent Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on cryptography and information security.

Dr. Swarnendu Kumar Chakraborty, he received his Ph. D. degree from National Institute of Technology, Arunachal Pradesh. Currently, he is an Assistant Professor as well as Head of Computer Science & Engineering Department, NIT Arunachal Pradesh. His research interest includes Networking, Network Security, Cryptography.

Prof. Chandan Tilak Bhunia did his B. Tech. in Radio physics and Electronics in 1983 from Calcutta University. He received his M. Tech. in Radio physics and Electronics in 1985 and then joined North Bengal University as a lecturer of Computer Science & Applications in 1988. He became Assistant Professor of ECE at NERIST, Govt. of India in 1990. He got P. hd. in Computer Science & Engineering from Jadavpur University. He became a full Professor in 1997 at NERIST. Currently, he is working as a Director of National Institute of Technology, Arunachal Pradesh. He has published around 150 research papers in various national and internatiol journals of repute. Under his supervision, five P. hd. scholars got awarded and nine scholars are currently working in various fields.