JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.8, Issue. 6, June 2020 E-ISSN: 2347-2693

Dual Secure Cryptographic Measures by Two-Phase Locking Protocol

Shabbir Hassan

Computer Science, CDE, Aligarh Muslim University, Aligarh 202002, India

Author's email id: hassan.analyst@gmail.com

DOI: https://doi.org/10.26438/ijcse/v8i6.7985 | Available online at: www.ijcseonline.org

Received: 15/June/2020, Accepted: 20/June/2020, Published: 30/June/2020

Abstract—Sender sends the lock of an encrypted binary number of a locker crisp value from a *Fuzzy Membership Table* which is defined on ASCII values of uppercase alphabets and membership function. The receiver then converts the binary number into a fuzzy number and then it is de-fuzzified using a suitable formula. *In terms of area costs, computing resources, web services, and full capabilities, Smart Grid are considered to be the enhancements over the existing grid system*. The future domain of the missions in the region is described by smart energy, smart grids, intelligent homes, and clever cities as the ambitious flagship programmer of the Indian digital initiative. *More than 100 intelligent cities in India are expected for ICT-led solutions with big data analytics.* The exponential growth of smart grids has posed several safety dangers, cyber threats, and data protection as a nation's security. *Smart grids, made up of numerous networks, intelligent control, access control, and power grid equipment, are more likely to be exposed to network security and cyber-attacks potentially interrupting delivery in a city.* The paper present a software-oriented binary grid system (a *Two-Phase Locking Protocol*) and problems associated with the intelligent grid system and discusses the use of smart grid smart hardware using the Advanced Encryption Standard (AES). To ensure that AES can be employed in the intelligent grid and communication infrastructure. The Xilinx ISE 14.2 software has designed the AES encryption and decryption unit and is synthesized in SPARTAN-3E FPGA to test for certain cases.

Keywords— Unintelligible text, Linear Recurrence, Unprotected AES implementation, fuzzy set, membership function, crisp number, smart grid communication, ASCII values, cryptography.

I. INTRODUCTION

Security has become one of the key issues in this fast-moving world. Fuzzy cryptography dissipates the situation in this circumstance. Cryptography plays a crucial role in encryption and deception. Many cryptography algorithms are available to ensure more secure communications. While several cybercrime problems arose with advanced technology growth, communication began to fail. This fugitive logic is a strong method for keeping inputs unknown [26]. Ravindu et al. Madanayake in 2012 [6, 28] have been found that the only security issues of the current algorithms, which are equally important in process duration, are both processed duration and safety using encryption and decryption algorithms. The main purpose of these algorithms was to create a strong algorithm that is valid in terms of low processing length and long processing time with high series. And thus their algorithm has been compared and shown good results to the previous algorithm. In 2016 K. Ganeshkumar et.al [3] has developed a new cryptographic based algorithm using fuzzy communication logic. At first, the errors caused to the proposer's hack during data transfer over the network were understood. Then it was corrected and no data was lost. Their concept was based on the encryption of text data using cryptographic fuzzy which provides high accuracy data transfer. In several cases, the previous algorithm was nodded for hidden rather than complex communication. Thereupon the result was eventually contrasted with the algorithm that is currently in use by researchers. Kamilah Abdullah et al. in 2017. [4] gave key importance to communication as it failed to address protection, this was replaced by an RSA Cryptosystem implementation concentrating both on communications and security. RSA was developed by a fuzzy set theory. For the encryption and decryption algorithm, they used triangular fluid numbers. RSA's cryptosystem hackers have been faced with difficulties in generating and decrypting encryption, which allows RSA's cryptosystem more safe communications.

2017 M. Ethiopia et.al. [5] said the art of science includes the concepts and methods for turning a message into an intelligible message and redevelops it in its original form, to provide greater stability. The goal was to create a simple, real, and secure system, which can be accomplished by implementing software. A fuzzy logical approach to incorporate the encrypted message was included in your message. 2018 P. Amudha and.al. [1] Ciphers are said to have been transformed into secret communication maps. Because OF its different features and its simple matrix representation in a computer, the field of graph theory was commonly used as an encryption method. They practiced the use of cryptography graph theory. In this paper, a double encryption and decryption algorithm (lock to a locker method) is implemented for the development of new algorithms. Data cannot be hacked without the protection formula. The main objective of this article is to eliminate data consistency in data transmission unless the security formula is understood. The algorithm can't transfer safer data and it is not possible to modify the data communications. In this paper, we have proposed a key exchange based Dual Secure Cryptographic Measures by Two-Phase Locking Protocol (DSCM-TPLP).

II. RELATED WORK

Smart grid for the future energy system [10, 11, 26] and the newly-established electrical network which relies on two approaches to digital communication between the user and provider systems in an intelligent way to enhance reliability, performance. The main work focuses on the intelligent grid are communication, security, and management infrastructure. The intelligent grid supports advanced information control networks, energy generation, transmission and use, advanced measurement technology, and technology of communication. The smart grid safety infrastructure offers protection against eavesdropping, system breakdown, reliability analysis, privacy, and security. The intelligent grid network needs physical resources to be incorporated into the cyber system. The implementation of the cyber grid network makes the system more energy-effective and modern, while its crests are also the setting in which many cyberattacks are likely to be harmful [12] to national facilities, customer service, and health.

Interoperability between the transmission network and the end to end should be efficient and safe two-way communication with adequate bandwidth and low latencies needed to produce, transfer, distribute, and consume energy for intelligent grid infrastructure. High-level system monitoring is required to provide reliability and stability to prevent cyber-attacks from transforming the network to make it robust. To be stable and usable, efficient, reliable infrastructure, quality-of-service, scalability, critical times, network latency, time syncing, multicast support, and critical data delivery are necessary as an important issue.

In addition to regulatory and policy initiatives, the structures relating to the intelligent grid infrastructure and architecture should be strong and stable. The Supervise Control and Data Acquisition (SCADA) security should be one of the most relevant secret files. It operates with encrypted signals and offers remote device control based on network computers. Public Key Infrastructure (PKI) [13, 27] is used by a range of systems to ensure that smart grids secure and respond to the hardware and software protection problems by authenticating, checking, identifying and validating linked network access meters. It is leveraged for securing revenue streams, service continuity, and data integrity.

Encryption and encryption now provide encrypted correspondence, and secret sharing, identification, and authentication for a few days. AES algorithm is commonly used to encrypt and decrypt data encryption algorithm. For the cryptography perspective, it is important to analyze cryptographs in which the key value is decrypted in a trial-based process. It is like a cryptographic split with a speed greater than an attack by brute force. This split from existing technology is the unfeasible consequence. Often theoretical breakdowns may provide intuition rather than realistic knowledge on vulnerability trends [28].

The well-known and effective brute force attack against the 64 bit algorithm of RC5 has been widely used and applied with a block cipher encryption algorithm. For all additional bits, the main keyspace is expanded by a factor of two. It also doubles the average brute strength search slot if the key has an appropriate value for every choice. The technique of brute force search implies that this is exponentially useful when extending the key size. The ciphers are fragile and cannot tell us whether broad key lengths would prove effective against many kinds of cryptographic attacks. They have very long key values.

III. TWO-PHASE LOCKING PROTOCOL

The 2-phase commit protocol (2PC) is the type of Atomic Engagement Protocol (ACP) for transaction processing, databases, and computer networking. It is a distributed algorithm which co-ordinates all the processes involved in a distributed atomic transaction on whether the transaction is committed or aborted (rollback). Even in many cases (including either the process, network node, communication, etc.) the protocol achieves its goal and is therefore widely used. This Protocol calls for the mutual access of all data items [27]. This means that no other transaction should interrupt the same object if one transaction is executed. A two-phase lock-up agreement will be enforced if two-phase lock-outs can be carried out. New locks can be acquired in the Growing Phase on data items, but none can be released while the existing locks may be released in Shrinking Phase, however, no new locks may also be acquired [28, 32].

IV. THE ADVANCED ENCRYPTION STANDARD

The AES [14, 15] is one of the famous National Institute of Standards and Technology (NIST)'s encryption and decryption algorithm and is originally named for Rijndael [16] in 2001. It is developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen and is based in the Rijndael cipher algorithm. During the AES selection process, they sent a proposal to NIST [17]. Rijndael is a cipher family of different block sizes and key sizes. The symmetric encryption method is more common and widely applied. DES and three-fold DES have shown to be at least six times quicker. The main size of the DES algorithm was very limited and the algorithm had to be replaced because the computing power of the hardware was increased. It was deemed vulnerable to comprehensive key size attacks. The generation of AES and mixed column transition is shown in Figure. 1. The following features are present in AES [18, 19, 30].

- *Used by symmetric block cipher and symmetric key algorithms.*
- *Having block* $\mathbf{128}$ *bits and key size* $\mathbf{128/192/256}$ *bit long.*
- *Much faster and robust than Triple DES.*

- *Provides a complete design pattern and specifications.*
- *The software and hardware implementable of the algorithm are possible in C, Java, and HDLs respectively.*

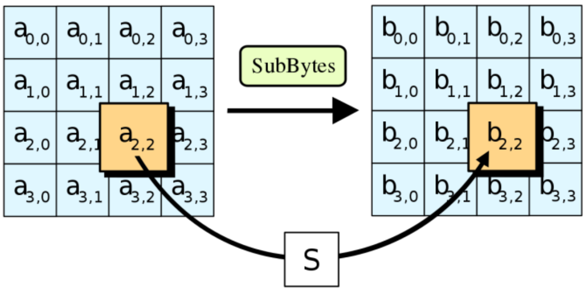

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

Figure 1. Mixed column transition in AES

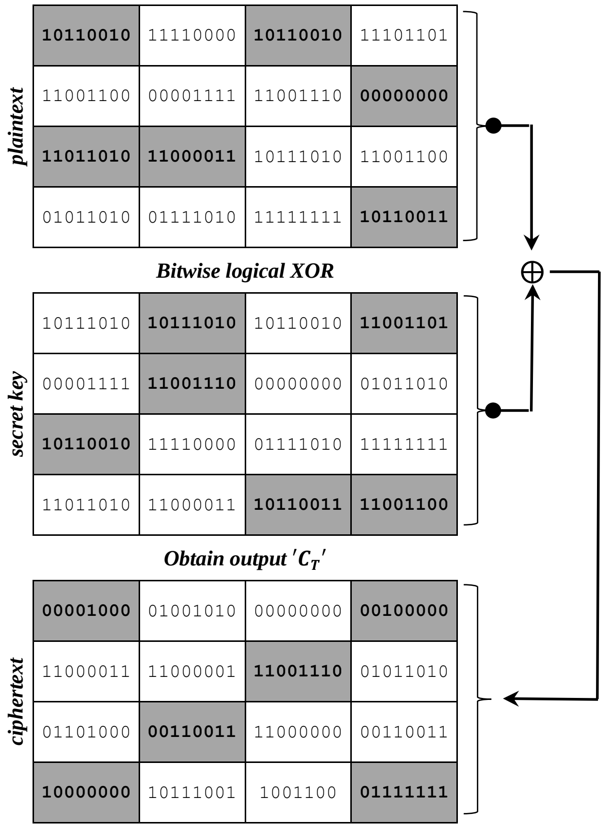
The AES algorithm is a technique based on a substitution and permutation principle rather than an iterative technique of Feistel network cipher. It is comprised of different series of connected sub-operations, some involving the replacement of inputs using similar replacement outputs, and others include permutations or shuffling. Instead of bit operation, the AES algorithm works on byte manipulations. If the plaintext size is **128** bits, AES can process it as **16** bytes. Afterward, all **16** bytes in the column matrix (**4 9 4**) are organized in the row shape. The AES round numbers depend on the key length and are variable. The scale of the main bit (**128/ 192/256**) takes **10** rounds, **12** rounds, and **14** rounds for AES [20, 21]. The entire round is followed by a **128**-bit round key and is computed using the old values.

Encryption: The definition of the rounding method in AES encryption is not discussed in detail. There are **4** sub-processes in every AES round. The first round is defined as information.

Byte Substitution (Sub Bytes): The AES algorithm has six bytes that are replaced by the design-listed fixed table matrix (S-box). The matrix (**4, 9, 4**) is made up of four columns and rows is shown in Figure 2.

Shift Rows: Matrix is shifted to the left side of each row. The drop-off entry is reinserted from the right-hand side after moving. The change is performed accordingly [29].

- *No first-row shifting.*
- *Second row will take the left-shift operation, and contents will be transferred to one-byte location.*
- *Two-byte locations move the third row to the left in the same way.*
- *Three-byte positions move the fourth row to the left.*
- *The shifting produces a new matric.*
- *The result is an all **16** bytes matrix that has been moved from one matrix to another.*



10110010	11110000	**10110010**	11101101
11001100	00001111	11001110	**00000000**
11011010	**11000011**	10111010	11001100
01011010	01111010	11111111	**10110011**

10111010	**10111010**	10110010	**11001101**
00001111	**11001110**	00000000	01011010
10110010	11110000	01111010	11111111
11011010	11000011	**10110011**	**11001100**

00001000	01001010	00000000	**00100000**
11000011	11000001	**11001110**	01011010
01101000	**00110011**	11000000	00110011
10000000	10111001	1001100	**01111111**

Figure 2. Byte substitution in model DSCM-TPLP

Mix Columns: The special arithmetic function is used for every column with **4** bytes. The function accepts these four bytes as an input in one column and gives the original column to four new bytes as outputs. A new matrix consisting of **16** new bytes is created in this manner. It is necessary to remember that in the last round this move is not taken.

***Add round key*:** The matrix consists of **16** octets, **128** bit, and XOR [22, 23] is taken with a **128** bit round key. The result is the last round cipher file. The resulting **128** bits would otherwise be called **16** bytes and we can continue a similar round again.

V. PREREQUISITES TOOLS OF DSCM-TPLP

This section includes the notation for encryption of fuzzy subsets and ASCII upper cases for alphabets.

Definition 2.1: Mathematically a graph $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$, is a set of vertices and edges whereby $\boldsymbol{V}$ is the same set whose element is called vertices and $\boldsymbol{E}$ is a set of dual-sets (sets of two distinct elements) of vertices, whose elements are called the edges of vertices. The $\boldsymbol{x}$ and $\boldsymbol{y}$ vertices of the $\{\boldsymbol{x}, \boldsymbol{y}\}$ edge are called edge terminals. The edge will be $\boldsymbol{x}$ and $\boldsymbol{y}$, and $\boldsymbol{x}$ and $\boldsymbol{y}$ event.

Definition 2.2: A fuzzy set $\boldsymbol{X}$ over a set $\boldsymbol{S}$ is defined by the function $\boldsymbol{f}: \boldsymbol{S} \to [\boldsymbol{0}, \boldsymbol{1}]$ is referred to as the membership function and is represented as $\boldsymbol{X} = (\boldsymbol{S}, \boldsymbol{f})$.

Definition 2.3: A fuzzy subset over a universe of discourse $\boldsymbol{S}$ is defined as a mathematical mapping that creates an object which is generalized as a membership function $\mu(\boldsymbol{f}): \boldsymbol{S} \to [\mathbf{0}, \mathbf{1}]$.

Definition 2.4: Crisp sets are the sets most of our lives have been using. Either an element is a part or not in a crisp set. For instance, a jelly bean belongs to the food class called candy. Potatoes mashed don't. On the other hand, fuzzy sets allow elements to belong partially in a set. Due to this reason, the crisp set is more often used.

Definition 2.5: Cryptography is the art of data security by converting it (encrypting), which is called ciphertext, into an unreadable format. Only those with a coded key may decode the message into plain text (or decrypt it).

Definition 2.6: Encryption is the mechanism by which data is transformed into code, in particular, to avoid unauthorized access. The key difference between secrecy and secret writing is that secrecy is that converting an unintelligible document is indescribable until it is decrypted. Though Hidden Writing is the first encrypted information retrieval document.

Definition 2.7: Decryption is the process of converting into its original form of encrypted data. It is typically an inverse encryption operation. It is called the decryption when the encrypted data are translated into its original form. It is typically an inverse encryption operation. It decodes encrypted information to decode the data from an authorized user only because a secret key or password is needed for decryption.

Definition 2.8: Binary is a number of the base $\mathbf{2}$ number system or a binary system of two symbols only: the "$\mathbf{0}$" (null) symbols and the "$\mathbf{1}$" symbols. The number base $\mathbf{2}$ method is a radius notation of $\mathbf{2}$.

Definition 2.9: The most common form for text files on computers and the Internet is ASCII (American Standard Code for Information Exchanges). The ASCII file represents a 7-bit (**7 0**s or **1**s) binary number (string) for every alphabetic, numeric and special character. There are specified $\mathbf{128}$ potential characters. ASCII values vary between $\mathbf{97}$ and $\mathbf{122}$, and between $\mathbf{65}$ and $\mathbf{90}$ for the upper case.

VI. PROPOSED MODEL DSCM-TPLP

The main aim of this paper is to use an encryption method to improve the protection of an existing cryptosystem. As an improved cipher, we suggest a "two-step model of encryption." This contains three fundamental encryption methods: uncertainty, diffusion, and drug. In user authentication and resource sharing applications, the two phases of encryption are used to provide a secure service. If an environmentally friendly security system is affected and claims the cryptosystem to be able to withstand the selected plaintext attack, then we may use the two-phase cryptography addressed in this article to increase the security of the cryptosystem. It must therefore only use the cryptosystem, to resist the attack by the known-plaintext, to resist the attack by the selected plaintext. It, therefore, improves the security, economic, and practicality of the original application framework. We offer a two-phase database system encryption algorithm. The system allows the encryption and decryption of fields in a database by writing and reading sub key bodies of fields, as a data-oriented cryptosystem. In the subkey scheme, two simple strategies are proposed to solve the key management problem.

A. Dual Secure Encryption

Step 1: Let us suppose the ordered pair $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ denotes an uppercase alphabet letter whose ASCII ranges from $\mathbf{65}$ to $\mathbf{90}$ such that the value of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are two distinct integers are shown in Table 1.

Table 1. Order pair of membership function $\mu(\boldsymbol{\alpha}, \boldsymbol{\beta})$

(a, b)	$\boldsymbol{C}(\mathbf{67})$	$\boldsymbol{O}(\mathbf{79})$	$\boldsymbol{M}(\mathbf{77})$	$\boldsymbol{P}(\mathbf{80})$	$\boldsymbol{U}(\mathbf{85})$	$\boldsymbol{T}(\mathbf{84})$
$\boldsymbol{C}(\mathbf{67})$	A	B	C	**D**	E	**F**
$\boldsymbol{O}(\mathbf{79})$	G	**H**	I	J	K	L
$\boldsymbol{M}(\mathbf{77})$	**M**	N	O	P	Q	**R**
$\boldsymbol{P}(\mathbf{80})$	S	**T**	U	**V**	W	X
$\boldsymbol{U}(\mathbf{85})$	Y	**Z**	0	1	2	3
$\boldsymbol{T}(\mathbf{84})$	4	5	**6**	7	8	**9**

Containing the same digits (such as $\mathbf{57}$ and $\mathbf{75}$) or a two digits palindrome number. The range provided by the doublet $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is assigned to a letter of the uppercase alphabet and digits ranging from **0** to **9** randomly [31].

Step 2: Based on the outcome of the order pair value, a membership value of each mapping is obtained and has tabulated in Table 2. Again the results of this ordered pair $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ have associated with the fuzzy membership function μ such that $\mu: \{\boldsymbol{\alpha}, \boldsymbol{\beta}\} \to \{\mathbf{0}, \mathbf{1}\}$ under the correspondences [25, 32]:

$$\mu(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \frac{\mathbf{100}\boldsymbol{\alpha} + \boldsymbol{\beta}}{\mathbf{88000}}$$

Table 2. Obtained crisp value of membership function $\mu(\boldsymbol{\alpha}, \boldsymbol{\beta})$

$(\boldsymbol{a}, \boldsymbol{b})$	$\boldsymbol{C}(\mathbf{67})$	$\boldsymbol{O}(\mathbf{79})$	$\boldsymbol{M}(\mathbf{77})$	$\boldsymbol{P}(\mathbf{80})$	$\boldsymbol{U}(\mathbf{85})$	$\boldsymbol{T}(\mathbf{84})$
$\boldsymbol{C}(\mathbf{67})$	0.07690	0.09053	0.08826	0.09167	0.09735	0.09622
$\boldsymbol{O}(\mathbf{79})$	0.07703	0.09067	0.08840	0.09181	0.09749	0.09635
$\boldsymbol{M}(\mathbf{77})$	0.07701	0.09065	0.08838	0.09178	0.09747	0.09633
$\boldsymbol{P}(\mathbf{80})$	0.07705	0.09068	0.08841	0.09182	0.09750	0.09636
$\boldsymbol{U}(\mathbf{85})$	0.07710	0.09074	0.08847	0.09188	0.09756	0.09642
$\boldsymbol{T}(\mathbf{84})$	0.07709	0.09073	0.08845	0.09186	0.09755	0.09641

And the value of fuzzy membership value of μ is obtained as listed in Table 2. It is noted that the Fuzzy membership value $\mathbf{0.00000}$ is presumed as an outcome of empty space.

Step 3: By using the following getRand method, a positive random number is obtained and is converted into their equivalent binary representation. Suppose the random binary value of function getRand is represented by the variable/symbol $\boldsymbol{R\_bin}$ (a random binary number).

```
public static double getRandom(){
   double rand = Math.random();
   return rand;
}
public static String toBinary(int R_int) {
   String to_bin="";
   int[] bytes = new int[1000];
   int i = 0;
   while (R_int > 0){
       binaryNum[i] = R_int % 2;
       R_int = R_int / 2;
       i++;
   }
   for (int j = i - 1; j >= 0; j--){
        to_bin += bytes[j];
   }
   return to_bin;
}

public static double getBR(double MIN, double
                                       MAX){
   double rand= getRandom();
   double bounded_rand=(int)rand*()*((MAX-
                    MIN)+1))+MIN;
   return bounded_rand;
}
```

Step 4: at this stage, we multiply the number $\boldsymbol{R\_bin}$ with the outcome of the fuzzy membership number that provides much secrecy, robustness, and ambiguity to the encrypted message.

Step 5: in this step, we have run reverse engineering of crisp value to obtain the binary representation of the same. This reverse engineering protects the cipher from several cryptographic attacks like correlation attack, linear masking attack, guess, and determine attack and correlation attack [24].

B. Dual Secure Decryption

Step 1: First we will convert the obtained binary number into their equivalent crisp value closed under the same universe of discourse.

Step 2: At each pass of the loop, the obtained crisp value gets divided by the same random number $\boldsymbol{R\_bin}$ so that the range of '$\boldsymbol{r}$', where $\boldsymbol{r}$ belongs to [0, 1] is obtained.

Step 3: Further at this point, by using the decryption algorithm as the round of two decimal places, the value of $\boldsymbol{r}$ if defuzzified.

C. Numerical example

In this section, we have discussed the simulation result of the proposed algorithm with some variant length plaintext and obtained ciphertext.

- ***The encryption*** | $\boldsymbol{C_T\ e(P_T, KEY)}$

Let's suppose a $\mathbf{25}$ characters plaintext ***"Aligarh Muslim University",*** I have to encrypt this message using the "**343243esdsvdgfd24**". The process of encryption are as follows:

Step 1: first find the corresponding membership value of each character belonging to the plaintext message like ***A=0.08238, L=0.02015, I=0.18360,*** …., and so on. So the corresponding membership values of the phrase is:

token[0]	**A**	~	0.08238	~	0010000000101110
	L	~	0.02015	~	0000011111011111
	I	~	0.18360	~	0100011110111000
	G	~	0.11015	~	0010101100000111
	A	~	0.32560	~	0111111100110000
	R	~	0.34001	~	1000010011010001
	H	~	0.22890	~	0101100101101010
token[1]	**Φ**	~	0.23750	~	0101110011000110
token[2]	**M**	~	0.18138	~	0100011011011010
	U	~	0.12314	~	0011000000011010
	S	~	0.58869	~	1110010111110101
	L	~	0.21010	~	0101001000010010
	I	~	0.42564	~	1010011001000100
	M	~	0.13000	~	0011001011001000
token[3]	**Φ**	~	0.02130	~	00000100001010010
token[4]	**U**	~	0.81012	~	10011110001110100
	V	~	0.19860	~	00100110110010100
	I	~	0.90014	~	10101111110011110
	V	~	0.70067	~	10001000110110011
	E	~	0.71002	~	10001010101011010
	R	~	0.41030	~	01010000001000110
	S	~	0.08010	~	00001111101001010
	I	~	0.12060	~	00010111100011100
	T	~	0.19008	~	00100101001000000
	Y	~	0.91063	~	10110001110110111

Figure 3. Tokens truncate and membership convertor

Here the symbol $\boldsymbol{\Phi}$ represents a white space character. It's noted that the crisp value of two identical white space characters is not the same. This makes the cipher more robust against any guess and determines attack.

Step 2: Truncate the fractional part of the crisp value and convert them into equivalent binary numbers as shown in Figure 3.

Step 3: In order to achieve "**3*4bJ3A5h4%b!**" security of the encrypted plaintext ***"Aligarh Muslim University",*** the hexadecimal representation of the ciphertext is shown in Table 3.

Table 3. Simulation result of the proposed model

PLAINTEXT	CIPHERTEXT
Aligarh Muslim University	202e7df47b82b077f3084d1596a5c c646da301ae5f55212a64432c8852 13c744d9415f9e111b31155aa0461 f4a2f1c4a40163b7
a random run	c03052805a3001e31e150c001e31e 1146031e3001ef0005462a150121e 002466090
@*&^%$+=0`!!?/;:'###	c1200484500c1200302281201140c 600021c054828720001822833c
encryption	c28f528b15b001ae5f505d94a146c2

Implementation of function *doEncrypt* is as follows:

```
public static String doEncrypt(String
                  strToEncrypt, String KEY) {
    try{
       setKey(KEY); Cipher cipher =
Cipher.getInstance("AES/ECB/PKCS5Padding");
       cipher.init(Cipher.ENCRYPT_MODE,
secretKey);
    return Base64.getEncoder().encodeToString
    (cipher.doFinal(strToEncrypt.getBytes("UTF-
8"))); }
    catch (Exception e) {
       System.out.println("Error while
encrypting: " + e.toString());
    }
    return null;
}
```

- ***The decryption*** **|** $\boldsymbol{P_T\ d(C_T, KEY)}$

Decryption is the process of reverse engineering of the obtained ciphertext to get the same plaintext. The steps involved in this process is as follows:

Step 1: Convert the binary number to crisp number and then dividing each crisp number by 100000 we get:

0.07710	0.08838	0.08841	0.0000	0.08826
0.07690	0.09065	0.0000	0.09750	0.08840
0.09065	-	-	-	-

Step 2: Using the decryption formula 88000r (round of to two decimal places) we get,

67.85	77.77	77.80	00.00	77.67	67.67	79.77
00.00	85.80	77.79	79.07	7.85	27.87	79.80
97.80	12.75	47.80	-	-	-	-

The corresponding decrypted alphabet from the fuzzy membership vector is ***"Aligarh Muslim University".***

Implementation of function* doDecrypt *is as follows:

```
public    static    String    doDecrypt(String
strToDecrypt, String KEY) {
        try {
            setKey(KEY); Cipher cipher =
  Cipher.getInstance("AES/ECB/PKCS5PADDING");
            cipher.init(Cipher.DECRYPT_MODE,
            secretKey);
            return new String(cipher.doFinal

(Base64.getDecoder().decode(strToDecrypt)));
        }
        catch (Exception e) {
            System.out.println("Error while
            decrypting: " +e.toString());
        }
        return null;
}
```

VII. CONCLUSION

The paper present a *Fuzzy membership function* based double encryption algorithm for fixed length plaintext encryption. *The proposed algorithm is based on two-phase locking protocol.* As suggested by the result (refer to Table 3), the algorithm seems to be more secure and fast for encrypting bulk data in two-phase locking mode for both software and hardware platform. The model is fairly implemented and considered to be secure and resistant to a variety of cryptographic attacks. It has become secure and tends to achieve better results by comparing the number of *clock cycles, processing time, output, efficiency, and bits per cycle*. After a comprehensive theoretical attack immune analysis, it has found that the cipher can withstand with many cryptographic attacks like *guess-and-determine attacks, algebraic attack, side-channel attacks, the time-memory trade-off with huge precomputation, correlations attack and linear masking attack*. For future research, we inspired to explore some other approach.

Conflict of interest: *The authors declare no conflict of interest regarding this work.*

ACKNOWLEDGMENT

I would like to pay my sincere thanks and gratefulness to my academic advisor ***Dr. Aasim Zafar,*** whose constant encouragement and support acted as an impetus for working hard and completing this paper with sincerity. Also, *I would like to pay my heartiest gratitude to my family and my alma mater Aligarh Muslim University for their unforgettable support whenever I needed it.* There are no words that can express gratitude for their love, affection, and patience. They always stood by my side, had faith in my work, and always prayed for my success.

REFERENCES

[1] P. Amudha, A.C. Charles Sagayaraj A, C.ShanthaSheela,"*An application of Graph theory in Cryptography*", International Journal of Pure and Applied Mathematics, 119(13), 375-383, 2018.

[2] Anita Pal, National Institute of Technology Durgapur West Bengal-713209, India.

[3] K.Ganeshkumar, D.arivazhagan, et.al,'*New Cryptography Algorithm with Fuzzy logic for Effective Data Communication*'. International journal of Science and tech. vol 9(48), DOI: 10.17485 /ijst/2016/v9i48/108970, Dec 2016.

[4] Kamilahabdullah. Sumarni Abu Baskar, Nor Hanimakamis, and Harialimais, '*RSA cryptosystem with Fuzzy set Theory for encryption and decryption*', AIP conference Proceeding 190, 030001(2017), volume 950, Issue 10.063/1.5012147.

[5] M. Muthumeenakshi, T. Archana, P. Muralikrishna,"*Fuzzy Application in Secured Data Transmission*", International Journal of Pure and Applied Mathematics, 116(3), 711-715, 2017.

[6] Ravindumadanayake, et.al, '*Advanced Encryption Algorithm Using Fuzzy Logic*", International Journal of Computer networks ((ICICN 2012) IPCSIT vol 27(2012) IACSIT Press), Singapore.

[7] S.Shara et. al. on "*RSA algorithm using modified subset sum Cryptosystem,*" in computer and commTech. (India, 2011) pp. 457-461.

[8] L.A.Zadehand R.RYager et al. (John Wiley, New York, 1987). "*Fuzzy Sets and Applications* :"

[9] L.A Zadeh, information And control, vol. 8, 338- 353(1965)

[10] Bari A, Jiang J, Saad W, Jaekel A (2014) *Challenges in the smart grid applications: an overview*. Ataul Hindawi Publishing Corporation. Int J Distrib Sensor Netw 974682:11. https://doi.org/10.1155/2014/974682.

[11] Fadel E, Gungor VC, Nassef L, Nadine A, Abbas Malik MG (2015) "*A survey on wireless sensor networks for smart grid.*" Comput Netw Elsevier 71:22–33

[12] Wang W, Lu Z (2013) "*Cyber security in the smart grid: survey and challenges.*" Comput Netw 57:1344–1371.

[13] Guo X, Liu Z, Xing J, Fan W, Zou X (2006) "*Optimized AES crypto design for wireless sensor networks with balanced S-box architecture:*" In Proceedings of International Conference on Informatics and Control Technology (ICT 2006). pp 203–208.

[14] Deshpande AM, Deshpande MS, Kayatanavar DN (2009) *"FPGA implementation of AES encryption and decryption*." In: International conference on control, automation, communication and energy conservation (INCACEC 2009). IEEE, pp 1–6.

[15] Hodjat A, Verbauwhede I (2006) "*Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors.*" IEEE Trans Comput 55:366–372.

[16] Daemen J, Rijmen V (2013), "*The design of Rijndael: AES-the advanced encryption standard.*" Springer, Berlin.

[17] Daemen J, Rijmen V (2005) Rijndael/aes. In: van Tilborg HCA (ed) "*Encyclopedia of Cryptography and Security.*" Springer, US, pp 520–524.

[18] Hammad I, Sankary KE, Masry EE (2010) "*High-speed AES encryptor with efficient merging techniques.*" IEEE Embed Syst Lett 2(3):67–71.

[19] Dyken JV, Delgado-Frias JG (2010) "*FPGA schemes for minimizing the power-throughput trade-off in executing the advanced encryption standard algorithm.*" J Syst Architect 56(2–3):116–123.

[20] Sklavos N, Papakonstinou A, Koufopavlou STO (2002) *Low-power implementation of an encryption/decryption system with asynchronous techniques*. VLSI Design 15(1):455–468.

[21] Priya SS, Karthigaikumar P, Siva Mangai NM. et al. (2017) "Wireless personal communication." 94: 2259. doi: https://doi.org/10.1007/s11277-016-3385-7.

[22] Good T, Benaissa M (2006) "*Very small FPGA application-specific instruction processor for AES*." IEEE Trans Circ Syst I Regul Pap 53(7):1477–1486.

[23] Zhang X, Parhi KK (2004) "*High-Speed VLSI architectures for the AES algorithm*." IEEE Trans Very Large Scale Integr VLSI Syst 12(9):957–967.

[24] Li, Chaoyun, and Bart Preneel. *"Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree.*" International Conference on Selected Areas in Cryptography. Springer, Cham, 2019.

[25] Shabbir Hassan, Prof. M. U. Bokhari, presented a paper entitled *"Lightweight Cryptography: A Review", Recent Trends in Mathematical and Computational Science (NCRTMCS),* January 2015, pp-78.

[26] Shabbir Hassan and Mohammad Ubaidullah Bokhari. "*Computing in Cryptography.*" 2016 3rd International Conference on Computing for SustainableGlobal Development (INDIACom). IEEE, 2016. ISSN 0973-7529; ISBN 978-93-80544-20-5.

[27] Shabbir Hassan, M.U. Bokhari and Md. Zeyauddin. "*Radio Frequency Identification Tag: A Review.*" 2017 4th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2017. ISSN 0973-7529; ISBN 978-93-80544-24-3

[28] Bokhari, M. U., and Shabbir Hassan. "*A comparative study on lightweight cryptography."* Cyber Security. Springer, Singapore, Cyber Security, Advancesin Intelligent Systems and Computing 729. 2018. 69-79. https://doi.org/10.1007/978-981-10-8536-9_8

[29] Hassan, Shabbir and Mohammad Ubaidullah Bokhari, (2019), "*Analysis and Design of LFSR Based Cryptographic Algorithm.*" Journal of Advances and Scholarly Researches in Allied Education (JASRAE), ISSN 2230-7540, Vol. 16, Issue No. 9, June-2019.

[30] Hassan, Shabbir and Mohammad Ubaidullah Bokhari, *"Design of Pseudo Random Number Generator using Linear Feedback Shift Register.*" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

[31] Prof. M. U. Bokhari, Shabbir Hassan, 2020, *"Design of a Lightweight Stream Cipher: BOKHARI" 256,* International Journal of Engineering Research & Technology (IJERT) Volume 09, Issue 03 (March 2020).

[32] Shabbir Hassan. "*The Implication of Deep Neural Networks in Solving Optimization Problems for Network Security."* International Journal of Computer Applications 176(20):6-13, May 2020.

Author's Profile

Mr. Shabbir Hassan is a *Sun Certified Java Programmer (SCJP),* currently working as Assistant Professor at Centre For Distance Education, Aligarh Muslim University (AMU), Aligarh. He holds a Master in Computer Science and Applications (MCA) and currently pursuing Ph.D. at the Department of Computer Science, Aligarh Muslim University. His thrust area is "*Analysis and Design of Lightweight Stream Cipher*" and area of interest include Applied Mathematics, Analysis, and Design of Algorithms, Dynamic Programming, Network Security and Cryptography. He has qualified UGC-National Eligibility Test (NET) and has availed Junior Research Fellowship (JRF) during the Research Work. Throughout his career, he has been involved in innovative Software Development and Academic Teaching of Computer Science subjects like *C, JAVA, Python, Data Structure, Operating System, Automata Theory, and Computer Networks.* He has presented his research work in several National and International IEEE Conferences and marked his active participation in many Conferences, Workshops and Symposia. His research papers have published in many reputed peer-reviewed Journals of International repute like *Springer, Elsevier, JASRAE, IJEAT, IJERT, IJCA, InderScience* and *SCOPUS Indexed Database.* Apart from the Academic Research and Software Development, he is enriched with the passion of poetry and philosophy and engages himself in social work.