Enhancement of Data Security on Transmission Network Using Fuzzy Logic

Onwughalu, M.K, Ogwata, C.M

Department of Electrical/Electronic Engineering Technology, Federal Polytechnic Oko, Anambra State

Abstract- Security of data is an important factor in data transmission through network. This paper proposed a new method using fuzzy set theory to enhance the security. The data in the form of text to be transmitted is encrypted by using the AES Rijndael algorithm. The encryption algorithm is the mathematical procedure for performing encryption of data. A key is used to cipher a message and to decipher it back to the original message. Then the scrambled encrypted text is converted into numeric form by applying the fuzzy set theory. The fuzzy logic provides the text in the zero to one value. These numerical values before decryption are again converted into scrambled text. if the key provided by the user is the same key that is used for the encryption then original data will be retrieved. The paper, integrates the encryption of text and conversion of the unscrambled text from numerical to original by using fuzzy logic.

Index Terms- Fuzzy logic, Fuzzy set theory, Encryption, AES Rijndael Algorithm.

I. Introduction

Fuzzy logic is a problem solving control system methodology that lends itself to implementation in systems ranging from simple, small, embedded microcontrollers to large,networked, multi-channel pc (or) workstation-based data acquisition and control systems. It can be implemented in hardware, software (or) a combination of both. Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, and noisy (or) missing input information Fuzzy sets and fuzzy logic are powerful mathematical tools for modeling and controlling uncertain systems in industry, humanity and nature they are facilitators for approximate reasoning in decision making in the absence of complete and precise information [1]. The basic concept underlying fuzzy logic is that of a linguistic variable.

A variable whose values are words (or) sentences in natural (or) artificial languages are called linguistic variables. Fuzzy sets are a generalization of classical sets and infinite valued logic is a generalization of classical logic. There is also correspondence between these two areas.

Network Security is becoming more and more crucial as the volume of data being exchanged on the internet access [2]. Based on the above, the security involves four important aspects: Confidentiality, message authentication, integrity and non – repudiation. Popular application of multimedia technology, and increasingly transmission ability of network gradually leads us to acquire, information directly and clearly through various methods. In cryptography, public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely [3]. However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. Cryptography is the process of transforming plain text into unintelligible form called the cipher text. The technology of the encryption is called cryptology[4]. In this paper the text encryption is based on the symmetric key algorithm where both the encryption and the decryption keys are the same. Symmetric cryptography refers to encryption methods in which both the sender and receiver share the same key.

II. Review

Related work done on fuzzification and its result shows that security problem involving computer based systems are getting more frequent for security attention. The number and variety of attacks by person and malicious software from outside organization, particularly and consequences of inside attacks also remain a major concern.

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electrical commerce

Public key cryptography is a fundamental and widely used technology around the world. It is the approach which is employed by many cryptographic algorithms and cryptosystems. Public-key algorithms are most often based on the computational complexity of hard problems often from number theory[5] Most of the users do not have the required resources for the communication. Current algorithms which are available for the encryption either takes high processing time and not secure enough to help the limited bandwidth

The encryption algorithm is an integral work of data encryption and decryption process. They should preserve high security to the data transmitted. Basically, encryption algorithms are divided into three major categories transposition, substitution and transposition-substitution technique [6].

III. Background

Security is the main problem in the modern data communication. There are a lot of cyber-crimes have arises with the development of technology. Cryptography consists of cryptology and crypto analysis. Encryption comes under cryptology. In this paper the text encryption is based on the symmetric key algorithm where both the encryption and the decryption keys are the same

AES Rijndael Algorithm

The encryption algorithm is an integral work of image encryption and decryption process. They should preserve high security to the image transmitted. Rijndael algorithm is one of the AES (Advanced Encryption Standard) algorithms, used for text encryption technique. It is a block cipher algorithm, in which the block means the information to be encrypted is divided into blocks of equal length, It is an iterated block cipher, with a variable block length and variable key length.

AES Rijndael Algorithm Operations:

- Describe the set of rounds keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth final round of state manipulation.
- Copy the final state array and as the encrypted data (cipher text)

Fuzzy set theory

Fuzzy set theory is an extension of classical set theory where elements have varying degrees of membership. A logic based on the two truth values True and false is sometimes inadequate when describing human reasoning [7]. Fuzzy logic uses the whole interval between 0 (false) and 1 (True) to describe human reasoning. A fuzzy set is any set that allows its members to have different degree of membership function in the interval [0,1].The degree of membership (or) truth is not same as probability [5]. Fuzzy truth is not likelihood of some event (or) conditions. The fuzzy truth represents membership in vaguely defined sets.

IV. Methodology

Symmetric key cryptography refers to encryption methods in which both the sender and receiver share the same key (and, less commonly, in which their keys are different, but related in an easily computable way) [8]. The modern study of symmetric ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher take as input a block of plaintext and a key, and output a block of cipher text of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some better security in one aspect or another than others. They are the mode of operations which must be carefully considered when using a block cipher in a crypto system. Rijndael algorithm is one of the AES (Advanced Encryption Standard) algorithm used for data encryption technique. It is a block cipher algorithm in which the block means the information to be encrypted is divided into blocks of equal length. It is an integrated block cipher, with a variable block length and variables key lengths [9].

Internally, the AES algorithms operations are performed on a two dimensional array of bytes called the state. The state consists of four rows of bytes, where Nb is the block length divided by 32. The function of AES Rijndael is as follow

i. SubBytes Transformation: The sub Bytes () Transformation is a non

-linear byte substitution that operates independently on each byte of the state using a substitution table.

ii. Shift Rows Transformation: In the shift rows () Transformation, the bytes in the last three rows of the state are cyclically shifted over different number of bytes. The first row will not get shifted.

Iii. Mix Column Transformation: In mix column () Transformation. The columns of the state are considered as polynomial and then multiplied by modulous with fixed polynomial individually.

iv. Add Round Key Transformations: In the Add Round Key () Transformation, a round key is added to a state by a simple bitwise XOR operation. Each round key consists of Nb words from the key schedule those Nb words are each added into the columns of the state.

Encryption and Fuzzification

The secret evaluation on communication between various networks is concerned with the working effect of secret regulatory authorities and with the economic interests of the evaluated objects. The quality of the secrecy evaluation not only affects the message that is transmitted between the nodes. In the traditional process of encryption evaluation mainly studies the security system of evaluated enterprises by the findings. Finally, they evaluate enterprises on the basis of the total points. There are a lot of uncertainty and fuzziness in the course of this evaluation. Eg, the difficulty in quantifying the indexes. Therefore, the fuzzy set theory and method were introduced in the secrecy evaluation. It is the organic combination of quantitative and qualitative evaluation, so the secrecy censorship evaluation becomes more scientific and realistic.

Encryption of data using Matrix Transformation

A new method to transmit the data over the network is proposed. The communication involves the encryption of data before passing it to the receiver. For the data encryption the key is generated using the AES standard algorithm, which is symmetric. Then, store the encrypt file in the memory for comparing for later process. The matrix transformation is the next step in this process. For the matrix conversion the ASCII value of the encrypted text is considered. The conversion ends in the binary coded value which is in ones and zeros. After this step, get the encrypted data put into matrix formation, get the fuzzy membership matrix.

For the decryption of the text again the matrix transpose formation is created. The following steps are taken place in the decryption process to retrieve the encrypted data from the remote system, Convert the matrix with encrypted text into matrix transpose formation. The fuzzy evaluation score is now received. After the retrieval of the data the decryption process is taken place by use the symmetric key algorithm. This file is compared with the original data for processing. At the end of the process the original data can be retrieved and the data can be transferred between the users without any modification.

V. Results

The proposed system ends in the encryption and the fuzzification of the user defined text. The test result shows that the encrypted data have to be loaded, while the symmetric key for the text to be encrypted is given and saved. From the test result, it is discovered that the conversion as matrix took place after the encryption of the text. This matrix transformation provide the security and the authentication so that the intruders cannot able to know the transformation code of the text.

VI. Conclusion

In this paper, a symmetric cryptosystem is introduced, enhancing a new method to encrypt the user defined text that eliminates the random and man-made factors of secrecy evaluation to the maximum. It plays an important role in enrichment and development of multi-object evaluation technique, which raises the secrecy level. Each block of the data is encrypted using symmetric key rounds which then will also get the matrix conversion. This work is done using Rijndael cryptography symmetric algorithm for encryption/decryption. Hence the matrix form of data consists of only the binary values of the original data. This will eliminate the modification of the data by the intruders.

References

[1] Fuzzy Sets and Applications: Selected Paprs by L.A Zadeh, ed. R.R Yager et al. (John Wiley, New York, 1987).

[2] William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.

[3] Shafi Golgwasser Mihir Bellare, "Lecture Notes on Cryptography", July 2008. (Dhenakaran S.S and Kavinilavu, 2012).

[4] V.Potdar and E.chang,"Disguising text cryptography", International Network Conference in Plumouth, Uk, 6-9 July, 2004.

[5] Dhenakaran S.S and Kavinilavu N "A New Method For Encryption Using Fuzzy Set Theory", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.

[6] B.Gladman, "A Specification for Rijndael, the AES Algorithm", May 2003 http://fp.gladman.plus.com/cryptography_technology/Rijndael.aes.spec.311.pdf. accessed on 28 April, 2016.

[7] Le Luo, A method of quality evaluation of hydropower project based on fuzzy mathematics. Journal of Huazhong University of Science andTechnology (Natural Science Edition), 2004, 32(08); 82-84.

[8] Dr. Brian Gladman, Rijndeal (by Joan Daeman & Vincent Rijmen), "A Specification for the AES Algorithm", 15 April 2003.

[9] J.Daeman and V.Rijndael, http://www.esat.kuleven.ac. e/rijmen/rijndael/rijndael- v2.zip,1999 accessed on 28 April, 2016.

Authors

First Author – Onwughalu, M.K, Department of Electrical/Electronic Engineering Technology, Federal Polytechnic Oko, Anambra State
Second Author – Ogwata, C.M, Department of Electrical/Electronic Engineering Technology, Federal Polytechnic Oko, Anambra State