November-December 2019
ISSN: 0193-4120 Page No. 4750 - 4753

A Research on Application of Fuzzy Logic in Data Communication

Kavitha S
Assistant Professor, Department of Information Technology, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India. (E-mail: kavithasb26@gmail.com)

Anjana Dass
UG Scholar, Department of Information Technology, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India. (E-mail: anju11313@gmail.com)

Kiruthiga. J
UG Scholar, Department of Information Technology, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India. (E-mail: kiruthigaj18bit027@skasc.ac.in)

Article Info
Volume 81
Page Number: 4750 - 4753
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *23 December 2019*

Abstract:
In current scenario security is the most important problem in passing information from one point to another point. Missile codes, number bank accounts and encryption keys are the major areas which are facing the security issues. One may find a solution using the mathematical concept of Fuzzy Logic with the help of encryption algorithm. Also, affine transformation is used to encrypt the context. Implementation of cipher a message and decipher it back to the original message, can be intricate and caring data from unconstitutional access is the foremost difficulty. Integrity is also the main perception in data communication. In this paper, Advanced Encryption Standard (AES) algorithm is used to enhance the performance of encryption in data communication and this algorithm plays very important role in multimedia data transfer applications. The proposed system describes the Advance Encryption Standard (AES) algorithm to ensure both security and integrity in data communication.

Keywords: *Encryption, Security and Integrity*

I. INTRODUCTION

Fuzzy Logic has been used in various real time applications for multi objective optimization of power systems. It is a technique for representing and manipulating certain information. Information encryption means security. In ref [6] A Fuzzy Logic is utilized for encryption and mystery shares. Accordingly, information is encoded to relieve misfortune and burglary. Data encryption does not capture the theft, but it rather keeps the message content from the interceptor. Another solution for this problem is Cryptography. It consists of cryptology and crypto analysis. In ref [8] Cryptography is the science which deals with protection and storage space of information. Here the method depends on the secret key which is used for data encryption.

However, users having links with short bandwidth require an algorithm for encryption, which use stumpy processing control. In ref [3] Elevated protection algorithms tend to have high processing power when compare to low protection algorithms. Latest implemented algorithms have the capability to organize the protection and processing stage will

November-December 2019
ISSN: 0193-4120 Page No. 4750 - 4753

be a huge improvement for many latest applications.

In ref [1] Data communication plays significant role, it can be used for data swapping between source and recipient in the structure of broadcast media. Explains about security problems where hacking corrupts take place in data communication. Several protective privacy measures are applied to prevent unauthorized access to the user's computers, databases, and websites. In this journal, we have proposed an algorithm using Advanced Encryption Standard.

II. ENCRYPTION AND DECRYPTION

The highly developed Encryption Standard also identified unique name Rijndael, a pattern of encryption of electronic fact. Rijndael is famous as a family of ciphers having dissimilar blocks with size. AES is a symmetric key algorithm used to enhance the performance of data encryption and data decryption. Advanced Encryption Standard is a cipher, used in encrypting and decrypting the information. The security protocols such as HTTP, FTP and OFTP are used to transmit the files over the group.

Encryption is converting information into a cryptographic encoding which can't be read without a key. Encrypted data can't be decrypted by unauthorized parties without the correct key. The most successful way to attain data protection is encryption. Decryption can be used to convert encrypted data into its original form. It is the repeal process of encryption. The encrypted information is decoded so an approved user can only decrypt the data as decryption requires a secret key or password.

The most critical aspects were considered to be security. AES has the best ability to improve sensitive data from breaking the encrypt data. The design and length of key algorithms are enough to keep confidential information with the secret level. Top secret information's will involve the 192 or 256 key lengths.

III. STAGES OF ADVANCED ENCRYPTION STANDARD & RESULTS

The AES algorithm is a symmetric block cipher that can be used for data encryption and decryption in blocks of 256 bits. To decrypt the image and configure data the decryption block uses AES algorithm. Modern secure file transfer protocol is used because symmetric and asymmetric algorithms have their own strength. Asymmetric key ciphers are used for key distribution and are used for symmetric encryption.

Encryption is the core technology prevents unauthorized access of the content. The Advanced Encryption Standard is an encrypted algorithm and one of the mainly classified. The equivalent key can be used for encryption and decryption of symmetric encryption. The algorithm is elastic in supporting any multimedia data and AES consists of "AES-128, AES-192 and AES-256".

For all bit key there are dissimilar rounds. Spinning plaintext into chipper text is a method called as round. The bit which has 10 rounds is "AES-128", the bit that has 12 rounds is the "AES-192" and the bit that has 14 rounds is "AES-256". The key must be shared with other individuals to access the encrypted data. AES algorithm is of four stages which are described below,

Byte sub transformation:

Here sub bytes transformation uses a non-linear transformation. The (s-box) table is constructed by using multiplicative inverse and affine transformation. Multiplicative inverse is also called as reciprocal performs mapping. Affine transformation uses a linear mapping method that preserves data. It is represented using both polynomial evaluation and matrix-vector multiplication. This affine function ensures the original data after transformation.

Shift rows transformation:

The function can be used to shift the bytes in every row of a matrix by an assured offset,

determined by the encryption algorithm. For AES, the initial matrix row is left unchanged. Every byte in the next row is shifted one position to the left. Bytes in the third and fourth rows are shifted by offsets of two and three correspondingly.

Mix-columns Transformation:

Mix-columns transformation consists of two types. It is defined by matrix. The matrix multiplication is equivalent to columns of the states. In Fixed matrix, all column vectors are multiplied. Here the bytes are considered as polynomials other than statistics. In this stage, using an invertible linear transformation four bytes of every attributes is pooled. Four bytes for input and four bytes for output are taken by the mix columns.

Add round Key Transformation:

The XOR operation is used by transformation. The size of state equals the length of round key. In the add round key step, the state the sub key is combined. For each round, from the main key a sub key is derived using Rijindael's key schedule. The same site as the state is same as each sub key. By combining each byte of the state with the corresponding byte of the secondary key using bitwise XOR the subordinate key can be further.

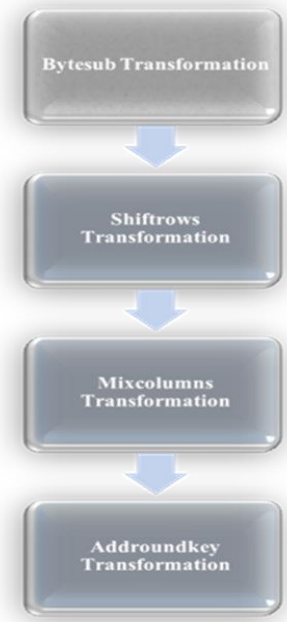

Fig 1. Stages of AES Algorithm

IV. OBSERVATIONS

Use In this section, we have observed four stages of AES. Speed of encryption and decryption is increased with less time. Performance and security will be improved by using these four stages. Internet and network are increasing rapidly day by day. In a daily usage, a set of digital data are being exchanged between users. Various data are classified which are to be protected from intruders. Encryption algorithms do play important roles by protecting creative data from unconstitutional access. A range of algorithms are developed for data encryption. Advanced Encryption Standard algorithm is one of the proficient algorithms which is broadly supported and adopted on all hardware and software. Each stage has a different method of encryption. These stages avoid threats and cyber-attacks. Implementation of such transformation keys would preserve data.

V. CONCLUSION AND FORTHCOMING WORK

In this paper, we have studied about AES and its stages. Different methods are provided to protect data from third party access. This paper has been proposed for the security and integrity of data communication. The future scope of this paper is that AES can be made more secure, reliable, faster using implementation and coding techniques.

REFERENCES

[1] Advanced Encryption Standard-Wikipedia.
[2] "Improvement in the performance and security of Advanced Encryption Standard"-journal by Amit Verma, Simarpreet Kaur, Bharti Chhabra- Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College.
[3] "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data-journal" by Ako Muhammed Abdullah, University of Sulaimani.

November-December 2019
ISSN: 0193-4120 Page No. 4750 - 4753

[4] "Performance Analysis of Advanced Encryption Standard on FPGA-journal" by Lokesh Namdeo & Himanshu Nautiyal, Dept. of Electronics & Communication Engineering Sagar Institute of Research & Technology Bhopal (M. P.).

[5] "Advanced Encryption Standard "- www.research gate.com

[6] "Fuzzy logic-based image encryption for confidential data transfer"- Miss.Hinal, M.Mudia, Prof.Miss.Pallavi V.Chavan.

[7] "Applications of fuzzy logic in daily life- Poonam Gupta", Department of Mathematics, Hindu Girls College, Soniapat, India.

[8] "New Cryptography algorithm with fuzzy logic for effective data communication",- K.GaneshKumar& Dr.Arivazhagan, IIT department, AMET University, Kanathur, Chennai.

[9] "Advanced encryption using fuzzy logic and secret sharing scheme"-Joseph James, SRM Institute of science and technology.

[10] "Advanced Encryption algorithm using fuzzy logic-Ravindu Madanayake", Sri Lanka Institute of information technology.

[11] "Advanced Encryption Standard-Tutorials point".

[12] "Computer and Network Security"-by Avi Kak, Avinash Kak, Purdue University.

[13] "An Acquisition on Big Data Model for Quality Tracing of Iron Steel Industries", S.Priyadharsini,K.Ponnalagu,E.Glory Bebina,A.V.R.Aarthi, Vol-8,Issue-10,Aug 2019.

BIOGRAPHY

Prof. Kavitha S - She is working as an Assistant Professor, Department of Information Technology in Sri Krishna Arts and Science College, Coimbatore, Tamilnadu. Her Areas of Interest are IoT, Data Mining and Computer Networks. She has published more than 8 research papers on Data Mining and Computer Networks.

Anjana Dass – She is studying II B.Sc Information Technology in Sri Krishna Arts and Science College, Coimbatore, Tamilnadu. Her Areas of Interest are IoT and Computer Networks. She has published a journal on IoT.

Kiruthiga.J – She is studying II B.Sc Information Technology in Sri Krishna Arts and Science College, Coimbatore, Tamilnadu. Her Areas of Interest are IoT and Computer Networks.