International Journal of Humanities Education
ISSN: 2327-0063 (Print) ISSN: 2327-2457 (Online)
Volume 11 No. 2, 2023

A Study on Data Security by using Compression Techniques

Sagrika[1], Dr. Gursewak Singh Brar[2], Dr. Sandeep Sharma[3]

[1]Research Scholar, PTU, Jalandhar, Punjab, India

[2]Head&Prof., BBSBEC, Fategarh Sahib, Punjab, India

[3]Head&Prof., GNDU, Amritsar, Punjab, India

Abstract

For every network app that uses an unsafe communication channel, securing internet traffic has always been a prerequisite. The aim for this is to protect data sent over the system from unwanted disclosure & manipulation of messages among messages exchanged. When it comes to data transmission security, Cryptography is really crucial. The major goal is to use a hardware method to boost the throughput of the AES algorithm by processing many rounds at the same time. In this work, raising AES difficulty to improve Confusion & Diffusion in Cipher text as well as applying Diffie Hellmen, the AES approach with hybrid algorithm provided in this work would be an economic way to ensure robust security in the data transmission. The secret key method is utilized to encrypt data, while the Huffman encoding technique is being used to compress & encapsulate the information. The outcomes demonstrated that the suggested data security measures are superior to existing ones.

Keywords

Data Security, Compression, Diffie Hellmen Key Exchange, Huffman Encoding Algorithm

I. INTRODUCTION

The CIA's basic rules are used to evaluate the integrity of the system or information (Confidentiality, Integrity, Availability). Confidentiality protection for people who don't want to get data, referring to transferring data to third parties for specific objectives and only allowed for particular reasons.

[1]Corresponding Author, email: sagrika93@gmail.com

Acceptance: 15October2023, Publication: 18December2023
[2]Second Author, email: gursewak_singh@bbsbec.ac.in
[3]Third Author, email: sandeep80@yahoo.com

Encryption is the process of encrypting data so it can be read by unauthorized persons. The AES, often called as Rijndael, is an electronic encrypted communication specification[1]. AES is an encryption technology that uses cryptographic methods to protect information. The DES standard encryption approach is continued in AES. Power analysis could be used to assault the devices, and this technique could be used to find an answer obtained in the AES approach. This is performed to see if it's possible to find the key in the AES algorithm[2].

For a deeper understanding of the Advanced Encryption Standard method, it is essential to understand the state. The nation is an array of characters that is processed in among several phases & well recharged for each level. However, in the Rijndael method, the crystallite size is the block size. Authors know that 4 bytes read 32 bits is utilize to comprise, which comprises of four lines & Nb rows, where Nb is the amount of bits in blocks multiplied by 32. The AES approach, since authors all know, uses 128 bits. For hardware configurations versions, the AES approach varies depending on the application. Certain systems, including e-commerce servers, require extremely high throughputs.

This research aimed to examine the reduction of microgrid operating cost, by building accurate predictive model and improved scheduling technique. The paper is organized as follows: The AES Encryption are explained in Section II. The Diffie-Hellman Key Exchange Protocol is described in Section III. The Huffman encoding is depicted in Section IV. The literature review is included in Section V. The suggested work's goals and approach are presented in Section VI. Section VII assesses the results of the calculation. The result is shown in Section VIII.

VIII. CONCLUSION

A network is made up of nodes. The primary goal of a network is to transport data from one location to another. Clearly, this data must be protected from unauthorized access. The requirement to protect important data sent over unsecure networks gave rise to the notion of cryptography. The sender encrypts or encodes the information using a secret key and cryptography so that only the tender destination could understand it. Through raising AES complexity to improve Confusion & Diffusion in Cipher text as well as applying Diffie Hellmen, the AES method with hybrid algorithm provided in this work would be an economic way to ensure robust security in the data transmission. The secret key method is utilized to protect data, while Huffman encoding is used to compress & encapsulate the data. The

outcomes demonstrated that the suggested data security measures are superior to existing ones.

REFERENCES

[1] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model", pp. 16–29, 2004.

[2] C. O'Flynn, "A Framework for Embedded Hardware Security Analysis", 20th International Conference on Microwaves, Radar and Wireless Communications (MIKON), June 2014.

[3] Sonali A. Varhade1 , N. N. KasatImplementation of AES Algorithm Using FPGA & Its Performance Analysis International Journal of Science and Research (IJSR) , Vol. 4, Issue 5, May 2015.

[4] C. O'Flynn, "A Framework for Embedded Hardware Security Analysis", 20th International Conference on Microwaves, Radar and Wireless Communications (MIKON), June 2014.

[5] K. Mateur, M. Alareqi, A.Mezouari, H.Dahou, L. Hlou R. Elgouri, "Design and hardware implementation of AES algorithm on FPGA board", The International Conference on Wireless Technologies embedded and intelligent Systems WITS, April 2016.

[6] W. Stallings, Diffie-Hellman Key Exchange, in Cryptography and Network Security Principles and Practice, Pearson Education, pp. 287-291,2013.

[7] Seonyoung Park and Youngseok Lee, "A Performance Analysis of Encryption in HDFS", Journal of KISS : Databases, Vol.41, No. 1, pp.21-27,2014.

[8] R, S. K., R, S., "Design of High Speed AES System for Efficient Data Encryption and Decryption System using FPGA", International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT),2018.

[9] Thinn, A. A., & Thwin, M. M. S., " A Hybrid Solution for Confidential Data Transfer Using PKI, Modified AES Algorithm and Image as a Secret Key",IEEE Conference on Computer Applications(ICCA),2020.

[10] Nuradha, F. R., Putra, S. D., Kurniawan, Y., & Rizqulloh, M. A., " Attack on AES Encryption Microcontroller Devices With Correlation Power Analysis", International Symposium on Electronics and Smart Devices (ISESD),2019.

[11] Shrividhiya, G., Srujana, K. S., Kashyap, S. N., & Gururaj, C., "Robust Data Compression Algorithm utilizing LZW Framework based on Huffman Technique", International Conference on Emerging Smart Computing and Informatics (ESCI),2021.

[12] Wu, H., Chen, R., Wu, J., & Huang, Y., "A Fast Generation Algorithm of Huffman Encode Table for FPGA Implement", 8th International Conference on Electronics Information and Emergency Communication (ICEIEC),2018.

[13] Sivakumar, P., NandhaKumar, M., Jayaraj, R., & Kumaran, A. S., "Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud", IEEE International Conference on System, Computation, Automation and Networking (ICSCAN),2019.

[14] Youngho Song, Young-Sung Shin, Miyoung Jang, & Jae-Woo Chang., "Design and implementation of HDFS data encryption scheme using ARIA algorithm on Hadoop", IEEE International Conference on Big Data and Smart Computing (BigComp),2017.

[15] Kaushik, A., & Srivastava, V. K., "Performance Analysis Of AES And DESede On The Sensitive Data Stored In HDFS", 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN),2020.

[16] D'souza, F. J., & Panchal, D., " Advanced encryption standard (AES) security enhancement using hybrid approach", International Conference on Computing, Communication and Automation (ICCCA),2017.