ABSTRACT

I In the digital era, the need for secure file sharing systems has become increasingly important, especially in Linux-based network environments. This study proposes a file security system using a combination of the ChaCha20 encryption algorithm and a modified Advanced Encryption Standard (AES) through the AddRoundKey method. The system is implemented on the Server Message Block (SMB) version 1 protocol using Samba and is equipped with a Flask-based web client interface to facilitate encrypted file uploading, downloading, and management. The encryption process is layered: the data is first encrypted using the modified AES, and then re-encrypted using ChaCha20 to enhance resistance against attacks and eavesdropping.

Testing was conducted on various types of text and image files ranging from 10KB to 100MB to evaluate system performance in terms of encryption-decryption time, transfer speed, and data integrity. Security testing was performed through checksum validation and traffic analysis using Wireshark to ensure that the data remains protected during transmission. The results showed that the average encryption time was 0.02583 seconds and the decryption time was 0.02271 seconds for 1MB files, with decrypted files matching the original files exactly, as verified by checksum hash values. Additionally, histogram analysis of the encrypted files revealed a highly randomized distribution, supporting the algorithm's effectiveness in obfuscating data patterns. These findings demonstrate that the combination of these algorithms provides better protection than standard Samba methods and maintains file confidentiality and integrity during data sharing. This system proves the effectiveness of hybrid cryptography in enhancing security within SMBv1-based file sharing environments.

Keywords: *ChaCha20, AES, AddRoundKey, Hybrid Cryptography, Samba, SMBv1, File Security, Wireshark*