ABSTRACT

Data security in file transfer processes and sensitive information is a crucial aspect in mitigating risks of data misuse, including threats such as sniffing, phishing, and brute force attacks, which can lead to significant losses for users. The implementation of authentication and encryption mechanisms enhances data protection in Client-Server-based file transfer systems, providing a more secure transmission process. This study employs Advanced Encryption Standard (AES) 256 algorithm, One-Time Password (OTP) authentication via email, and system resilience testing against brute force attacks. The evaluation involves eight file types (.txt, .docx, .rar, .pdf, .png, .jpg, mp4, dan .mp3) categorized into two size groups to assess the system's capability in handling various file formats. The parameters measured include encryption resilience—evaluated based on encryption size and processing time—along with transfer speed and transmission duration.The experimental results demonstrate that the system effectively mitigates brute force attacks and ensures that only authenticated users can access and transfer files. The AES 256 algorithm performs efficiently in encrypting files, with transfer speeds on the client side generally exceeding those on the server. The highest transfer speed was observed for .txt files (3.62 KB/s client, 2.77 KB/s server), whereas .mp4 files exhibited the lowest speed (1.81 KB/s client, 1.71 KB/s server). Transmission time analysis indicates that small files can be transferred within 0 to 2 seconds, while larger files, such as .mp4, require up to 1,268 seconds on the server side and 1,197 seconds on the client side. Additionally, discrepancies in transmission times were noted for certain file types, such as .pdf (14 seconds client, 15 seconds server) and .doc (3 seconds client, 5 seconds server). Brute force testing conducted using the Cryptool application estimated that decrypting the AES 256 encryption would require approximately 5.5e+63 years, further confirming the robustness and security of the implemented encryption scheme.

Kata Kunci: *Authentication*, *File transfer*, AES 256, *socket programming*