Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time

ABSTRACT

Computer, Internet technology have grown exponentially, and constant evolution until today. The usage of digital data such as text, images, audio, animation and videos are commonly used in many aspects of daily activity. The continuous increase in the use of digital data transmission over a network and it exposed to the various kinds of attacks, unauthorized access and network hacking. Thus, it is very hard to ensure that the digital data transmission are secure from any attacks and unauthorized access especially for sensitive and important digital data. This has been raised researcher's concerns on security of the digital data. Digital data security has become one of the most important aspects in communication. Cryptography is one of the most important technology for protecting digital data. As there is need for secure communication, efficient and secure cryptographic processing is needed for desirable platform overall performance. Improvement of any communication platform with secure and complicated cryptographic algorithms incredibly relies on ideas of data safety that is essential within the current technological global. This paper propose a Secured Modified Advanced Encryption Standard Algorithm with decreasing the rounds of Advanced Encryption Standard (AES) to 14 rounds in order to minimize encryption and decryption process time and increasing digital data security as well. The results have been proved that the proposed technique provides higher efficiency in term of encryption and decryption process time compared to other researches while increase security which has been proved by using avalanche effect test.