A Systematic Review on Secure Data Transmission in the Cloud Using Steganographic Techniques and Cryptographic Algorithms

AKSA Anudini[1], G Gayamini[2], TL Weerawardane[2]

Department of Computer Science[1], Department of Computer Engineering[2] , Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

Abstract. Data and information can be considered as the most precious assets in electronic communication systems, but their security has become a struggle in this competitive world. Cloud computing has emerged as the most promising technology for on-demand internet computing, and it is now used by the military, healthcare, education, financial, and a variety of other organizations to handle their large volume of information. Cloud computing has many benefits including efficiency, high performance, scalability, accessibility, backup, and recovery. Security is a major concern in cloud computing because everyone in the organization shares the same cloud platform. The most significant issue for the user is to securely save, retrieve, and transmit data through the cloud network and storage. Cloud security is a subset of cybersecurity that deals with policies, procedures, and technologies for safeguarding cloud computing systems. It protects data in the cloud and other digital assets from data breaches, distributed denial of service (DDoS), hacking, malware, and other cyber threats. Cryptography and steganography can be defined as the most popular techniques that can be used to enhance data security. Cryptography scrambles the messages into the unreadable format while steganography hides the message as it is not visible to the attacker. High-level security is given for both the sender and the receiver inside the cloud platform when cryptography is used along with steganography. This paper analyses the performance of different cryptographic and steganographic techniques. Moreover, suggests that combining of the blowfish symmetric key cryptographic algorithm and Elliptic-Curve Cryptography (ECC) asymmetric cryptographic algorithm as the hybrid cryptosystem to perform double encryption to secure the data and Discrete Cosine Transform (DCT) and Least Significant Bit (LSB) image steganographic techniques can be combined to create a multilayer steganographic algorithm to hide the encrypted file to provide extra security. This proposed system will provide availability, integrity, authenticity, confidentiality, and non-repudiation to the data and information.

Keywords: *Cryptography, Steganography, Symmetric Key Cryptography, Asymmetric Key Cryptography, Image Steganography*