Next-Gen Multimedia Encryption by Combining Symmetric and Asymmetric Cryptographic Techniques

Mrs. P. Banuppriya M.E[1], J. Kaviya[2], C. Keerthana[3] ,P. Kowsalya[4], S. Kowsika[5]

[1]Assistant Professor, Department of CSE

[2,3,4,5] Students, Department of CSE

Mahendra Institute of Engineering and Technology Namakkal, Tamil Nadu, India

Abstract: *Multimedia data security and privacy have grown critical due to the increasing reliance on digital media. Protecting sensitive data from unwanted access requires the use of encryption. The data structure, file size, and real- time processing requirements of images, audio, and video each provide different encryption issues. The many encryption methods and algorithms for digital picture, audio, and video security are examined in this study. Audio encryption frequently uses frequency masking or scrambling to protect media and transmission, while techniques like frequency domain encryption and pixel shuffling are proposed for images. Video encryption, which is crucial for streaming and content distribution, usually uses bitstream-level techniques and selective encryption to guarantee security and compliance with compression requirements. There is also discussion of the difficulties in obtaining real-time encryption and preserving quality throughout the encryption and decryption processes. In an increasingly interconnected world, these methods are essential for digital rights management, secure communications, and personal data security. So, in this paper we can implement hybrid cryptography techniques which includes the Elliptical curve cryptography and Advance encryption standard (AES) algorithm to secure the multimedia data.*

Keywords: Network security, Cryptography, Multimedia, Asymmetric encryption, Sensitive data