Abstract for Major Project - M.Tech - 2024

Title: CipherShield: Pioneering Multi-Key Cryptography Framework for Dynamic File Encryption

Author: Mohammed Abdul Lateef

University Roll Number: 22011DA802

Under the guidance of: Dr. P. Swetha, Professor of CSE & Deputy Director, Directorate of Academic Affairs

Department: Department of Computer Science

Course: Master of Technology

Specialization: Cyber Forensics and Information Security

Duration: 2022-2024

Semester: III semester

Subject: Dissertation Project Review

Institutional Affiliation: Jawaharlal Nehru Technological University Hyderabad

Abstract:

The proliferation of digital content consumption, particularly in the form of text and video files, underscores the paramount importance of securing these assets against unauthorized access and copyright infringement.

In response to this imperative, this intiative presents a comprehensive approach to file encryption, tailoring the cryptographic strategy based on the nature of the content. For text based inputs, a hybrid of RSA and AES encryption model is employed, combining key exchange strength with efficient encryption. Video based data is emphasized to utilize a blend between RSA and Elliptic Curve Cryptography (ECC) approach, adapting to the dynamic nature of video data through multiple key generation. The implemented system is realized through dynamic software featuring dedicated modules for text and video encryption and decryption

In this innovative approach, real-time key generation, based on unique identifiers, dynamically encrypts and decodes file chunks, adapting to evolving data. To assess the effectiveness of the system, rigorous evaluations of its security and performance were conducted. The empirical results underscore the proposed approach's superiority, showcasing advancements in both performance and security metrics. The initiative stands at the forefront of addressing contemporary challenges in the realm of file security, offering a resilient and efficient solution to combat copyright infringement and piracy risks through cryptographic implementation.

Keywords: Multi-Key Cryptography, Hybrid Cryptography, Elliptic Curve Cryptography, Real-time File Securing, Dynamic Encryption, Performance Metrics.