The advent of digital media has necessitated the development of advanced cryptographic techniques to safeguard video content against unauthorized access and tampering. Our model leverages a hybrid cryptographic approach, combining RSA for initial key encryption and AES for chunk-wise dynamic key encryption, ensuring a high level of security and performance. The primary motivation behind this research is to address the growing demand for secure video transmission in various applications, including confidential communications, media broadcasting, and digital rights management. The model's efficiency is rooted in its innovative use of elliptic curve cryptography (ECC) for dynamic key generation. The ECC-based equation ensures that each video chunk is encrypted with a unique key derived from the video ID, system-specific information, and previous keys, providing robust protection against cryptographic attacks. Our implementation integrates seamlessly with a Flask-based web application, enabling user-specific video encryption and decryption. The system's performance is further optimized by efficiently handling video chunking and real-time key generation, resulting in minimal processing overhead and latency. Experimental results demonstrate the model's superior encryption and decryption efficiency, with detailed metrics highlighting its scalability and robustness. This research sets a new standard for secure video communication, offering a comprehensive solution that combines advanced cryptographic techniques with practical implementation for real-world applications.