

PAIRING-FREE CP-ABE BASED CRYPTOGRAPHY COMBINED WITH STEGANOGRAPHY FOR MULTIMEDIA APPLICATIONS

Abstract:

Technology development has led to rapid increase in demands for multimedia applications. Due to this demand, digital archives are increasingly used to store these multimedia contents. Cloud is the commonly used archive to store, transmit, receive and share multimedia contents. Cloud makes use of internet to perform these tasks due to which data becomes more prone to attacks. Data security and privacy are compromised. This can be avoided by limiting data access to authenticated users and by hiding the data from cloud services that cannot be trusted. Hiding data from the cloud services involves encrypting the data before storing it into the cloud. Data to be shared with other users can be encrypted by utilizing Cipher Text-Policy Attribute Based Encryption (CP-ABE). CP-ABE is used which is a cryptographic technique that controls access to the encrypted data. The pairing-based computation based on bilinearity is used in ABE due to which the requirements for resources like memory and power supply increases rapidly. Most of the devices that we use today have limited memory. Therefore, an efficient pairing free CP- ABE access control scheme using elliptic curve cryptography has been used. Pairing based computation is replaced with scalar product on elliptic curves that reduces the necessary memory and resource requirements for the users. Even though pairing free CP-ABE is used, it is easier to retrieve the plaintext of a secret message if cryptanalysis is used. Therefore, this paper proposes to combine cryptography with steganography in such a way by embedding crypto text into an image to provide increased level of data security and data ownership for sub-optimal multimedia applications. It makes it harder for a cryptanalyst to retrieve the plaintext of a secret message from a stego-object if steganalysis were not used. This scheme significantly improved the data security as well as data privacy.

SHIELD TECHNOLOGIES

SHIELD TECHNOLOGIES,

2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64

Mail us: shieldtechnobl@gmail.com / manager@shieldtechno.com

Contact: 9972364704 / 8073744810