115. IMPLEMENTATION OF KEY AGGREGATE CRYPTO WITH STEGNOGRAPHY FORSECURED DATA SHARING IN CLOUD COMPUTING

Ms. S.RAMYA,1 Mr. S.PRASANNA2
1 Second Year M.E Computer Science,Mailam Engineering College,Mailam,Villupuram,
sramyamec@gmail.com
2 Associate Professor Computer Science,Mailam Engineering College,Mailam.

Abstract—Data sharing is an important functionality in cloud storage. Although Cloud Computing is vast developing technology, the challenging problemis how to effectively share encrypted data in cloud computing. In the proposed system, Data owner randomly generates public/master-secret key pair after account is created in the server. Data owner encrypts the data, public key and data index & then uploaded in the Cloud Server. Data owner Generates Aggregate Decryption Key (ADK) using its master-secret key, Data owner can share the data to other Users by sending it's ADK to those via Secured E mail. Original Data, Index and the Public key is downloaded only after Verification of ADK. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In the modification process, we are using steganography. Encrypted Outlet of original Data, Public Key and Index is made stegno into an Image. Data owner has to share the selected Image along with the ADK to download the Original Data. Remote Cloud would authenticate the Image along with the ADK to download Data which ensures security. In particular, our schemes give the first public-key patientcontrolled encryption for flexible hierarchy.

Index Terms—Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

ISBN 978-81-904760-6-5