234. EFFICIENT FINE-GRAINED PRIVACY PRESERVING SYSTEM FOR PUBLIC CLOUD NETWORKS

K.Suganya,
ME –final year department of computer science & Engg,
Mailam engineering college.

An important problem in public clouds is how to selectively share documents based on fine-grained attribute-based access control policies (acps). An approach is to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and/or proxy re-encryption. However, such an approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs. A direct application of a symmetric key cryptosystem, where users are grouped based on the policies they satisfy and unique keys are assigned to each group, also has similar weaknesses. We observe that, without utilizing public key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the above weaknesses. Based on this idea, we formalize a new key management scheme, called broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACV-BGKM. The idea is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. A key advantage of the BGKM scheme is that adding users/revoking users or updating acps can be performed efficiently by updating only some public information. Using our BGKM construct, we propose an efficient approach for fine-grained encryption-based access control for documents stored in an untrusted cloud file storage.

Index Terms—Group key management, privacy, identity, cloud computing, policy, encryption, access control

Journal of Science and Innovative Engineering & Technology

ISBN 978-81-904760-6-5