Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.1 – 9

RESEARCH ARTICLE

Reputable Re-encryption in Unrepeatable Clouds

S. Guna Sree[1], K. Naresh[2]

PG Scholar, Department of Software Engineering, TKR College of Engineering and Technology[1]
Hyderabad, A.P-500 097, India
Email: gunasree34.sunkam@gmail.com

Assistant Professor, Department of Software Engineering, TKR College of Engineering and Technology[2]
Hyderabad, A.P-500 097, India

Abstract— In our Scheme cloud computing users has to get Key information to Re Encrypt the data which has been in Encrypted to get Key information in order to decrease the number of keys used we are proposing Broadcast encryption Broadcast encryption is the cryptographic problem of delivering encrypted content over a broadcast channel in such a way that only qualified users can decrypt the content. The challenge arises from the requirement that the set of qualified users can change in each broadcast emission, and therefore revocation of individual users or user groups should be possible using broadcast transmissions, only, and without affecting any remaining users. As efficient revocation is the primary objective of broadcast encryption solutions are also referred to as revocation schemes. Rather than directly encrypting the content for qualified users, broadcast encryption schemes distribute keying information that allows qualified users to reconstruct the content encryption key whereas revoked users find insufficient information to recover the key. The typical setting considered is that of a unidirectional broadcaster and stateless users which is especially challenging. In contrast, the scenario where users are supported with a bi-directional communication link with the broadcaster and thus can more easily maintain their state, and where users are not only dynamically revoked but also added (joined), is often referred to as multicast encryption.

Keywords—Element-based encryption; cloud computing; substitute re-encryption

Full Text: http://www.ijcsmc.com/docs/papers/December2013/V2I12201301.pdf