# 189. PRIVACY PRESERVING PUBLIC AUDITING THE CORRECTNESS OF DATA BETWEEN THE CLOUD USING IBE

M.SHALINI 1, A.USHA RUBY 2,
Department of Computer Science and Engineering, CSI College of Engineering1
Research Scholar, Bharath University2
Email: manishalini29@gmail.com, ausharuby@gmail.com

In Cloud Storage, users will remotely store their knowledge and delight in the on demand prime quality applications and facilities. Each knowledge to permit many mechanism designed in house owners and public verifiers to expeditiously audit cloud knowledge integrity while not retrieving the whole knowledge from the cloud server. Knowledge to share the public auditing on the integrity with these existing mechanisms can inevitably reveal hint identity privacy to public verifiers. Shared knowledge keep within the cloud that exploit ring signature to calculate verification data required to audit the correctness of shared knowledge. So a Thirdparty auditor (TPA) is in a position to verify the integrity of shared knowledge for users while not retrieving the whole knowledge. A public verifier, like a Third party auditor (TPA) providing expert data auditing services or a knowledge user outside the group desiring to utilize shared data, is ready to publically verify the integrity of shared knowledge hold on within the cloud server. Once a public verifier desires to see the integrity of shared knowledge, it first sends associate degree auditing challenge to the cloud server. After receiving the audit challenge, the cloud server responds to the general public verifier with an audit proof of the possession of shared knowledge. Then, this public verifier checks the correctness of the whole knowledge by substantiate the correctness of the audit proof. Essentially, the method of public auditing is a challenge and response protocol between a public verifier and the cloud server.

Index Terms Public auditing, privacy-preserving, shared data, cloud computing.



ISBN 978-81-904760-6-5