



# International Journal on Recent Researches In Science, Engineering & Technology

(Division of Computer Science and Engineering)

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.

It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.

Research Paper

Available online at: [www.jrrset.com](http://www.jrrset.com)

Chief Editor : Dr. M.Narayana Rao, Ph.D., Rtd. Professor, NIT, Trichy.

ISSN (Print) : 2347-6729

ISSN (Online) : 2348-3105

Volume 3, Issue 4,  
April 2015

JIR IF : 2.54

DIIF IF : 1.46

SJIF IF: 1.329

---

## Enabling Public Verifiability for Storage Security In Cloud Computing

UMA K S

II year PG Student, Computer Science and  
Engineering  
KCG College of Technology  
Chennai, India.  
umaskn@gmail.com

P M BOOMA ME

Assistant Professor, Department of Computer  
Science and Engineering  
KCG College of Technology  
Chennai, India.  
booma.cse@kcgcollege.com

**Abstract:** This paper shows however firmly, expeditiously, and flexibly knowledge is often shared with others. To describe new asymmetric cryptosystems that produces constant-size cipher texts such economical delegations of coding rights for any set of cipher texts are potential. The novelty is that one can aggregate any set of secret keys and create them as one key, however encompassing the facility of all the keys being collective. The main concept of this project is how to send the data through receiver in secure way. The sender is termed the data owner. Data owner send the data to server in associate encrypted kind. Here the system acts as a server. A special asymmetric cryptosystem is employed to get a cipher text. The owner decides the cipher text size. Since the cipher text ought to be transferred to the receiver confidentially. The data owner setup the general public system, Key Generation algorithm which generates a public or master secret key. By using this key, user will convert plain text to cipher text. Then user can provide input as master secret key by extract function. The server send key through an email to the receiver. Using this key the receivers download the data. It provides formal security analysis of our schemes within the commonplace model. Particularly, our schemes provide the primary public key secret writing for versatile hierarchy.