



**PRIVACY PRESERVING AND  
UNTRACEABLE GROUP**



**A PROJECT REPORT**

*Submitted by*

**DINESH KUMAR.S (710419106007)**

**KARTHIKA.K (710419106014)**

**SIBI CHAKRAVARTHI.B (710419106027)**

*In partial fulfilment for the award of the degree  
of*

**BACHELOR OF ENGINEERING**

**IN**


**ELECTRONICS AND COMMUNICATION ENGINEERING**

**CHRIST THE KING ENGINEERING COLLEGE,  
COIMBATORE-641104**

**ANNA UNIVERSITY: CHENNAI 600 025**

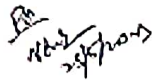
**APRIL-MAY 2023**



  
**Dr. M. Jeyaraj Murugan, M.E., Ph.D.**  
**PRINCIPAL**  
**CHRIST THE KING ENGINEERING COLLEGE,**  
**Chikkarampalayam village,**  
**Karamadai, Mettupalayam Taluk,**  
**Coimbatore - 641 104.**

## BONAFIDE CERTIFICATE

Certified that this project report "PRIVACY PRESERVING AND UNTRACEABLE GROUP" is the bonafide work of "DINESH KUMARS (710419106007), KARTHIKA.K (710419106014), SIBI CHAKRAVARTHI.B (710419106027)" who carried out the project work under my supervision.



SIGNATURE

Dr. A. Kingsly Jabal Kumar, M.E., Ph.D.,


HEAD OF THE DEPARTMENT,

ASSOCIATE PROFESSOR,

Department of Electronics and  
Communication Engineering,

Christ The King Engineering

College, Coimbatore – 641104.



23/05/2023

SIGNATURE

Mr. K. Sedhu Ramalingam, M.E., (Ph.D.),

SUPERVISOR,

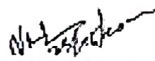
ASSISTANT PROFESSOR,

Department of Electronics and  
Communication Engineering,

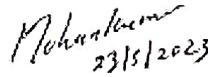
Christ The King Engineering

College, Coimbatore – 641104.

The project report submitted for the viva voce held on 23/5/23




INTERNAL EXAMINER



23/5/2023

EXTERNAL EXAMINER



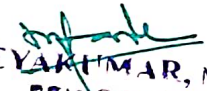
Dr. M. JEYAKUMAR, M.E., Ph.D  
PRINCIPAL  
CHRIST THE KING ENGINEERING COLLEGE,  
Chikkarampalayam Village,  
Karamandi, Mettupalayam Taluk,  
Coimbatore - 641 104.

## ABSTRACT

With the development of cloud computing, the great amount of storage data requires safe and efficient data sharing. In multiparty storage data sharing, first, the confidentiality of shared data is ensured to achieve data privacy preservation. Second, the security of stored data is ensured. That is, when stored shared data are subject to frequent access operations, the server's address sequence or access pattern is hidden. Therefore, determining how to ensure the untraceability of stored data or efficient hide the data access pattern in sharing stored data is a challenge. By leveraging proxy re-encryption and oblivious random access memory (ORAM), a privacy-preserving and untraceable scheme is proposed to support multiple users in sharing data in cloud computing. On the one hand, group members and proxies use the key exchange phase to obtain keys and resist multiparty collusion if necessary. The ciphertext obtained according to the proxy re-encryption phase enables group members to implement access control and store data, thereby completing secure data sharing. On the other hand, this paper realizes data untraceability and a hidden data access pattern through a one-way circular linked table in a binary tree (OCLT) and obfuscation operation. Additionally, based on the designed structure and pointer tuple, malicious users are identified and data tampering is prevented. The proposed scheme is secure and efficient for group data sharing in cloud computing. This project also enhanced Traitor Tracing Once the user's secret key is leaked for profits or other purposes, server runs trace algorithm to find the malicious user. After the traitor is traced, user will be blocked in cloud server. The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys.

v



  
**Dr. M. JEYAKUMAR**, M.E., Ph.D.  
PRINCIPAL  
CHRIST THE KING ENGINEERING COLLEGE,  
Chikkaraipalayam Village,  
Karamadai, Mettupalayam Taluk,  
Coimbatore - 641 104.

## CHAPTER- 7

### CONCLUSION


#### 7.1 CONCLUSION

In this project, we present a secure and untraceable protocol for group data sharing in a cloud storage scheme. Based on key exchange, the proposed approach can efficiently generate the users conference key, which can be used to protect the security of shared data and prevent malicious user collusion with other users. In addition, security of shared group data in the cloud and access control is achieved with respect to the encryption technique. The sufficient security proof indicates the security of our protocol. The experimental comparison results could be considered as validation of the performance of our protocol, making it substantially more convincing.

#### 7.2 SCOPE FOR FUTURE ENHANCEMENT

There is scope for future development of this project. The world of computer fields is not static; it is always subject to be dynamic. The technology which is famous today becomes outdated the very next day. To keep abstract of technical improvements, the system may be further refined. So, it is not concluded. Yet it will improve with further enhancements. Enhancements can be done in an efficient manner. We can even update the same with further modification establishment and can be integrated with minimal modification. Thus the project is flexible and can be enhanced at anytime with more advanced features.



  
**Dr. M. JEYAKUMAR, M.E., Ph.D**  
PRINCIPAL  
CHRIST THE KING ENGINEERING COLLEGE,  
Chikkarampalayam Village,  
Karamadai, Mettupalayam Taluk,  
Coimbatore - 641 104.