17-18

ICI
SCOPUS

PRIVACY AND OWNER AUTHERISATION FRAMEWORK TO MANAGE KEYS

Darshan Chavan[1], Prof.P.M.Yawalkar[2]
[1] *M.E., Computer Engineering Department, Maharashtra, India*
[2] *Computer Engineering Department, Maharashtra, India*

ABSTRACT

The number of encryption keys increases due to limit of web app users get exceeds. Outsourcing keys to the professional password managers is an attractive trend. Traditional outsourcing scenarios are not capable to meet the security requirements for outsourcing keys such as, privacy & confidentiality of keys, privacy on attribute ties to keys at the time of search. In proposed system, SC-PRE scheme is utilized. It combines two approaches such as, Proxy Re-encryption (PRE) and Hidden Vector Encryption (HVE). It encrypts key tuple similar to normal data encryption. The proposed cloudKeyBank framework achieved three security requirements for outsourcing of keys such as, confidentiality of key privacy, attributes of search ties with key and owner controllable authorization on shared keys. Bloom filter is space-efficient probabilistic data structure designed to specify whether an element is present or not in the set. It is rapid and memory efficient strategy which we contribute in our proposed work. It can save search space and time of searching.

Keyword: *SC-PRE, search privacy, key management, keys outsourcing*

1. INTRODUCTION

Password and key management is the challenging task which occurred in the scenario of outsourcing data. In this era, there is huge growth in the use f web applications. Users have multiple online accounts for various purposes. Web development deploys 'n' number of applications such as, social networking (Facebook, twitter, linkend), shopping sites (Amazon, eBay, snapdeal etc) and data storages such as, googledrive. To provide authorization for individuals account there is registration and login page, by using this new user can registered their details to web application and further use this registered credentials for accessing their accounts. Similar approach is carried out in case of data outsourcing to the cloud server or cloud storage. Generally, user uploads their data to cloud in encrypted format for the perspective of data security. Data encryption is performed using cryptographic functions or using encryption algorithm. In the process of data encryption, some secret keys are generated at the user's end which may uploaded to cloud server for their appropriate management and these keys are also forwarded to other user's for data retrieving purposes. Due to cost efficient and scalable data storage, many users and huge business industries take benefit of it for management and maintenance of their heavy data. According to survey analysis, 90% of students were concern about privacy to their key or password. There are two types of situations about privacy concern such as, they do not fully trust the service providers because there is no governance about how keys can be used by them and whether the key owner can actually control their keys on their own OR they trust the service providers, but keys could be disclosed if there exists an misbehaving internal employee or broken server. Hence to provide privacy for key is to encrypt key tuple before outsourcing them and encryption process is similar to the normal data encryption. It is promising solution to maintain trust and also to ensure key privacy and owner control on outsourced keys.

Proposed system is based on SC-PRE i.e. Searchable Conditional Proxy Re-Encryption scheme. It combines two techniques namely, hidden vector encryption (HVE) and proxy re-encryption (PRE). It can efficiently solves the challenging issues occurred in key tuple encryption. During key tuple encryption some critical issues are identified such as, keys are highly sensitive and they need to be secured from honest-but-curious service provider and malicious attacks.

In proposed cloudkeybank framework, there are three main entities are included such as, cloud, trusted client and cloudkeyBank. Trusted client is the intermediate between cloud and cloudkeyBank. Two types of protocols used for key traversal i.e. depositeKey protocol and withdrawKey.