International Conference on Engineering & Technology (ICET-2020)

Available at: *International Journal of Scientific Research and Engineering Development*

RESEARCH ARTICLE OPEN ACCESS

Data and User Confidentiality Privacy Preservation in Distributed Servers

Mr. M.Prabakaran, M.E Assistant professor,
Department of CSE
Selvam College of technology, Namakkal.
Karn.mp0712@gmail.com

C.Manivarma.UG student,
Department of CSE
Selvam College of technology, Namakkal
Varmavirat143@gmail.com

G.Poovarasan.UG student,
Department of CSE
Selvam College of technology, Namakkal.
Poovarasancse77@gmail.com

S.Dharmadhurai. UG student,
Department of CSE
Selvam College of technology, Namakkal
dharmadhurais3698@gmail.com

ABSTRACT

Distributed data and its processing to cloud storage server delivers an efficient way to organize large scale file storage and its related operation. In accordance with privacy and security issues on user data that are sensitive need to stored and protected from the distributed cloud server and and from intruders. The proposal is to distribute encrypted data to the cloud server to perform necessary processing on the data that has been encrypted. It is a tedious process to organize and support queries in the distributed server that has been stored and encrypted. Which has been stored in an efficient and secure manner in a most prominent way that the cloud server doesn't gain or attain any knowledge that has been stored in the server. In our proposal, we investigate the problem of secure skyline queries over encrypted data. The skyline query is efficient for securing data in the server, i.e.: skyline controls the entire data with an encrypted data and database. We utilize a complete secure skyline query on encrypted data using semantically-secure encryption. We implement a secure dominant protocol which secures the data with its own dominance, from which unauthorized access can be blocked. The outsourced data in the distributed database server are quiet unsecure when compared with the current techniques and security measures. So that we propose a methodology based on skyline queries, along with that we include the user data as a illusion data and the data and the database are in an encrypted format, so that the distributed server has no knowledge about the data that has been saved by the user to the data owner. The data has been stored within an image using the morse code analysis procedure. It stores the user information in to an image and retrieves the user data using specific private key generation. Data owner is the authorized person who transmits the data to the distributed database.the distributed server has no knowledge about the data that has been saved by the user. In case of intruder breach the intruder attains the illusion data and the intruder alert intimation will be given to the concern data owner and user.

INTRODUCTION

As an emerging computing paradigm, cloud computing attracts increasing attention from both research and industry communities. Outsourcing data and computation to cloud server provides a cost effective way to support large scale data storage and query processing. However, due to security and privacy concerns, sensitive data need to be protected from the cloud server as well as other unauthorized users. A common approach to protect the confidentiality of outsourced data is to encrypt the data. To protect the confidentiality of the query from cloud server, authorized clients also send encrypted queries to the cloud server. It illustrates our problem scenario of secure query processing over encrypted data in the cloud. The data owner outsources encrypted data to the cloud server. The cloud server processes encrypted queries from the client on the encrypted data and returns the query result to the client. During the query processing, the cloud server should not gain any knowledge about the data, data patterns, query, and query result. Fully homomorphism encryption schemes ensure strong security while enabling arbitrary computations on the encrypted data. However, the computation cost is prohibitive in practice. Trusted hardware such as Intel's Software Guard Extensions (SGX) brings a promising alternative, but still has limitations in its security guarantees. Many techniques have been proposed to support specific queries or computations on encrypted data with varying degrees of security guarantee and efficiency (e.g., by weaker encryptions). Focusing on similarity search, secure k-nearest neighbor (knn) queries, which return k most similar (closest) records given a query record, have been extensively studied.

EXISTING SYSTEM

- A location-privacy preservation scheme, called movewithme automatically generates a number of decoys to move with the user and serve as distractions.
- In the movewithme system, each decoy queries has its own moving patterns based on the user's needs.
- Unlike previous approaches our decoys may further confuse the attackers about the locations of the real user.
-

DISADVANTAGES

- MoveWithMe system against a variety of existing location-based services it results in low feasibility, effectiveness, and efficiency.

- Compared with existing approaches, movewithme system

