PROVIDING PRIVACY AND SECURITY OF SENSITIVE DATASETS IN UNTRUSTED CLOUD ENVIRONMENT

R.S. Pratheeba[1], M. Lavanya[2]

Department of Computer Science, Assistant Professor, Dr.APJ Abdul Kalam Centre for Research,
Adhi College of Engineering and Technology,Chennai, India
pratheegreen@gmail.com

Abstract

Data streams are exchanged to an advantageous rich cloud server for internal cloud evaluation, a normal building of cloud frustrate in various applications such that statistical monitoring, Market analysis and traffic management. On the other hand, verification of the remote cloud computation results in playing a crucial role in identifying the issue of trust. Since the high quality and affordable data collection likely comes from various data sources, it is desired for the system to be able to indicate the errors generated by the originator by allotting each data source a unique secret-key. This key needs the inner product verification to be performed under any two parties' keys. The present situation either depend on a single key encryption or powerful but practically inefficient fully homomorphic cryptosystems. The more challenging thing that we use is multiple key scenario where data sets are uploaded by multiple data sources with different keys. We focus on a new method called homomorphic framework to verify the dynamic data sets from various data sources inner product computation and then to concentrate data set security by splitting up of data sets. The proposed system uses DES algorithm for multiple key generation still to make more security and accessing data in efficient manner.

Keywords: **Data sets; DES; homomorphic cryptosystems; Multiple keys; Public verifiability**

I. INTRODUCTION

Many of the software industry have entered the development of cloud services. It is the greatest on-demand service system along with a "Pay as you go" Policy. Based on agent Cloud computing, it consists of the design and development of software agents Cloud services. Distributed and constantly changing Cloud computing environments facade new challenges to automated service composition such as: (i) Dynamically contract service providers, which set service fees on a supply-and-demand basis, and (ii) Dealing with incomplete information regarding Cloud resources. Sometimes it allows resource agents to take advantage of the delegation of tasks[6].

There is a sudden increase in the cloud computing system's intervention that provide computing resources based on demand and multiplexing many users on the same physical infrastructure. These cloud computing environments provide a fantasy of unlimited computing resources to cloud users so that they can increase or decrease their consumption of resources and thus rate according to the demands. The cloud environment provides a number of challenges. Cloud providers and cloud users, follow different goals, providers want to maximize profits by achieving high resource consumption, while users want to minimize expenses. However, it is difficult for resource allocation in a comfortable way due to the shortage of information sharing between those members[7].

The past few years have witnessed the proliferation of streaming data generated by a variety of applications/systems, such as GPS, Internet traffic, asset tracking, wireless sensors, etc. Retaining a local copy of such exponentially growing volume of data is becoming prohibitive for resource-constrained companies / organizations, let alone offering efficient and reliable query services on it. Consider a stream-oriented service (e.g., market analysis, weather forecasting and traffic management), where *multiple* resource-constrained sources continuously collect or generate data streams, and outsource them to a powerful external server, e.g. cloud, for desired critical computations and storage savings. For example, using inner product computation over any two outsourced stock data streams from different sources for correlation analysis, a stock market trader is able to spot the arbitrage opportunities [1].