Trusted Cloud based Storage and Retrival Process using Symmetric Searchable Encryption

S.Ponni[1], Prakash S[2], Preetha R[3], Srinivedha M P[4]
[1]Assistant Professor CSE,
[2][3][4] Final Year Students Department Of CSE
Velalar College Of Engineering And Technology
Thindal, Erode-12

Abstract:- **Cloud computing plays a dominant role in the growth of the country's economy. A security challenge has become a major threat in the modernization economy. This makes**
the problem in rapid economy. Cloud computing techniques are the better choices for this purpose. Cloud computing has many techniques for the purpose of secure protection. Trusted Cloud Based technique involves symmetric key encryption for the safe and secure retrieval of data and files using the keyword. K-means clustering is used for the faster retrieval of data. It will be helpful in faster and secure retrieval of data. Encrypt ; Kmeans

Keywords: Cloud computing; client; Multi-keyword; Admin; clustering.

I. INTRODUCTION

Every website can have its own identity management system to get entry to information and computing resources. Websites today secure safe and secure way to store and access their data. This is where cloud technology comes in. Many companies today depend on the cloud for the smooth running of their businesses. Security is one of the most important challenges which might be faced by many Business and Management system. For the safety motive a login key is used. An authorized client can get entry to the website via the login key. Only then view the files and documents that are uploaded. For downloading the file, the client has to enter some of the details that are required for the website to get entry to. An activation code is sent to the respective mail of the client that entered. After entering the code, the client can download the file as required. By doing so, security is ensured. Using cloud infrastructure reduces prices because organizations don't have to spend large quantities of cash buying and preserving equipment. This reduces their capital expenditure costs because they don't need to spend money on hardware, facilities, utilities or building large data centers to deal with their growing organizations.

Cloud computing is a popular option for people and organization for a number of reasons including value savings, expanded productivity, speed and efficiency, performance and security. Cloud computing is known as such because the facts being accessed is found remotely inside the cloud or a digital space.

II.BACKGROUND

Cloud computing has become the ideal way to deliver enterprise applications and the preferred solution for companies extending their infrastructure or launching new innovations. There are different processes and techniques used to carry out cloud computing successfully.

This section discusses about various related works already done in cloud computing techniques using previous references. Most of the researchers focused on the problem for security, faster an accurate retrieval of data.

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. It constructs a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search [9]. The secure Knn algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors.

In cloud computing, searchable encryption scheme over outsourced data is a hot research field. However, most existing works on encrypted search over outsourced cloud data follow the model of "one size fits all" and ignore personalized search intention. Moreover, most of them support only exact keyword search, which greatly affects data usability and user experience [10]. So how to design a searchable encryption scheme that supports personalized search and improves user search experience remains a very challenging task.

To ensure security and privacy these data are first encrypted before being uploaded onto the cloud servers thus making search a complicated task. Although in traditional

cloud computing encryption searching schemes allows user to search encrypted data through keywords securely. These techniques employed exact keyword search and will fail if there are any morphological variants or spelling errors. This leads to low in efficiency and also affects system usability very badly [11]. Fuzzy keyword search increases the system usability by allowing matching the exact or closet match text to the stored keywords and retrieving the approximate closest results.

III.EXPERIMENTAL STUDY

K-means clustering is used for the faster and accurate retrieval of data using a symmetric searchable encryption.

Data owner will upload their data in encrypted way in cloud. Here cloud is used for storing and retrieving process alone hence there is no chance for leakage of any private information. Dynamic searchable encryption is used to encrypt the data. Once data has been encrypted and uploaded in cloud it will be searched by users through the keyword. The uploaded content will be retrieved efficiently using k means clustering. Based on user query, related content is collected and grouped together and accurate result has been obtained.

Special Issue - 2020

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
RTICCT - 2020 Conference Proceedings

1. ENCRYPT MODULE

This module is used to help the server to encrypt the file the use of RSA Algorithm and to transform the encrypted document to the Zip document with activation code after which activation code ship to the client for download.



ENCRYPTED AND UPLOADED FILES

LOGIN PAGE

2. CLIENT MODULE

This module is used to assist the client to go looking the document the use of the multiple keywords concepts and get the correct and result list based totally at the client query. The client goes to select the required document and sign up the client info and get the activation code in mail from the preetha.ramalingam2016@gmil.com email

earlier than input the activation code. After client can download the zip record and extract that document.
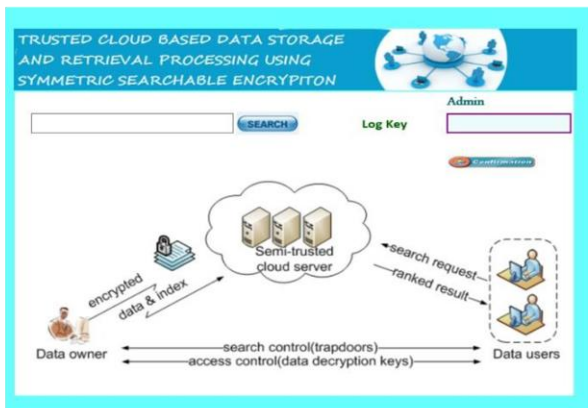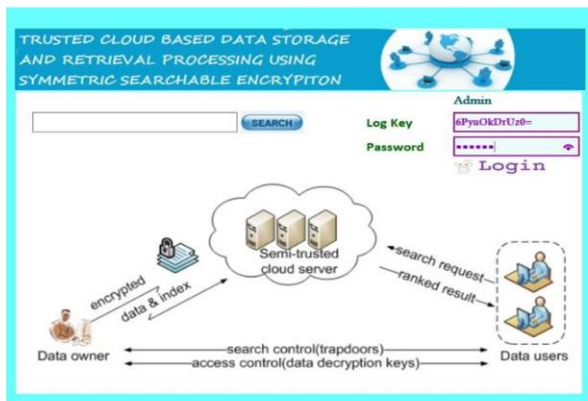
CLIENT ENTERS KEY AND PASSWORD

**CLIENT ENTERS THE DETAILS**

3. MULTI-KEYWORD MODULE

This module is used to help the client to get the accurate result based on the multi keyword concepts. The client can enter the multiple words query, the server is going to split that queries into unmarried phrase after search that phrase document in the database. Finally, show the matched document listing from the database and the client receives the document from that listing.

4. ADMIN MODULE

This module is used to help the server to view details and upload documents with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and think about the client downloading details and the counting of file documents request details on flowchart. The admin can add the document after the conversion of the Zip document format.

IV.WORK FLOW
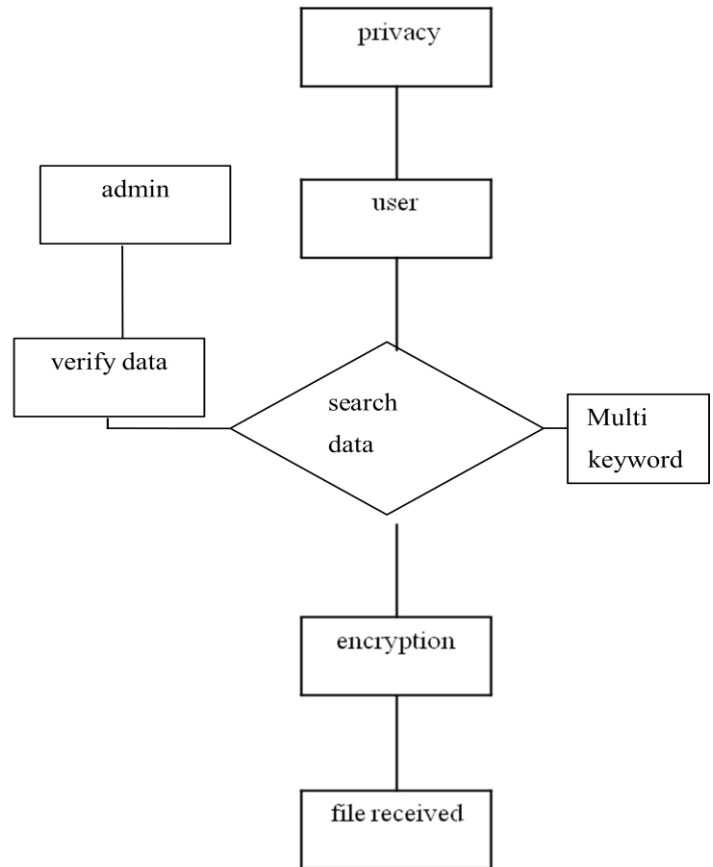
V.CONCLUSION AND FUTURE ENCHANCEMENTS

According to the result, a secure and effective multi-keyword ranked search scheme over encrypted cloud data is done. Also, our scheme more successfully supports dynamic operations that contain deletions or insertions in a document. Thus, we proposed the problem of multiple-keyword ranked search over encrypted cloud data, and construct a variety of security requirements. From various multi- keyword concepts, we pick the efficient principle of coordinate matching. We first propose secure inner data computation. Cloud computing will derive the enterprise in future. These applications will drive enterprise efficiency, file sharing, social media and CRM. Some of the IT primarily based cloud applications will address Big Data, Helpdesk, Mobile application, Security, System management and so on. However, organizations are smooth emigrate mission-critical workloads to public clouds. One of the motives for this shift is that enterprise executives who need to make sure that groups can complete inside the new world of the digital transformation.

VI.REFERENCE

[1] Alistair McMonnies, "**Object-oriented programming in Visual Basic.NET**", Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.

[2] Chris Goode, John Kauffman, "**Microsoft Visual Basic.NET Programmer's Cookbook**", (Tata McGraw Hill Edition) - 2002.

[3]Elias M. Awad, " **System analysis and design**", May 2001.

[4] Gary Cornell, "**Visual Basic 6 from the Ground Up**", Published by McGraw Hill, Edition 2002.

[5] Jittery R.Shapiro, "**The Complete Reference Visual Basic .NET**" Edition 2002, Tata McGraw-Hill, Publishing Company Limited, New Delhi.

[6] Peter Wright, "**Beginning Visual Basic 6**", Published by Wrox Press, August 1998.

[7]"**ProgrammingDistributed Applications With Com and Microsoft Visual Basic 6.0**", Ted Pattison Published by Microsoft Press, Paperback, Edition 2000.

[8]Somerville, "**Software Engineering**", 5th Edition.

[9] Z Xia,X, Wang,X, Sun,Q, Wang, "**A Secure And Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data**", 2015.

[10] Z Fu,K Ren,J Shu,X Sun, "**Enabling Personalized Search Over Encrypted Outsourced Data With Efficiency Improvement**", 2015.

[11] J Li,Q Wang,C Wang,N Cao,K Ren, "**Fuzzy Keyword Search Over Encrypted Data In Cloud Computing**", 2010.