Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

EFFICIENT AND ANONYMOUS AUTHENTICATED KEY EXCHANGE SCHEME FOR WEARABLE COMPUTING

BASIVIREDDY SURESH KUMAR[1], Dr. B. V. RAM KUMAR[2], Dr. G. SATYANARAYANA[3]
#1 M.Tech Scholar and Department of Computer Science Engineering,
#2 Professor, Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.
#3 Professor, HOD Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.

Abstract–

For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. The issue of recovering the encrypted data over the cloud is mind boggling. Numerous search procedures are utilized for recovering the scrambled data from cloud. This paper axes around an arrangement of keyword Search instruments over encrypted data, which gives secured data recovery high proficiency. Search over encrypted data is a method of extraordinary enthusiasm for the cloud computing time, in light of the fact that numerous trust that delicate data must be scrambled before outsourcing to the cloud servers with a specific end goal to guarantee client data security. Concocting a productive and secure search scheme over scrambled data includes strategies from ple spaces. It presumes that, keyword search is intended to be best methodology for searching the encrypted data in the Cloud. It gives more productivity than single keyword search.

Keywords: Cloud Computing, Keyword search, Outsourced data, Encrypted data, keyword search Ranked.

I. Introduction

Cloud computing has been considered as another model of big business IT framework, which can make huge asset out of computing, storage and applications, and engage clients to acknowledge inescapable, accommodating and on-request organize access to a shared pool of configurable figuring assets with inconceivable effectiveness and inconsequential financial overhead [1]. Pulled in by these connecting with highlights, the two people and endeavor are utilized to outsource their data to the cloud, as opposed to purchasing programming and equipment to manage the data themselves. Regardless of the distinctive purposes of enthusiasm of cloud administrations, outsourcing fragile data, (for instance, email, singular wellbeing records, association account data, government chronicles, et cetera.) to remote servers brings protection concerns. The cloud specialist co-ops (CSPs) that keep the data for clients may get to clients' touchy data without approval. A general method to manage secure the data protection is to encode the data before outsourcing [2].On the other hand, this will realize an immense cost regarding data convenience. For instance, the present strategies on keyword-based data recovery, which are comprehensively used on the plaintext data, can't be clearly associated on the scrambled data. Downloading every one of the data from the cloud and unscramble locally is plainly improbable. In the least difficult terms, cloud computing implies putting away and getting to data and projects over the Internet rather than your PC's hard drive. The cloud is only an illustration for the Internet. What cloud computing isn't about is your hard drive. When you store data on or run programs from the hard drive, that is called neighborhood storage and computing. All that you require is physically near you, which implies getting to your data is quick and simple, for that one PC, or others on the neighborhood arrange. Working off your hard drive is the way the PC business worked for quite a long time; some would contend it's as yet better than cloud computing, for reasons I'll clarify in no time. For it to be considered "cloud figuring," you have to get to your data or your projects over the Internet, or in any event, have that data synchronized with other data over the Web. In a major business, you may know everything to think about what is on the opposite side of the association; as an individual client, you may never have any thought what sort of gigantic data handling is occurring on the opposite end. The outcome is the same with an online association, cloud computing should be possible anyplace, whenever.

II. Related work

Cloud computing changes the way data innovation (IT) is consumed and managed, promising Enhanced cost efficiencies, stimulated advancement, speedier time-to-showcase, and the ability to scale Applications on intrigue (Leighton, 2009). [1]. according to Gartner, while the development grew exponentially amid2008 and continued since, unmistakably there is a critical development towards the cloud computing model and that the focal points might be huge (Gartner Hype-Cycle, 2012). Nevertheless, as the cloud's state Computing is rising and becoming rapidly both hypothetically and really, the honest to goodness/legally binding, money related, organization quality, between operability, security and assurance issues still stance basic troubles. In this Part, we portray diverse administrations and association models of appropriated figuring and perceive critical Difficulties. 2.2 Security challenges for people in general cloud Kui Ren, Cong Wang, and Qian Wang, In this paper, Cloud figuring speaks to the present most energizing computing change in outlook in data innovation. Nonetheless, security and protection are seen as essential obstructions to its wide appropriation. Here, the creators plot a few basic security challenges and propel facilitate examination of security answers for a reliable open cloud condition. cloud computing is the most up to date term for the since a long time ago envisioned vision of computing as an utility. The cloud gives helpful, on-request arrange access to a unified pool of configurable computing assets that can be quickly sent with awesome effectiveness and insignificant administration overhead. With its un-priority points of interest, cloud figuring empowers an essential change in outlook in how To send and convey computing administrations that is, it makes conceivable computing outsourcing to such an extent that the two people and endeavors can abstain from conferring substantial capital costs when buying and overseeing programming and equipment, as Toll as managing the operational overhead therein.[1] 2.3 Cryptographic cloud storage S. Kamara and K. Lauter, In this paper, To consider the issue of building a protected cloud storage benefit over an open cloud foundation where the specialist organization isn't totally trusted by the client. To depict, at an abnormal state, a few designs that join later and non-standard cryptographic natives keeping in mind the end goal to accomplish our objective. To study the advantages such an engineering would give to the two clients and specialist co-ops and give an outline of ongoing advances in cryptography persuaded particularly by cloud storage. [2] A completely homomorphism encryption scheme C. Upper class, In this paper, To propose the principal completely homomorphism encryption scheme, taking care of a focal open issue in cryptography. Such a scheme enables one to figure discretionary capacities over encrypted data without the unscrambling key { i.e., given encryptions E(m1); … ; E( ) of m1;… ; mt, one can proficiently process a reduced figure message that scrambles f(m1;… ; m) for any effectively calculable capacity f. This issue postured by Rivest et al. in 1978. Completely homomorphic encryption has various applications. For instance, it empowers private questions to a search motor { the client presents a scrambled inquiry and the search motor figures a compact encrypted reply while never taking a gander at the question free. It additionally empowers searching on encrypted data { a client stores scrambled documents on a remote record server and can later have the server recover just documents that (when unscrambled) fulfill some Boolean limitation, despite the fact that the server can't decode the records without anyone else. All the more comprehensively, completely homomorphic encryption enhances the proficiency of secure gathering calculation. Our development starts with a to some degree homomorphism boot-strappable" encryption scheme that works when the capacity f is the scheme's own unscrambling capacity. To then show how, through recursive self-implanting, boot-strappable encryption gives completely homomorphic encryption. The development makes utilization of difficult issues on perfect cross sections. [3] 2.4 Software security and reproduction on neglectful rams O. Goldreich and R. Ostrovsky, [4] In this paper, To exhibit a hypothetical treatment of programming security. Specifically, To distil and figure the key issue of finding out about a program from its execution, and lessen this issue to the issue of on-line reproduction of a self-assertive program on a careless RAM. To then present our fundamental outcome: a productive reproduction of a subjective (RAM) program on a probabilistic absent.

III. Cloud Computing Models

Cloud gives resources to user through different models. It is provided by the service providers and hosted by cloud vendors to users. Fig 2.1 and 2.2 explains the various cloud services and layered architecture of cloud services. The various Service models in cloud are explained as follows:

- ✓ SAAS: Software as a Service provides the required software, network and operating system to the users. Users don't need to install them in their hardware. It is an application that can be accessed from anywhere in the world only if we have a computer with an internet connection.

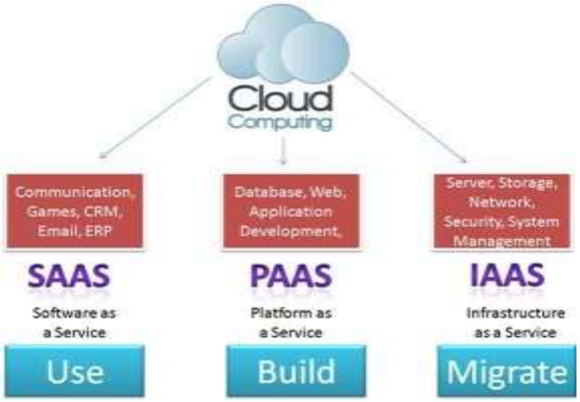
Cloud
Computing
Communication, Games, CRM, Email, ERP
Database, Web, Application Development,
Server, Storage, Network, Security, System Management
SAAS
Software as a Service
PAAS
Platform as a Service
IAAS
Infrastructure as a Service
Use
Build
Migrate

Figure 1: Different cloud services

- ✓ PAAS: Platform as a Service provides network and operating system to users. It is a platform for the developers to create their own application. At this layer user don't need to manage their virtual machines and no need to manage an operating system.

- ✓ IAAS: Infrastructure as a Service also known as *"hardware as a service"*. It's about the physical environment of cloud where it provides the storage space, networking and other needed resources. The user has the control on storage, network.

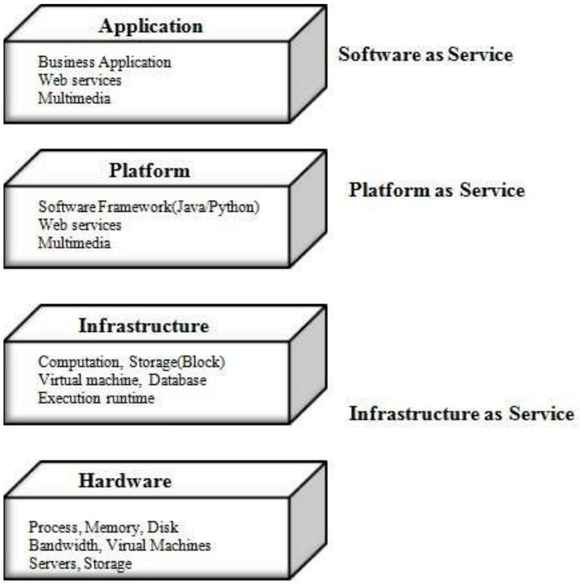

Figure 2: Layered Architecture of cloud services

Application layer is the most utilized layer of cloud computing where the users deploy their applications. Platform layer is useful to run applications for the user. Infrastructure layer enables user request for computing resources by accessing suitable resources and deploy huge numbers of virtual machines (*VMs)* on hardware. The hardware layer is referred to as server layer. It represents the physical hardware that provides actual resources. Hardware resources are of low cost.

IV. Trapdoor Generation:

Users register their identity tokens so as to get secrets to rewrite the info that they're allowed to access. Users register solely those identity tokens associated with the Owner’s sub ACPs and register the remaining identity tokens with the cloud in a very privacy conserving manner. It ought to be noted that the cloud doesn't learn the identity attributes of Users throughout this part. Once Users register with the Owner, the Owner problems them 2 set of secrets for the attribute conditions in command that are gift within the sub ACPs in ACPB cloud. The Owner keeps one set and offers the opposite set to the cloud. 2 totally different sets are employed in order to forestall the cloud from decrypting the Owner encrypted knowledge.

V. Ranked Keyword Searching

As cloud computing has become an integral part of IT industry, data owners share their outsourced data. Due to these vast amounts of information available on WWW, large number of users attempts to retrieve certain specific data files they are interested in. One of the most popular ways to do so is through keyword based search. Keyword searches are done to utilize cloud data for a certain query. Such keyword search techniques allow users to selectively retrieve files of interest and have been widely applied in plain text search scenarios (C.wang). Great efforts have been made for facilitating users via keywords search. However, there are few researchers about entertaining the exact user query and presenting a ranked URL list according to it. Keywords searchers are typically done in such a way that users can utilize clouds to query a collection (7). To eliminate unnecessarily network traffic by not sending back the irrelevant data, ranked keyword search is used. This technique is highly desirable in the "pay-as-you-use" cloud paradigm. For privacy protection, such ranking operation should not leak any keyword related information. To improve the search result accuracy as well as to enhance the user searching experience, it is necessary for such ranking system to support -keyword search, as single keyword search often yields far too coarse results (5). The information is retrieved from the matching files to calculate the relevance scores of given request. If ranking system supports ple keyword search then, it is possible to improve the search result accuracy as well as user searching experience can be enhanced. In all web search engines, users provide a set of keywords instead of only one keyword to indicate that they are interested in a particular area. Each keyword in the user query is used to narrow down the search process.

VI. Proposed System

There are three main actors present in these activities: cloud server, data owner, and data user. Data owner have her own sets of documents, to maintain these documents locally is become difficult task. Maintain and stored the documents locally are expensive for storage and it arises computational overhead. Hence data owner motivate to outsource their sets of documents on cloud to get more flexibility.

But before migration process, the data privacy issue is arises in front of owner, hence to maintain the security and privacy she used encryption methods and outsource the data in encrypted form and expects the cloud server to provide keyword retrieval service to data owner himself or other authorized users. Information leakage would affect the data privacy which is unacceptable to data owner. The data user is sanctioned to process keyword retrieval over the outsourced data. The data user encrypts the query and sends it to the cloud server that returns the pertinent files to the data user. Afterward, the data user can decrypt and make use of the files.

A. Vector space Model

It is used for accurate ranking. TF-IDF rule is used to find the accurate ranking and similarity measures. Where TF denotes occurrence count of term within a document and IDF is obtained by dividing the total number of documents in collection by number of document containing the term. It gives the top-k retrieval result. IDF =total number of documents in collection/ number of documents containing the term.

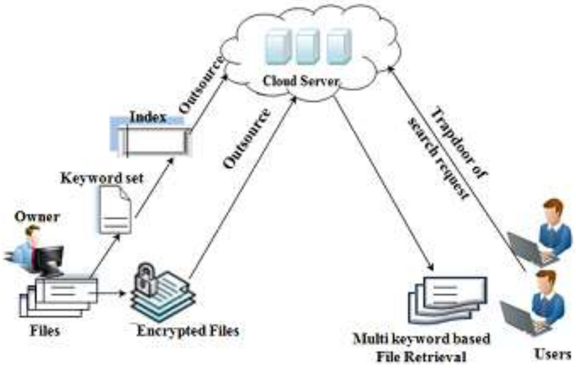

Fig. 3. Architecture of proposed system

B. Enhance Secure Index Scheme To achieve accurate -keyword ranked search, we adopt the cosine measure to evaluate similarity scores. In particular, we divide the original long document index vector into ple sub index vectors such that each sub index represent subset of keyword and becomes a part of ith level of index tree as shown in proposed system. The query vector is divided in same way as document index vector. The final similarity score for document 'd' can be obtain by summing up the score of each level. Based on these similarity score, the cloud server determine the relevance document d to query Q and send top most relevant document to user. By using level wise secure inner product scheme, the document index vector and query index vector are both well protected.

C. MD Algorithm

MD algorithm is used to find k-best match in database that is structure as MDB-tree. MDB tree represents by attribute domain and each attribute in that domain has attribute value.

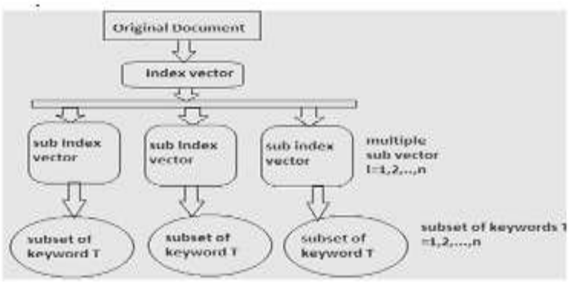

Fig. 4. Mechanism of document index formation

D. Check File Status

Proposed system announces a third party auditor to audit user file request for checking integrity of corresponding file. Audit result from third party would be helpful for cloud service provider to enhance cloud based service platform.

Proposed Algorithms

A. *Algorithm for Top Result selection:*

```
1)  Input
Take variable 'k' like a number and list source of selected item
2)  Initialization:
Set pointers tk & tid as a null
3)  Iteration phase
        a.  For all i ϵ source do
            Insert(tk,( i, index))
        b.  End for
        c.  For all tuple ϵ tk do
            tid.append(tuple[1])
        d.  End for
4) Output:
tid
```

B. *Algorithm for Insertion:*

```
    1)  Input
Take list tk to stored the top scoring items
Tuple( i,index)
    2)  Iteration
        a.  If length(tk) < k then
Insert( i, index) into tk in ascending order of items
        b.  Else
For all element ϵ tk do
If i< element[0] then Continue
Else  Discard tk[0],  insert( i, index) into tk in ascending order of item
EndIf
EndFor
EndIf
```

VII. Experimental Result

Some outcomes are resulting from this scheme:

A. Response Time

Fig.3 shows a graph in which time require to get search result after adding number of documents in database. If database size increases then time require to get result increases.

Results must require less time for MD search as compare to MRSE technique.

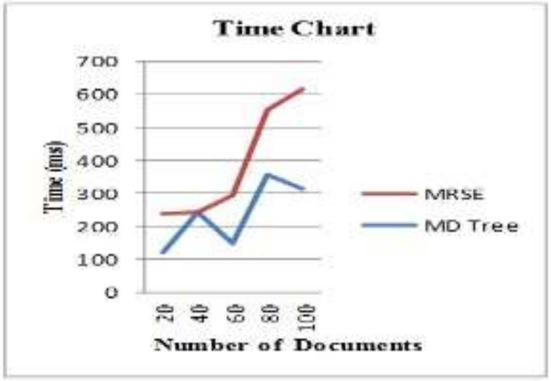

Fig. 5. Response Time

B. Encryption time

Fig.4 shows a graph in which graph shows the expected comparative analysis for time requires to encrypt keywords using both techniques.

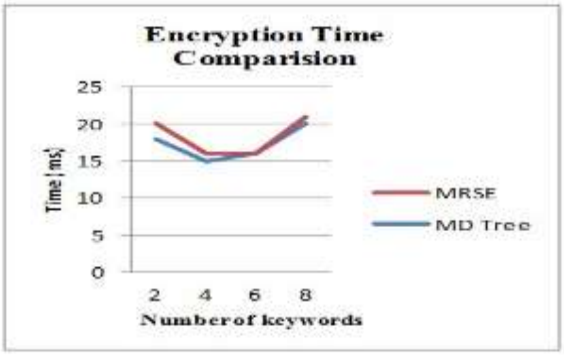

Fig. 6. Encryption time comparison

VIII. Conclusion & Future Scope

The previous work mainly focused on providing privacy to the data on cloud in which using -keyword ranked search was provided over encrypted cloud data using efficient similarity measure of co-ordinate matching. The previous work also proposed a basic idea of MRSE using secure inner product computation. There was a need to provide more real privacy which this paper presents. In this system, stringent privacy is provided by assigning the cloud user a unique ID. This user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the user's data on cloud from the CSP and the third party user. Thus, by hiding the user's identity, the confidentiality of user's data is maintained. In this paper, the asserting problem of searching encrypted cloud data using ranked -keyword (MRSE) is defined and solved. Out of distinct -keyword semantics, the adequate similarity measuring of "coordinates matching" and "inner product similarity, i.e., possibilities of many matches for capture the documents from query search perceptible evaluations for similarity measures. Adopting the basic idea for the MRSE based on secure inner product computation and archive privacy requirements in two distant thread models. Experiments based on the real-world data further showing an indeed advent of low overhead on computation and communication. In future, the cloud server is treated as entrusted state, the integrity checking of the rank order in search results analyze.

References

[1] Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li "efficient and expressive keyword search over encrypted data in cloud", IEEE JOURNAL OF , VOL. , NO. , 2016.

[2] Hongwei Li, Yi Yang,Tom H. Luan, Xiaohui Liang, Liang Zhou, Xuemin (Sherman) Shen, "Enabling FineGrained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data", IEEE Transactions On Dependable And Secure Computing, Vol. 13, No. 3, May/June 2016.

[3] Wei Zhang, Yaping Lin, Sheng Xiao, JieWu, Siwang Zhou, "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing", IEEE Transactions On Computers, Vol. 65, No. 5, May 2016.

[4] Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, Yingjiu Li, "Efficient and Expressive Keyword Search Over Encrypted Data in Cloud", IEEE Transactions on Dependable and Secure Computing Journal Of , Vol. , No., 2016.

[5] Chi Chen, Xiaojie Zhu, Peisong Shen, Jiankun Hu, Song Guo, Zahir Tari, Albert Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, April 2016.

[6] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, Fengxiao Huang", Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement," IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 9, September 2016.

[7] Zhihua Xia, Xinhui Wang, Xingming Sun,Qian Wang, Member, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 2, February 2016.

[8] Jingbo Yan, Yuqing Zhang, Xuefeng Liu, "Secure Multikeyword Search Supporting Dynamic Update and Ranked Retrieval", Services and applications, China Communications, 2016.

[9] Chia-Mu Yu, Chi-Yuan Chen, and Han-Chieh Chao, "Privacy-Preserving Multi-keyword Similarity Search Over Outsourced Cloud Data", 1932-8184 © 2015 IEEE Systems Journal.

[10]Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou, Hui Li, "Verifiable PrivacyPreserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 11, November 2014.

Authors

Basivireddy Suresh Kumar, Pursing M.Tech in Department of Computer Science and Engineering from D.N.R College of Engineering & Technology, Bhimavaram, Andhra Pradesh ,West Godavari, 534201,India. His area of Interest include Cloud Computing.

Dr. B V Ram Kumar M.E, Ph.D is working as a Professor, Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India, with an experience of 23 years.

Dr. G. Satyanarayana is working as a Professor and HOD in the Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India.