Efficient and Empiric Keyword Search Using Cloud

S.S. Swethapriyadarshni[1], S.Swathi Priya[2], P.Yuvarani[3], K.Hemapriya[4]

[1'2'3]Panimalar Institute of Technology
[4]Assistant Professor, Dept. of Computer Science Engineering, Panimalar Institute of Technology, Chennai, TamilNadu, India

---***---

Abstract - *Cloud is a Centralized Architecture Server, which serves as a platform for every user of the cloud wanted to store data and sensitive information's in safe secured storage space. The next logical stage in the growth of on-demand information technology services and products is cloud computing. Cloud computing will rely on virtualized resources to a considerable extent. Cloud computing allows IT skills to be reused, and it always includes current computing services such as distributed and grid computing. Users can perform a keyword-based search over encrypted material with searchable encryption. The majority of currently available searchable encryption systems are based on a single cloud server approach, which has some drawbacks, such as a single point of failure and hostile insiders. The multi cloud server strategy, on the other hand, provides more data availability and security. However, transferring existing keyword search strategies to the multi cloud will result in higher storage and search expenses, with no discernible improvement in data security. In addition, unlike single cloud, a challenge in a multi cloud environment is how to adequately check query integrity when certain cloud servers return inaccurate or incomplete data. We offer an iterative encryption approach to assure file privacy even if numerous cloud services collude with one another to ensure data security.*

***Key Words*: Cloud computing, Cloud Server, Encryption, Decryption, Multicloud, AES**

1. INTRODUCTION

Cloud computing has several attributes, blockchain, forward approach, and cryptosystem-based approaches are accustomed to preserving security. The cloud infrastructure has several characteristics they're remotely hosted, ubiquitous, and commodified. Currently, several firms are delivering cloud services example Google, Microsoft, etc… Virtualization is an associate degree abstraction of execution of the cloud, so virtual machines are used. To preserve the info, the info is encrypted before outsourcing it to the cloud. Cloud sourcing is turning into a giant deal as a result of its high scale usage and has inexpensive suppliers. There are also problems concerning the policy and access that are overcome by the cloud organization. One of the main challenges of the cloud is the constant net throughout the storage of information. Cloud Computing is the sought-after network access split pool organized computing riches.

1.1 SCOPE OF THE PROJECT

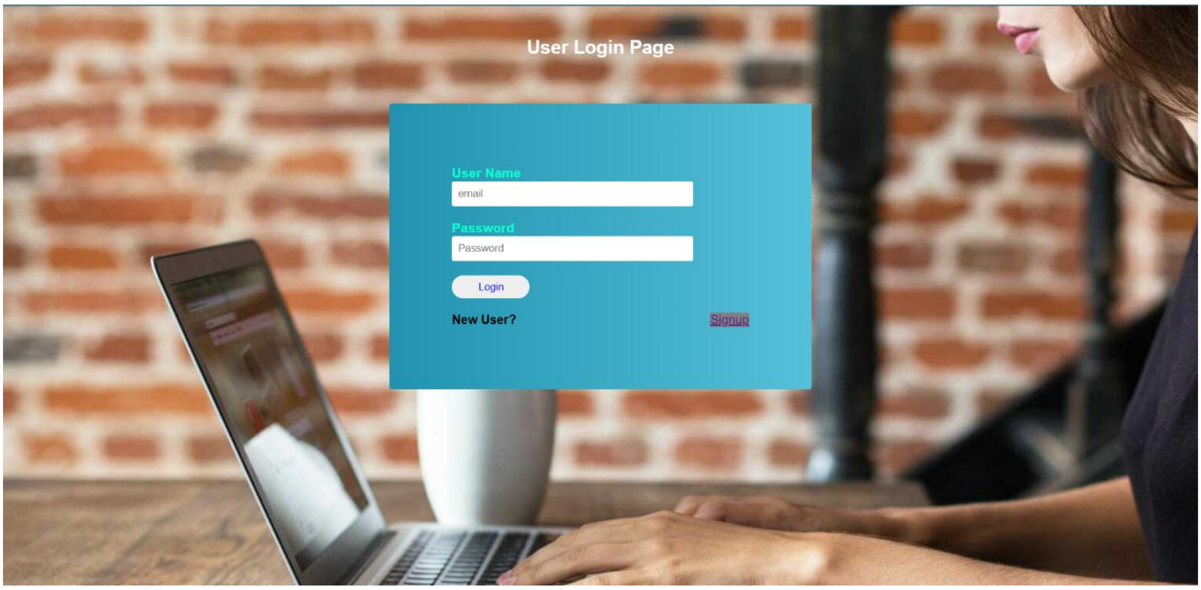
With searchable encryption, users can do a keyword-based search across encrypted material. The bulk of searchable encryption solutions currently available are based on a single cloud server architecture, which has several disadvantages such as a single point of failure and hostile insiders. The use of several cloud servers, on the other hand, increases data availability and security. Transferring existing keyword search strategies to the multicloud, on the other hand, will increase storage and search costs while providing no noticeable improvement in data security. One of these services is Amazon Elastic Compute Cloud (EC2), which allows users to have a virtual cluster of computers available at all times through the Internet. On AWS, virtual computers have hardware central processing units (CPUs) and graphics processing units (GPUs) for processing, as well as local/RAM memory, hard disk/SSD storage, a choice of operating systems, networking, and pre-loaded application software such as web servers, databases, and customer relationship management (CRM). The project's goal is to integrate keyword search across various clouds so that users can quickly locate a specific file or data, and to prevent the involvement of third parties so that data is secure and protected.

1.2 EXISTING SYSTEM

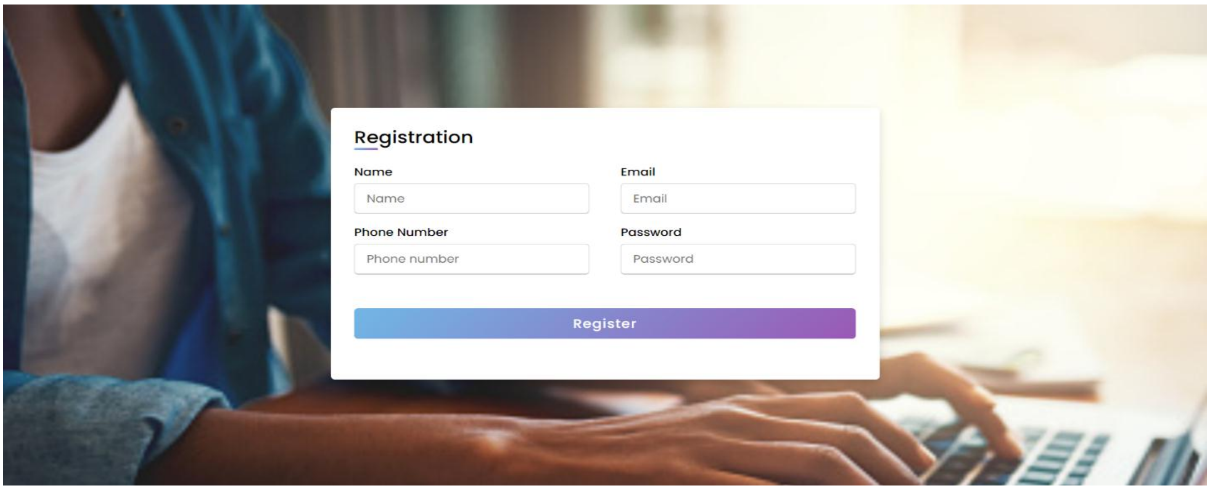
Without needing to learn the plaintexts, searchable encryption allows a cloud server to conduct keyword searches on behalf of data users over encrypted data. The majority of currently available searchable encryption systems, on the other hand, only support single or conjunctive keyword searches, and the few schemes that can perform expressive keyword searches are computationally inefficient because they are built from bilinear pairings over composite-order groups. In existing systems, an expressive public-key searchable encryption technique in the prime-order groups outperforms existing schemes significantly by allowing keyword search rules to be defined in conjunctive, disjunctive, or any monotonic Boolean formulas. When a user obtains data from a concerned person via the internet, unknown or invalid users may gain access to the data stored on a central server or database. It could result in data being lost or altered by a third party. Most existing PEKS methods, regardless of search authorisation, focus on data consumers' rich search functionalities. The framework allows clients to send encrypted data to the cloud, allows users to search for documents using different keywords, and allows them to check the server's response.

2. PROPOSED SYSTEM

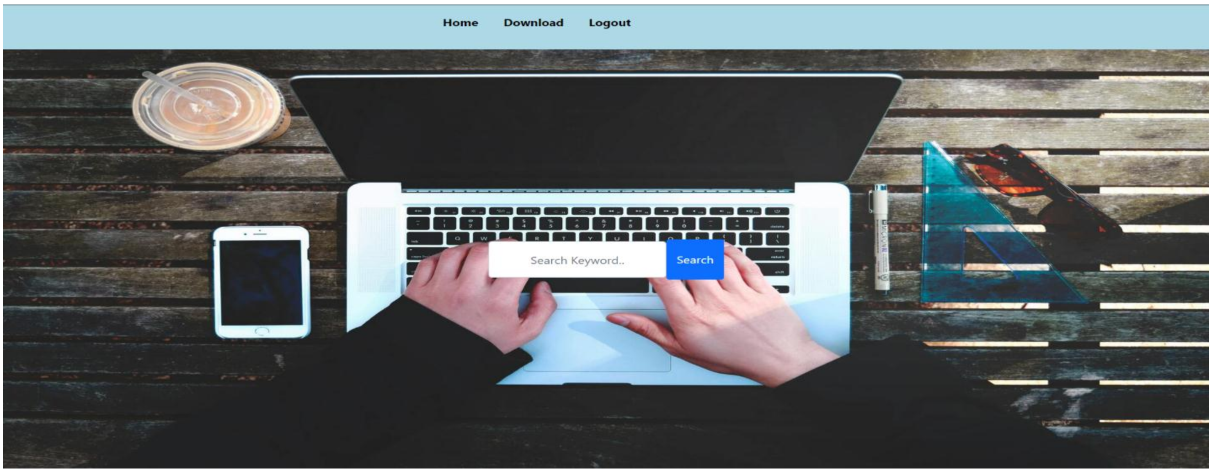
Encrypting a file, then making n copies of it, and distributing the n copies to n cloud servers is a straightforward file distribution solution in numerous clouds. Users can still retrieve the file even if (n-1) cloud servers are offline in this situation, indicating that this distribution mechanism is highly reliable. The cloud server is merely aware that if it engages in unethical behavior, it will almost certainly be discovered. The suggested design reduces storage overhead on both the client and user sides. The retrieval time lowers as the number of documents increases, cutting storage costs for both parties. However, this method necessitates an excessive amount of storage overhead. Furthermore, because each cloud server has access to the entire encrypted file, we build a secure and reliable file distribution strategy in various clouds to strike a better balance between storage overhead, privacy, and reliability. We present an iterative encryption strategy inspired by the two-layer encryption scheme to preserve the privacy of data files even if numerous cloud servers start a collusion attack at the same time. In this system, users can also produce a unique code to gain access to a record from an authorized individual. It will provide users with a safe access method as well as protect unknown individuals from dangerous activities.



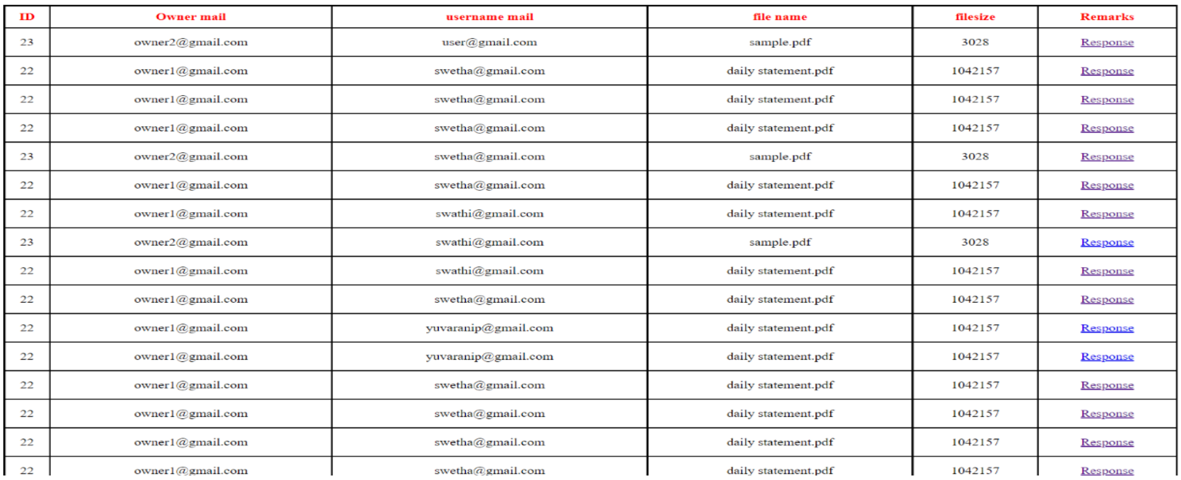
Output-1: User login page



Output-2: Registration page

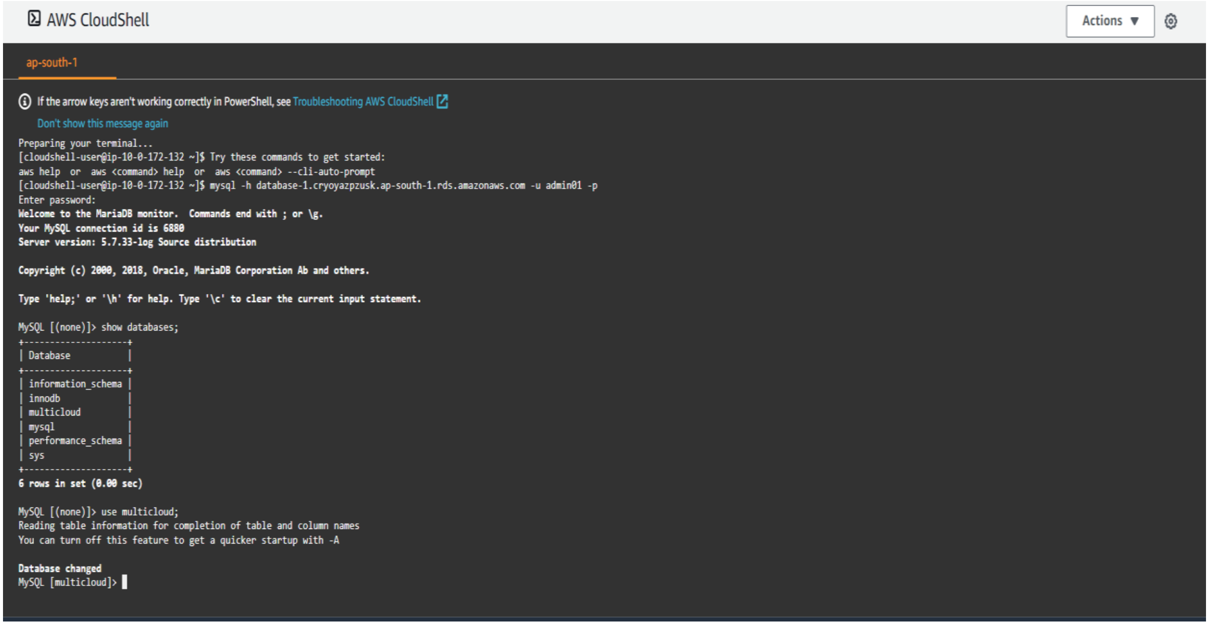


Output-3: Keyword Searching page



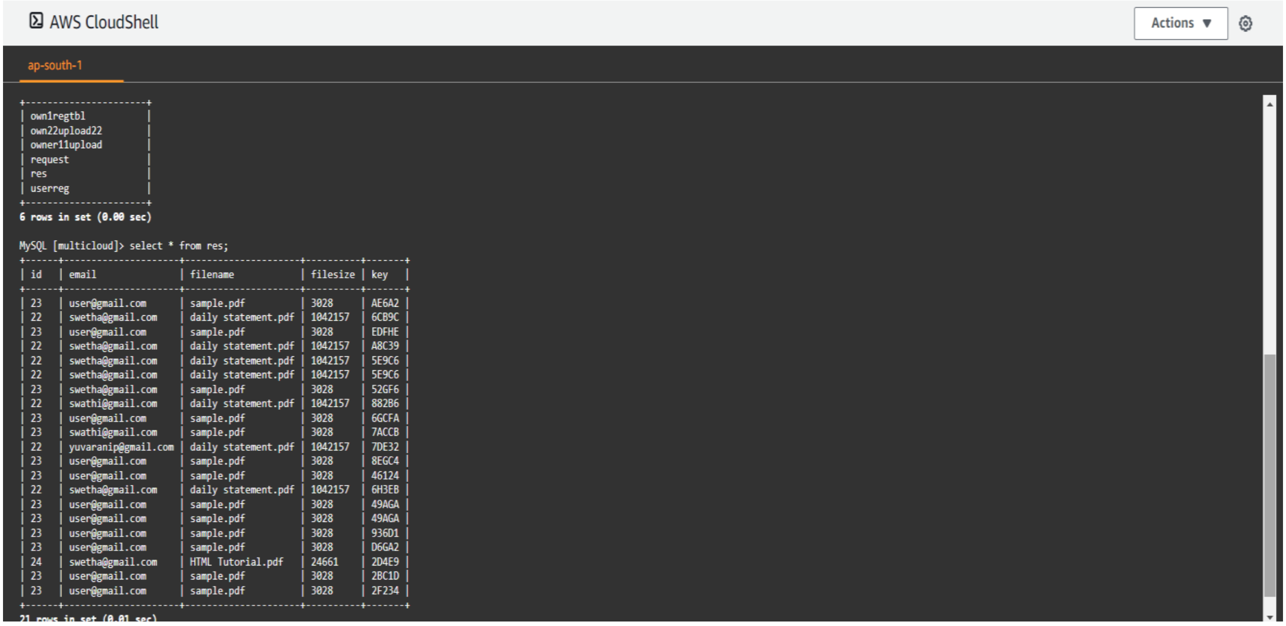
ID	Owner mail	username mail	file name	filesize	Remarks
23	owner2@gmail.com	user@gmail.com	sample.pdf	3028	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
23	owner2@gmail.com	swetha@gmail.com	sample.pdf	3028	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swathi@gmail.com	daily statement.pdf	1042157	Response
23	owner2@gmail.com	swathi@gmail.com	sample.pdf	3028	Response
22	owner1@gmail.com	swathi@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	yuvaranip@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	yuvaranip@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response
22	owner1@gmail.com	swetha@gmail.com	daily statement.pdf	1042157	Response

Output-4: Response page


AWS CloudShell
Actions ▼
ap-south-1
If the arrow keys aren't working correctly in PowerShell, see Troubleshooting AWS CloudShell
Don't show this message again

```
Preparing your terminal...
[cloudshell-user@ip-10-0-172-132 ~]$ Try these commands to get started:
aws help  or  aws <command> help  or  aws <command> --cli-auto-prompt
[cloudshell-user@ip-10-0-172-132 ~]$ mysql -h database-1.cryoyazpzusk.ap-south-1.rds.amazonaws.com -u admin01 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 6880
Server version: 5.7.33-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| multicloud         |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.00 sec)

MySQL [(none)]> use multicloud;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [multicloud]> 
```

Output-5: AWS Cloud shell



```
+---------------------+
| own1regtbl          |
| own22upload22       |
| owner11upload       |
| request             |
| res                 |
| userreg             |
+---------------------+
6 rows in set (0.00 sec)

MySQL [multicloud]> select * from res;
+------+---------------------+---------------------+----------+-------+
| id   | email               | filename            | filesize | key   |
+------+---------------------+---------------------+----------+-------+
| 23   | user@gmail.com      | sample.pdf          | 3028     | AE6A2 |
| 22   | swetha@gmail.com    | daily statement.pdf | 1042157  | 6CB9C |
| 23   | user@gmail.com      | sample.pdf          | 3028     | EDFHE |
| 22   | swetha@gmail.com    | daily statement.pdf | 1042157  | A8C39 |
| 22   | swetha@gmail.com    | daily statement.pdf | 1042157  | 5E9C6 |
| 22   | swetha@gmail.com    | daily statement.pdf | 1042157  | 5E9C6 |
| 23   | swetha@gmail.com    | sample.pdf          | 3028     | 52GF6 |
| 22   | swathi@gmail.com    | daily statement.pdf | 1042157  | 882B6 |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 6GCFA |
| 23   | swathi@gmail.com    | sample.pdf          | 3028     | 7ACCB |
| 22   | yuvaranip@gmail.com | daily statement.pdf | 1042157  | 7DE32 |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 8EGC4 |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 46124 |
| 22   | swetha@gmail.com    | daily statement.pdf | 1042157  | 6H3EB |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 49AGA |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 49AGA |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 936D1 |
| 23   | user@gmail.com      | sample.pdf          | 3028     | D6GA2 |
| 24   | swetha@gmail.com    | HTML Tutorial.pdf   | 24661    | 2D4E9 |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 2BC1D |
| 23   | user@gmail.com      | sample.pdf          | 3028     | 2F234 |
+------+---------------------+---------------------+----------+-------+
21 rows in set (0.01 sec)
```

Output-6: Fetched data from AWS Cloud shell

3. CONCLUSIONS

In this, we propose a solid and certain keyword search conspire in different mists, which permits the information client to perform catchphrase search in a safe, dependable, and unquestionable way. To begin with, we propose a solid and dependable document appropriation conspire, which guarantees security through iterative encryption and dependability by presenting RS deletion code innovation. Second, we plan a Bloom channel tree file structure and extend it to a multi cloud climate. Third, we execute a viable trustworthiness confirmation calculation that can rapidly check the respectability of inquiry results and recognize pernicious cloud servers. At long last, we do security investigation and exploratory assessment to check the security and viability of our plan. For the future work, first, we will investigate a quicker and more effective record dissemination conspire that permits clients to bear lower reproduction costs. Second, we will stretch out the protected hunt plan to accomplish fluffy question, positioning inquiry, and multi watchword question.

REFERENCES

[1]. Yunhong Zhou, Shihui Zheng, and Licheng Wang, "Privacy-Preserving and Efficient Public Key Encryption with Keyword Search-Based CP-ABE in Cloud", 13 October 2020.

[2]. Qingji Zheng Shouhuai Xu Giuseppe Ateniese, "VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data", the University of Texas at San Antonio, USA Sapienza University of Rome, Italy and Johns Hopkins University, USA.

[3]. Mrs. Zabiha Khan, Assistant Professor, Dept. of CSE, Ghousia College of Engineering, Karnataka, India, Ms. Kamala Kumari, B. K, Rumana Iffath, Saima Ahmed, Zaiba Tabassum UG Students Ghousia College of Engineering, Ramanagaram, "Review of Attribute-based Keyword Search Authorization in Cloud", www.ijert.org NConPCS - 2017 Conference Proceedings Special Issue - 2017.

[4]. XINRUI GE, JIA YU, CHENGYU HU, HANLIN ZHANG, AND RONG HAO, 1. College of Computer Science and Technology, Qingdao University, Qingdao 266071, China, "Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing", date of current version September 7, 2018.

[5]. Lincei, Chungen Xu, Lei Xiaoling Yu, and Cong Zuo, "Verifiable Identity-Based Encryption with Keyword Search for IoT from Lattice", Accepted: 24 February 2021.

[6]. Shangping Wang, Jian Ye, Yaling Zhang, China, "A keyword searchable attribute-based encryption scheme with attribute update for cloud storage" May 24, 2018.

[7]. Rui Zhang, Rui Xue, Ting Yuyz, and Ling Liux, "PVSAE: A Public Verifiable Searchable Encryption Service Framework for Outsourced Encrypted Data", Qatar, Email: tyu@qf.org.qa College of Computing, Georgia Institute of Technology, Atlanta, GA, USA, Email: lingliu@cc.gatech.edu.

[8]. A Shiny, Jayanth Das, M Venkat Aravind, C A Anirudh Srivatsaa, M Rahul, "Cloud Server Misbehavior Detection Using Ranked Keyword Search Results Verification", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-4, April 2019.

[9]. R. SaiVenkata Siva Kumar, T.P.Anithaashri, "Enhancement Of Cloud Data Search Using Symmetric-Key Based Verification", Chennai, anithaashritp.sse@saveetha.com, European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 08, 2020.

[10]. Devi Thiyagarajan, R. Ganesan, "USER VERIFIABLE MULTIPLE KEYWORD SEARCH SCHEME USING THE MERKLE TREE FOR OUTSOURCED DATA IN THE CLOUD", International Journal of Technology (2017) 4: 591-600 ISSN 2086-9614, (Received: November 2015 / Revised: February 2017 / Accepted: July 2017).