JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Improving Security And Encryption Based Data Sharing In Cloud Computing

Tejas Shitole[1], Meghali Waghmode[2],
Ritesh Sinkar[3], Chaithanya Nagoshe[4]

Department of E&TC, SKNCOE, SPPU, Pune

Abstract—**Data sharing is a convenient and economic service supplied by cloud computing. Data contents privacy also emerges from it since the data is outsourced to some cloud servers. To protect the valuable and sensitive information, various techniques are used to enhance access control on the shared data. In these techniques, Ciphertext-policy attribute-based encryption can make it more convenient and secure. Traditional CP-ABE focuses on data confidentiality merely, while the user's personal privacy protection is an important issue at present. CP-ABE with hidden access policy ensures data confidentiality and guarantees that user's privacy is not revealed as well. However, most of the existing schemes are inefficient in communication overhead and computation cost. Moreover, most of those works take no consideration about authority verification or the problem of privacy leakage in authority verification phase. To tackle the problems mentioned above, a privacy preserving CP-ABE scheme with efficient authority verification is introduced in this paper. Additionally, the secret keys of it achieve constant size. Meanwhile, the proposed scheme achieves the selective security under the decisional n-BDHE problem and decisional linear assumption. The computational results confirm the merits of the presented scheme.**

Keywords— Data Sharing, CP-ABE, Data Confidentiality, Authority Verification, Secret Keys, n-BDHE.

I. INTRODUCTION

Data dealing with organizations in the IT area that provide cloud connections to a wide range of clients, from small businesses to individuals, is referred to as appropriate registering. Individually best adapted figuring suppliers provide customers from all sizes of relationships through circulated registration. join Amazon's EC2 cloud service. Microsoft with Azure and Google Apps, disseminated processing portrayed in essential words as marketing certain IT benefits that are supported on the web, the most well recognized of which are stage as an organization, structure as an organization, and programming as an advantage. The most basic security and assurance problems should be taken into account before any processing is distributed to ensure that a basic market is established. When a system character organization faces several legal and security challenges, it has the opportunity to conduct risk management, final consistency investigations and logging, as well as distributed processing provider subordinate threats. That's why a secure database that enables programming is seen as the fundamental game plan that allows cloud dwellers take full advantage of database features like penetrability, perseverance quality and flexible adaptability without having to share encrypted messages with the cloud provider. Build strategy was inspired to enable customers to perform simultaneous assignments on encoded data; incorporate SQL illuminations that alter the Database structure to ensure information insurance and consistency at the customer and cloud levels, and eliminate any transitional server between cloud customer or cloud supplier. As in any decrypt database as software set-up, the likelihood of a conventional cloud database joining openness, adaptability, and flexibility is demonstrated through a model of Secure database as software that sponsors the implementation of concurrent in addition to free assignments to the remote encoded database from various geographically scattered clients. Existing coding plans and detachment sections, as well as new methods for the linkage of encrypted data with the dependent cloud database, may all be made easier with secure database software. The theoretical exchange discusses the consequences of synchronous and unfettered stakeholder access to blended information for information consistency challenges. As a result of their complex mathematical structure, homographic encryption plans cannot have any significant impact in this unusual case. Cloud masterminds have revised the Se-cure Database's programming architecture, and it no longer presents a go-between or merchant server between stakeholders and cloud providers. encrypts the file and specifies an access structure as ω = manager $\wedge$ (sales department $\vee$ then sends the trapdoor to the cloud server. The latter will search and return the corresponding encrypted documents to the data user.

II. LITERATURE REVIEW

In 2022, Leyou Zhang et.al wrote a paper titled "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing". Encryption using a public key and a keyword search. Different approaches to public-key encryption with keyword search (PEKS) have been proposed since the original work by Boneet al. began.

In 2021, Prof. Shankar Lingam, Sudhakar Kadarla wrote a paper titled "Improving Security And Attribute Based Data Sharing In Cloud Computing" in which Encryption is done using a Searchable Private Key. Different from the traditional public key encryption, searchable public key encryption allows a data owner to encrypt his data under a user's public key in such a way that the user can generate search token keys using her secret key and then query an encryption storage server.

In 2020 Afnan Ullah Khan proposed a technique known as Access Control and Data Confidentiality (ACDC) in his paper titled Data Confidentiality and Risk Management in Cloud Computing. The aim of the paper was to develop a novel scheme that would enforce access control policies on cloud computing scenarios. He used a scenario in Medical/Health care where he came out with the following compostions; Data Owner (Medical centre), Data Consumers (patients, nurses, doctors etc.), Infrastructure Provider and Trusted Authority. The paper focused on Infrastructure as a Service as its deployment model whereas data confidentiality and authentication were achieved through the proposed technique.

In 2019 Sudhansu Ranjan Lenka et.al wrote a paper titled "Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm. As the title of the paper suggests; they implemented both RSA Algorithm and MD5 Algorithm. In this paper, the RSA Algorithm is used for secured communication and file encryption and decryption purpose whilst MD5 Algorithm is used for digital signature as well as covering the tables for unauthorized users. The two algorithm proposed provides the three aspects of security which are Confidentiality, Integrity and Availability.

In 2018 Ali Asghary Karahroudy wrote a paper titled Security Analysis and Framework of Cloud Computing with Parity Based Partially Distributed File System. This paper proposed a technique called Partially Distributed File System with Parity (PDFSP) which is a protocol developed as a modification on the existing GFS/HDFS. This PDFSP has four main components; Client Access Machine, User Public Machine, Cloud Management Server and File Retrieval Server. All these components work together to ensure data being transmitted does not get into wrong hands. This paper addressed the three aspects of security which are Confidentiality, Integrity and Availability.

III. BLOCK DIAGRAM

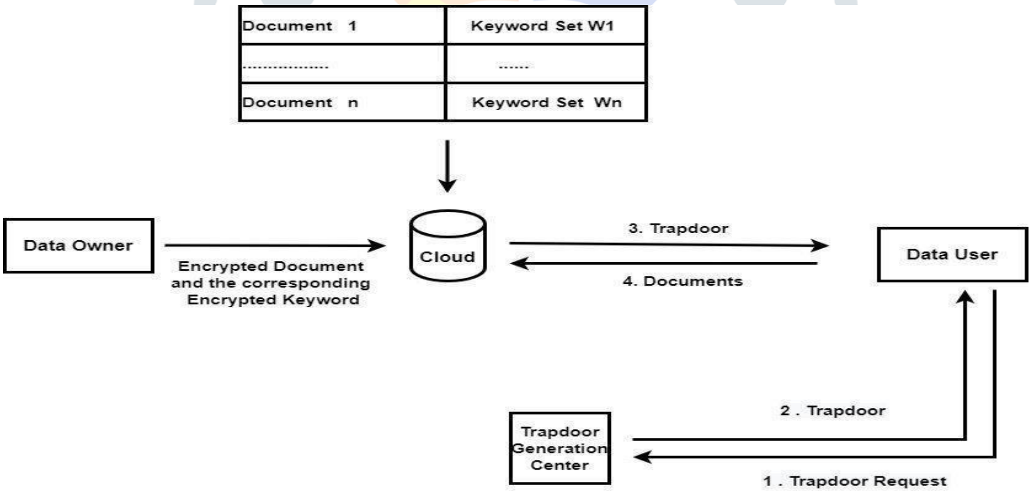


Figure 1: System Architecture of Improving Security And Data Sharing In Cloud Computing

1. The DFD is also called a bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data generated by this system.
2. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as a bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

IV. IMPLEMENTATION

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

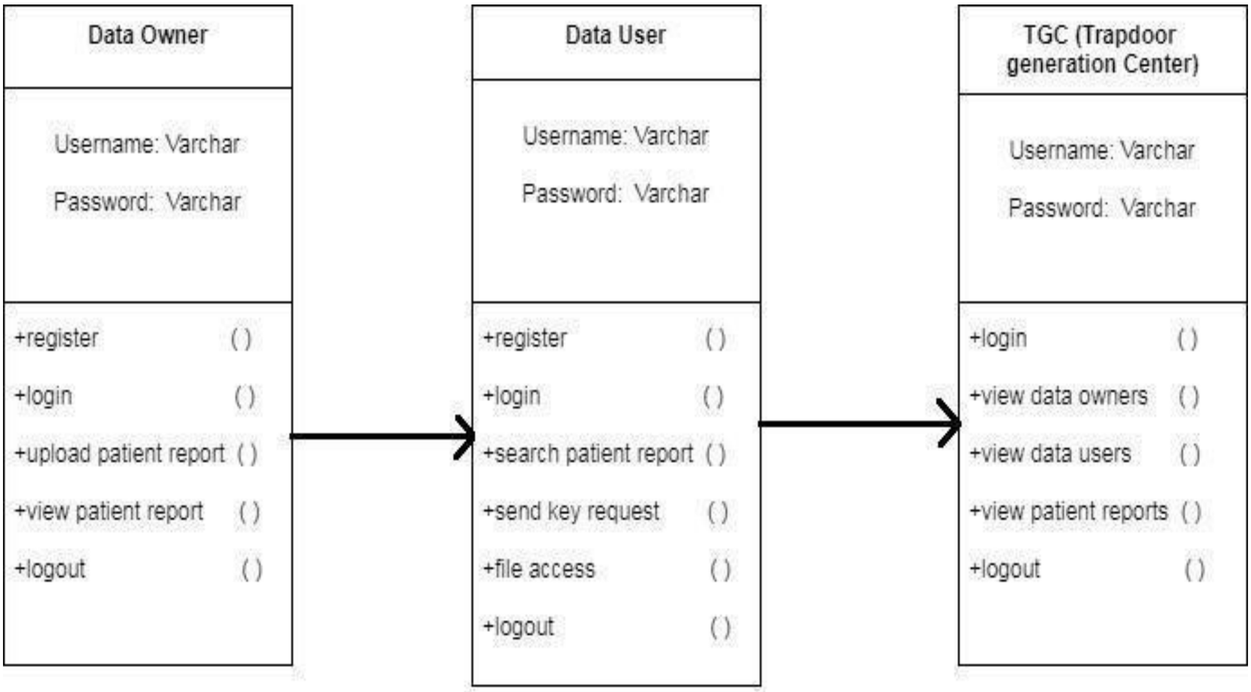


Figure 2: Class Diagram of System

ACTIVITY DIAGRAM OF SYSTEM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

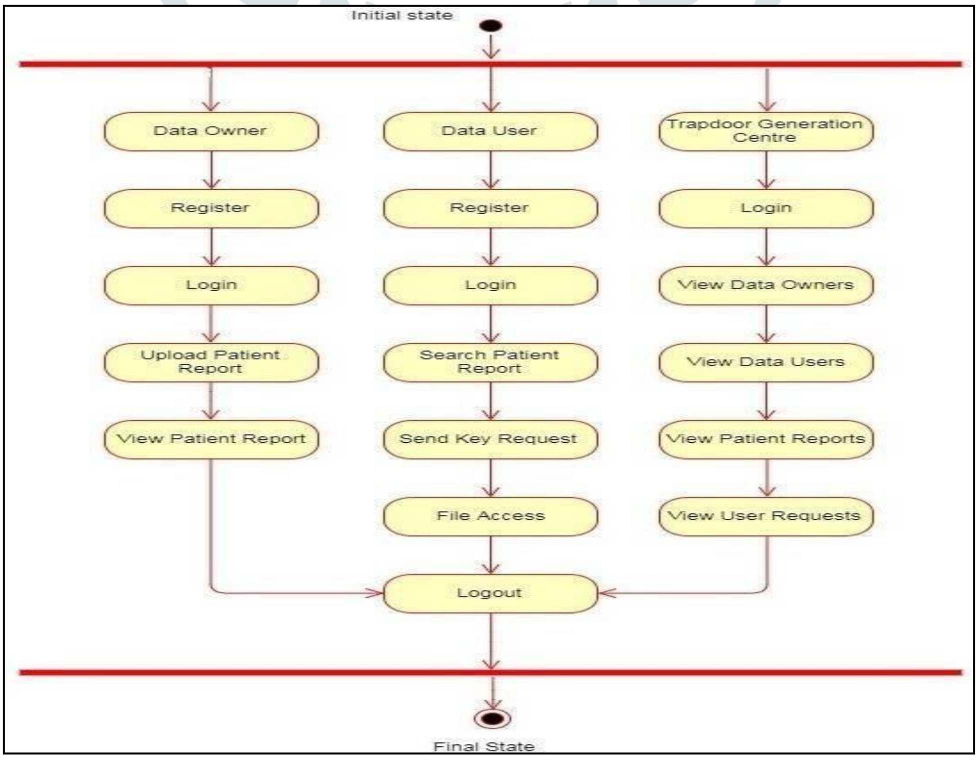
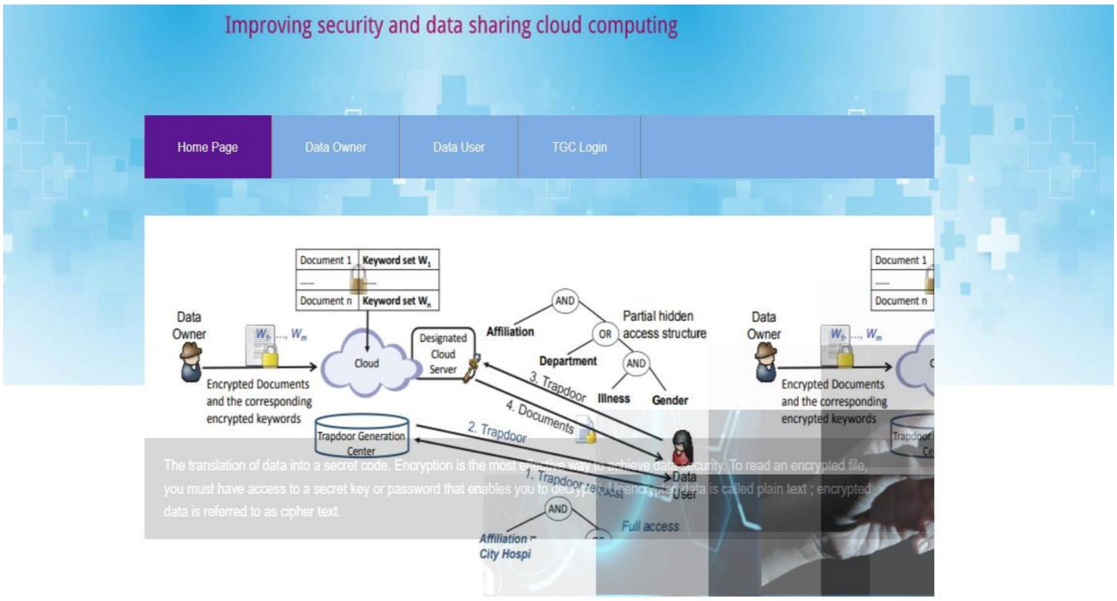


Figure 3: System Architecture

V. RESULT



The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text.

Figure 4: Home Page

After that, a random-access structure is created by picking 2 to 10 keywords at random. According to search engine query data, the average number of terms in a search query is fewer than 10. The policy tree is constructed in such a way that the difference between the node numbers on its left and right branches is less than two for every internal node. Ten trees are generated for each keyword count, and a trapdoor is built into each of those trees. The keyword value information is likewise removed from the traps. There are just keyword names, such as "Illness" and "Position," in the policy tree in the trapdoor.

DATA OWNER:

Data Owner is an entity who owns data, and desired to upload it into the cloud for ease of sharing or for cost saving. The main work of data owner is to define (AES based) access policy, and imposing it on its own data by encrypting the data under the policy before distributing it.

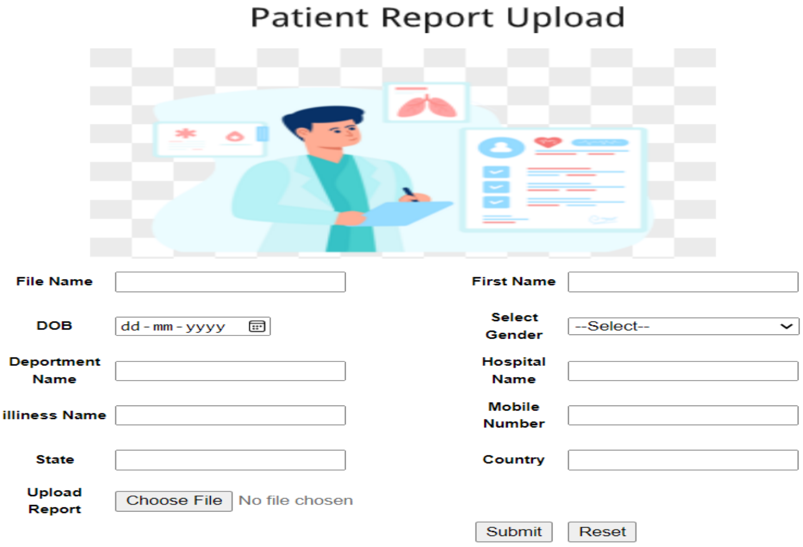

Patient Report Upload

Figure 4.1: Upload Patient Report

DATA USER:

The user is any person who has been authorized by the owner of the information to read, enter, or update that information. The user has the responsibility to use the resource only for the purpose specified by the owner, comply with controls established by the owner, and prevent disclosure of confidential or sensitive information. The user is the single most effective control for providing adequate security.

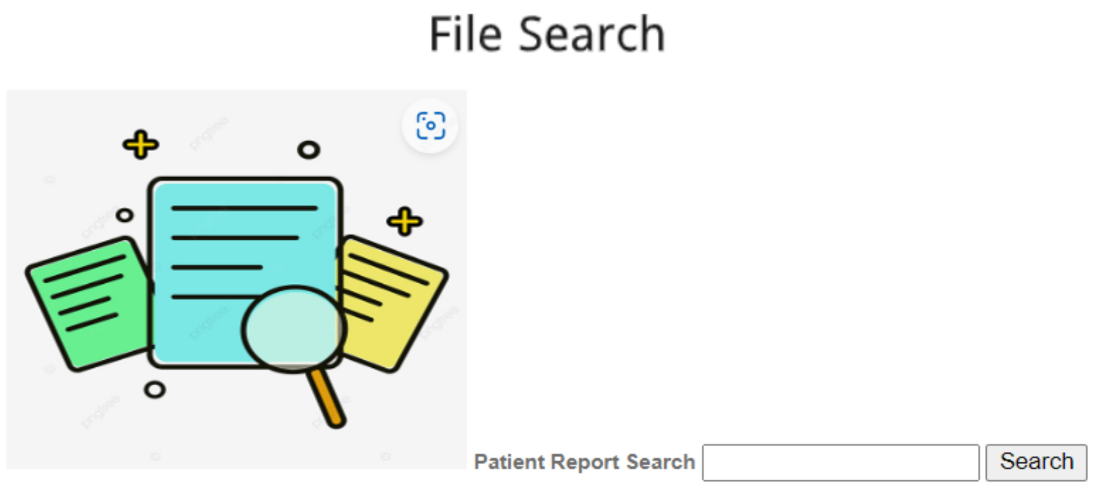
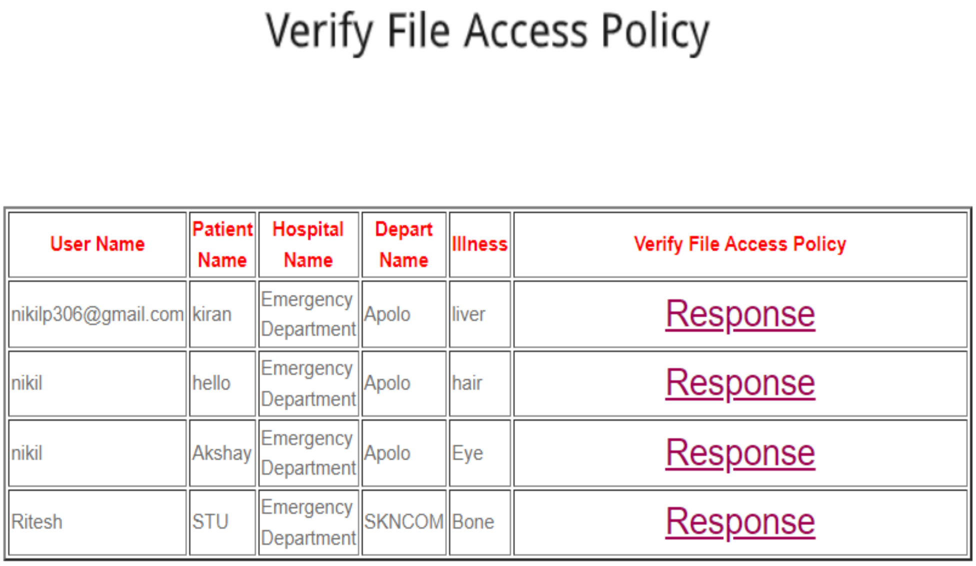


Figure 4.2: Search User Report

TGC:

TGC have all record of patients who are currently active as well as old patient who had taken treatment from the hospital. The patient report which can be visible to TGC only. When any doctor needs any file of patient then he/she need to take permission from TGC. This is necessary for data protection. Figure 4.3 shows TGC file access page where TGC can give permission to doctor by giving response or TGC can't allow permission.



User Name	Patient Name	Hospital Name	Depart Name	Illness	Verify File Access Policy
nikilp306@gmail.com	kiran	Emergency Department	Apolo	liver	Response
nikil	hello	Emergency Department	Apolo	hair	Response
nikil	Akshay	Emergency Department	Apolo	Eye	Response
Ritesh	STU	Emergency Department	SKNCOM	Bone	Response

Figure 4.3: Access Page

VI. CONCLUSION

As part of this article, a new cross-breed distributed computing system for outsourcing and sharing information is discussed. As well as providing search and service in a secure environment, it also provides a large amount of open cloud storage space. A cryptographic method known as open key encryption with a catchphrase glance (PEKS) is implemented in the public key setup, allowing the capacity server to execute the search on encoded information without acquiring the basic plaintexts. The system's encryption frameworks have evolved and been utilized in numerous ways since then, taking into account various future requirements, such as overhead correspondence, search criteria, and increased security. However, there are just a few open-key encryption frameworks that support expressive watchword search approaches, and they are all constructed from inefficient composite arrange gatherings. Open key accessible encryption frameworks in prime-at-range gatherings that can be used to search through various catchphrases in expressive searching recipes based on logic compositions rather than Bilinear Pairing mechanisms, which are comparatively good in results production and processing the search activity were the focus of this paper's design and evaluation.

ACKNOWLEDGEMENT

I would like to express my gratitude to the developers and researchers who have contributed to the development of security and data sharing in cloud computing. Their dedication and hard work have made it possible to achieve security of data using AES encryption techniques. I would also like to express my special thanks of gratitude to my guide Mrs. Meghali Waghmode for their guidance and support in completing my project. Additionally, I would like to thank the large and diverse community of researchers, developers, and enthusiasts who continue to contribute to this field and push the boundaries of what is possible with security in cloud computing.

REFERENCES

1] M. Iswariya and A. Kumarappan, “Refined Search and Attribute-Based Encryption Overthe Cloud Data,” 2022, pp. 205–212.

2] S. Ulukus, S. Avestimehr, M. Gastpar, S. Jafar, R. Tandon, and C. Tian, Private Retrieval, Computing and Learning: Recent Progress and Future Challenges. 2021. Z. Shang, S. Oya, A. Peter, and F. Kerschbaum, Obfuscated Access and Search Patternsin Searchable Encryption. 2021.

3] Y. Lin, L. Xu, W. Li, and Z. Sun, “Attribute Set-Based Boolean Keyword Search over Encrypted Personal Health Records,” Secur. Commun. Networks, vol. 2021, pp. 1–13, Dec. 2021, doi: 10.1155/2021/9023141.

4] N. Almrezeq, M. Humayun, A. E.-A. Ahmed, and N. Zaman, “An Enhanced Approachto Improve the Security and Performance for Deduplication,” Turkish J. Comput. Math.Educ., vol. 12, pp. 2866–2882, Apr. 2021.

5] R. Bhat, M. Kumar K M, and S. N R, “A novel recursive privacy-preserving information retrieval approach for private retrieval,” Int.J. Intell. Inf. Database Syst., vol. 14, Sep. 2021, doi: 10.1504/IJIIDS.2021.10041195.

6] J. Ning, J. Chen, K. Liang, J. K. Liu, C. Su, and Q. Wu, “Efficient Encrypted Data Search with Expressive Queries and Flexible Update,” IEEE Trans. Serv. Comput., 2020, doi: 10.1109/TSC.2020.3004988.

7] M.Jiang and H. Yang, “Secure Outsourcing Algorithm of BTC Feature Extraction in Cloud Computing,” IEEE Access, vol. 8, pp. 106958–106967, 2020, doi: 10.1109/ACCESS.2020.3000683.

8] U. Varri, S. Pasupuleti, and K. Kadambari, “A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, and recent developments,” J. Supercomput., vol. 76, Apr. 2020, doi: 10.1007/s11227-019-03087-y.

9] N. Matsuda et al., “Public-key Searchable Encryption with Index Generation for Shared Database,” J. Inf. Process., vol. 28, pp. 520–536, Jan. 2020, doi: 10.2197/ipsjjip.28.520.

10] Y.-F. Tseng, Z.-Y. Liu, and R. Tso, “Practical Inner Product Encryption with Constant Private Key,” Appl. Sci., vol. 10, p. 8669, Dec. 2020, doi: 10.3390/app10238669.

11] P. DATTA, T. Okamoto, and K. TAKASHIMA, “Adaptively Simulation-Secure Attribute35 SKNCOE. Pune-41, Dept. of E&TC Engineering Hiding Predicate Encryption,” IEICE Trans. Inf. Syst., vol. E103.D, pp. 1556–1597, Jul. 2020, doi: 10.1587/transinf.2019ICP0001.

12] A. Faeq Hussein, A. K. Abbas, Q. Habash, and M. Jaber, An Adaptive Biomedical Data Managing Scheme Based on Blockchain Technique. 2019.

13] L. Xu, W. Li, F. Zhang, and S. Tang, “Authorized Keyword Searches on Public Key Encrypted Data With Time Controlled Keyword Privacy,” IEEE Trans. Inf. Forensics Secur., vol. PP, p. 1, Dec. 2019, doi: 10.1109/TIFS.2019.2957691.

14] B. ali al-maytami, P. Fan, A. Hussain, T. Baker, and P. Liatsis, “An Efficient Queries Processing Model Based on Multi Broadcast Searchable Keywords Encryption (MBSKE),” Ad Hoc Networks, vol. 98, p. 102028, Oct. 2019, doi: 10.1016/j.adhoc.2019.102028.

15] R. Al-Dahhan, Q. Shi, Lee, and Kifayat, “Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption,” Sensors, vol. 19, p. 1695, Apr. 2019, doi: 10.3390/s19071695.

16] S.Fugkeaw, H. Sato, "Improved Lightweight Proxy Re-encryption for Flexible and Scalable Mobile Revocation Management in Cloud Computing", in IEEE 9th International Conference on Cloud Computing (CLOUD), pp: 894-899,2016.

17] X. Wang, F. Xhafa, Z . Zheng and J. Nin, "Identity Based Proxy Re-Encryption Scheme (IBPRE+) for Secure Cloud Data Sharing", 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), pp:44-48,2016.

18] H. Cui, Z. Wan, R. Deng, G. Wang, and Y. Li, “Efficient and Expressive Keyword Search Over Encrypted Data in the Cloud,” IEEE Trans. Dependable Secur. Comput., vol. PP, p. 1, Aug. 2016, doi: 10.1109/TDSC.2016.2599883.

19] Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment," Inform Sciences, vol. 258, pp. 355-370, 2014.

20] Z. Lv, C. Hong, M. Zhang, and D. Feng, Expressive and Secure Searchable Encryptionin the Public Key Setting. 2014.