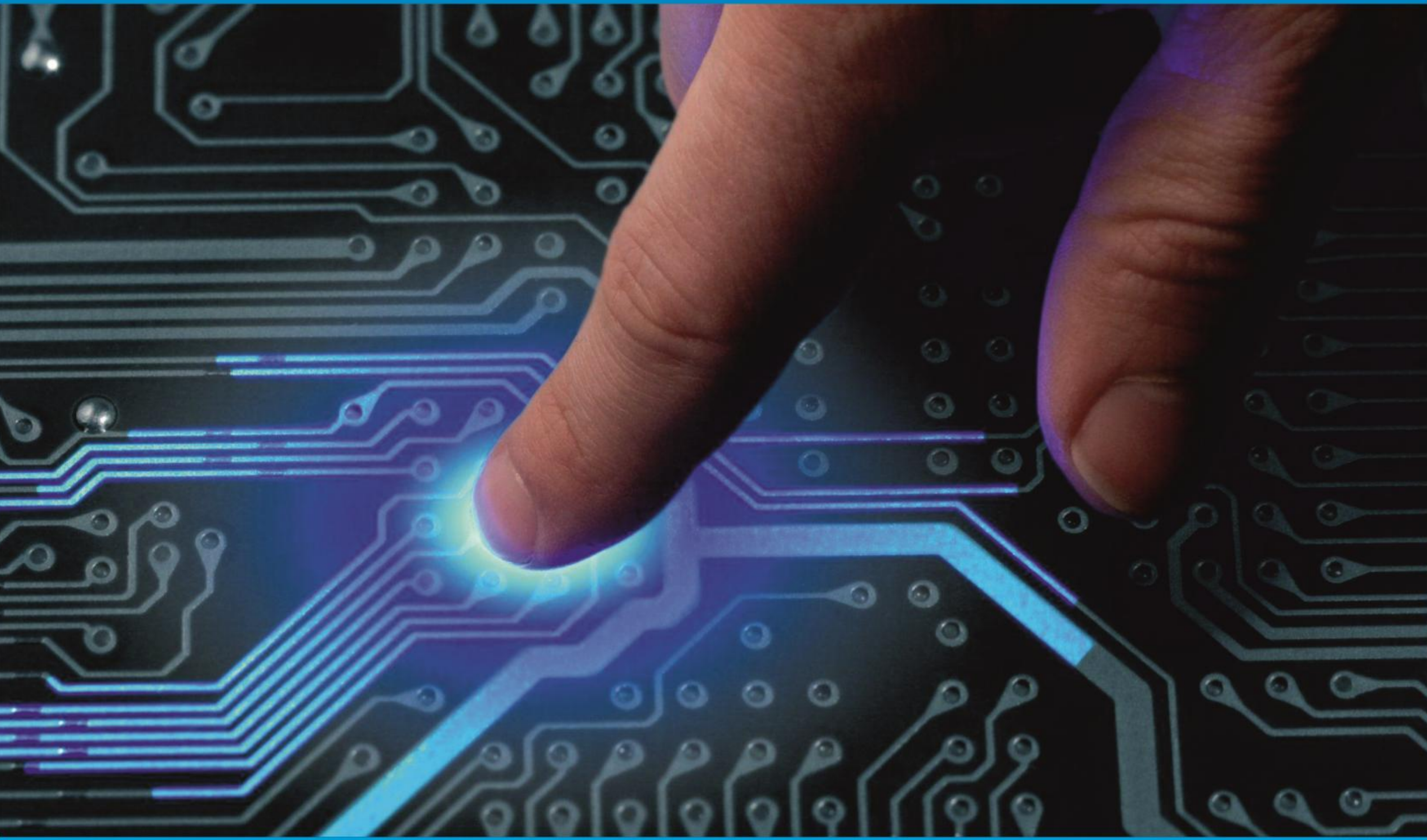
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

A Review on Enabling Search over Encrypted Cloud Data through Blockchain

Pratiksha Dhavale[1], Pratiksha Raut[2], Neelam Divekar[3], Aishwarya Kadam[4], Nagaraju Bogiri[5]

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India[1]

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India[2]

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India[3]

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India[4]

Assistant Professor, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India[5]

ABSTRACT: The rise in the usage of the cloud platform has been momentous in recent years. This is due to the undeniable benefits offered by the cloud storage approach that is incomparable to the costs and other hurdles that need to be crossed for the purpose of achieving the local storage for the same. Cloud storage offers an effective alternative that is better than a local storage solution in almost all aspects. The data stored on the remote cloud platform can be accessed anywhere in the world. The data and the infrastructure does not need to be maintained to allow for seamless integration. Therefore, the increase in cloud storage use corresponds to the services being provided. But there are primary concerns that need to be addressed before being uploaded on the cloud platform, the most important being privacy. Therefore, a number of researches have been analyzed in this survey article for the purpose of improving the data security of the files or the data being stored on the cloud. The prescribed approach will be utilizing the distributed Blockchain framework along with the RCC approach. This will be further elaborated in the upcoming researches.

KEYWORDS: Blockchain Distributed Framework, Reverse Circle Cipher Encryption.

I. Introduction

In recent years, there has been an increase in internet users as there an increased number of devices have been developed to access the internet platform. These devices are in the form of smartphones, laptops, Personal Computers, etc. The users of these devices are connected to the internet and contribute to the rising levels of data being generated on the online platform. This data is huge and it takes up a lot of space on the internet platform. These users also generate large amounts of data that need to be stored on their devices. Even organizations and large corporations need an effective technique to store their data securely.

This need for an effective approach to store, access, and manage the data with ease has led to the development of the Cloud Internet platform. The cloud approach significantly improves the capabilities of individuals and organizations which can be highly problematic to manage and maintain the infrastructure to achieve the storage of data easily. This is ameliorated with the introduction of the cloud platform. This platform has ameliorated the effects of achieving effective and complete outsourcing of the data to avoid these problems such as the ones faced when developing and maintaining the infrastructure for enabling the local storage.

The cloud platform reduces the efforts and improves the storage and the various services offered by it. The cloud storage platform enables services such as the effective remote storage of the customer's data. This allows the cloud platform to provide the respective authorized user access to the data. These services are cost-effective, which leads to a large number of people that were finding their solution for ubiquitous storage. The cloud service is also useful as it can allow the users to utilize the high scalability that can allow the user or an organization to scale up effectively. The scalability is not as expensive as the cost for the upgradation of the local storage solution to achieve effective scalability.

These characteristics of the cloud platform are very useful and enable the effective realization of storage and efficient computation without worrying about the various hardware platforms and their management. Also, the cloud platform allows stable storage, flexible access, easy management, and extremely low prices. This has led major corporations of the earth to utilize the cloud platform to effectively manage and outsource their data.

But the problem in storing large amounts of data on a remote server on the internet platform can lead to various scenarios that will impact the organization regularly. This is also problematic for individuals as their sensitive and personally identifiable information can be effectively be subjected to a data leak or breach. Certain cloud administrators and other individuals can gain unauthorized access to the user data which can be a huge privacy concern. Therefore, to safeguard the data on the cloud platform most of the users encrypt their data before uploading. This ensures that even in the event of a data leak, the data is secure and cannot be accessed by the attacker.

This research article effectively studies the various researches that have been performed for the purpose of enabling effective security to the data on the cloud platform. The encryption of the data makes it highly difficult to perform any search on the encrypted data. Therefore an effective approach has been discussed to achieve the security of the data while maintaining the search capability of the approach. The devised approach in this survey article utilizes the Blockchain Approach along with the Reverse Circle Cipher and Key generation to achieve effective search over the encrypted data being uploaded on the cloud platform. This approach will be outlined in detail in the upcoming editions of this research.

This literature survey paper dedicates section 2 for analysis of past work as a literature survey, and finally, section 3 concludes the paper with traces of future enhancement.

II. RELATED WORK

Jiguo Li et. al. introduced a CP-ABE scheme that can outsource the work of issuing keys, decrypting, and research keywords. The proposed method is efficient as it is required for a particular keyword to download partial decryption ciphertext. The time-consuming pairing process can be outsourced to the provider of cloud service in the suggested scheme, while users can use the light operation [1]. In this manner, customers and trusted authorities can reduce the cost of computing. The proposed system also supports a keyword search function that can greatly improve the performance of communication and further protect the safety and privacy of users.Zhirong Shen et. al. introduced a scalable system that combines fine-grained access control with multi-field keyword study. In the framework, to represent an attribute value, each authorized user gets a set of keys called credentials. An encrypted index to tag keywords and define access policies is followed by each file saved in the cloud. To make a search feature locally and send it to the cloud server for the cloud server to perform search and access control, each user may use passwords and search queries. Finally, the data file corresponding to the search request is received by the user, and access is granted [2]. Then, the research power is newly used through Hierarchical Predicate Encryption (HPE) to enable such a system. The authors present a scheme called KSAC based on HPE. It allows multi-field keyword search and access control services and facilitates the successful updating of access policies and keywords. Chang Liu et. al. introduced the KNK queries graph encryption framework. Lightweight cryptographic primitives such as pseudo-random function and symmetric key cryptographic encryption, not sluggish homomorphic encryption, are only used in the presented graph encryption framework. For a broad range of cloud computing focused on graph data and edge computing applications like social media, electronic maps, methodology review, the presented graph encryption framework is, therefore, advantageous [3]. The proposed device circuit offers a higher degree of protection compared to graph anonymizing methods from the database community, since the graph is encrypted, and the authors do not make any claims regarding attack forms.Rui Li et. al. offers initial privacy while protecting a complex query processing scheme that meets the demands of adaptive security, scalable index size, and efficient query processing [4]. The authors proposed an integrated Bloom Filter (IBF) data structure for indexing for adaptive security. For efficient query transforming and structural opacity, they recommend a balanced binary tree data structure called the Individual Binary Tree (IBT). The authors also proposed a versatile width minimization algorithm and side effect depth minimization algorithm to optimize the search function. To accomplish a scalable and compact index size, they present an IBtree space compression algorithm that removes IBFs redundant information. The authors demonstrate that their scheme is adaptively safe using a random oracle model. The experimental outcome shows that the presented framework is fast in the expression of query processing time and scalable in terms of index size.Hui Cui et. al. developed a cryptographic device called Public Key Encryption with Keyword Search (PEKS) that allows cloud servers to search encrypted data without having to learn the basic text in public parameters. Since then, a diversity of search encryption systems have been presented, for example, in the face of various requirements, the increased burden of communication, increasing search quality, and security. However, there are only a few searchable public clippers that support express keyword search policies, and they are all made up of inappropriate order groups [5]. In this research, the author's focal point on the design and analysis of public-key encryption systems in first-order groups that can be utilized to explore multiple keywords in expression search formulas. Based on an encryption framework depend on the key policy features of a vast universe, the authors introduced a remarkable first-order group searchable encryption system that supports access structures does express in all monotonous Boolean formulas.Boyang Wang et. al. suggested two effective and highly synchronized range SSE schemes, where clients can safely perform range queries on encrypted datasets. As a result, unreliable cloud boundaries can run queries efficiently and accurately but do not learn the question or the client's outsourced data. To align keywords with SSE, the authors convert category queries into a set of keyword queries and change Lizard's Word SSE into building blocks in the presented design. More importantly, the authors use additional and innovative constructs to increase index data and efficiency, where the presented schemes are far more efficient than direct solutions [6].Xiaofeng Ding et. al. presented a Multiple Keyword Keyword Group Search (GMTS) scheme, which is partition based and supports top-of-the-line similarity search on encrypted data. In this framework, the data owner split the dictionary keywords into multiple groups and fixed a search index for every group. On the other hand, to better control the size of the indexes, the authors adopt a list of champions in the presented scheme, where the index of the group of keywords only stores the top documents [7]. CK of the matching keyword (the top-CK documents of the keyword represent the CK documents that have the highest relevance points for that keyword, where C is a positive integer). Also, the authors provide a random translation versus algorithm (RTRA) to strengthen data security, where the data owner creates a binary tree as a search index and assigns a random switch to each node so that the user can assign a random key to each request. Therefore, the data user can modify the query results and paths using different keys, which maintains the high accuracy of the queries. Finally, the authors combine GMTS and RTRA into an efficient and safe solution to the proposed problem.Meng Shen et. al., introduced P3 which provides a new privacy-preserving phrase search system on encrypted, cloud-based data. The authors leverage the reverse index structure to create a secure index that provides greater flexibility and efficiency. The reverse index is one of the most popular and efficient index structures for plain text search. Compared to various self-designed index structures, the reverse index structure can enhance search efficiency and scalability in behavior [8]. To meet the challenge of determining the position relationship of queried keywords on encrypted data, the authors use homomorphic encryption and bilinear maps, which allows clients to obtain accurate search results with cloud servers with only one interaction. Since phrase research is a special case of multi-keyword research, the proposed solution can efficiently perform multi-keyword research jointly. Hui Yin et. al. developed encryption based on the attributes of the searchable ciphertext policy. This allows to simultaneously search for access to encrypted data and have fine-grained control. In fact, by providing the popular CP-ABE schema with search capabilities, the presented design inherits all the benefits of this schema, including security, flexible access policy expressions, and fine-grained command over data access. The authors provide detailed accuracy analysis, performance analysis, etc. of the presented CP-ABSE scheme and security certification. They implement the CP-ABSE scheme and a similar CP-ABKS working scheme[9]. Extensive experiments with real-world data indicate that the presented strategy is superior to CP-ABKS in many ways.Hoang Giang Do et. al. presented the design of a system called BlockDS. This system allows the outsourcing of data collection to the service providers of fluid distribution network. The system utilizes blockchain technology to implement data integrity through a proof of recovery scheme. The private keyword search module is designed to search the encrypted data set while the client controls the encryption for data security[10]. Anonymous credential grants, credential verification, and private keyword search processes are also carried out with the help of blockchain [10].Shan Jiang et. al., offered blockchain-based data management systems with privacy protection and efficient database configuration, dynamic updates, and multi-keyword research functions. The technique of splitting encrypted databases into protocols is common to other blockchain applications. The key contribution is the possibility of finding multiple keywords on an encrypted database on the blockchain and improving its performance in terms of time and financial cost [11]. To do this, the authors recommend using a bloom filter to search for low-frequency keywords and filter the encrypted database using keywords, which greatly reduces the search space.Yu Guo et. Al., Introduced a unique testing strategy leveraging the power of blockchain technology. The Blockchain-enabled SSE scheme has three main parties: data owner, storage servers, and blockchain platform. Servers are the public cloud or individuals who rent their storage resources, while data owners are data users who transfer their encrypted data to storage servers and request their data. And blockchain can be seen as a trusted party to ensure that results are validated by search engines. To make the operation irreversible and reversible, this operation is performed in the form of transactions on this blockchain so that other partners can validate the accuracy of the search and guarantee payment for services. The updated security of operations is protected by the present design [12]. The authors develop a valid online validation scheme that can ensure that the updated results are correct. The proposed design provides guaranteed security and easy network storage. This new primitive encrypted search service provides reliability and maintains further security for updated operations.N. Priya et. al. introduced a framework that influences blockchain innovation to provide protected dispersed information storage through the management of keyword searches. In this proposed work, two existing cloud agents with the symmetric key have been given the best security plans available for keyword verification. Then these methods of encryption developed blockchain methods in these secret key developments, then claimed to authenticate this agent and applied the encryption methodspresent in this Mac layer, then the hash work data security. Serves as a square of the necessary infrastructure and is used in various security applications and conventions, for example, to ensure the reliability of information and the authentication of the root of information. Developments are widely used: they are used to store passwords, in the PC view, in the database [13]. Here authors are using SHA which means a secure hashing algorithm for the need to reduce the square of information and improve information security. Because of this proposed work, the authors can save data management costs and honestly protect privacy. [13].

III. CONCLUSION AND FUTURE SCOPE

The approach for the purpose of enabling effective and useful data security and privacy of the data being stored on the cloud platform. The most effective and useful approach for cloud storage has been increasing in popularity in recent years. This has been noticed in the increased usage of the cloud and its services. There are individuals and organizations that are using this cloud service increasingly. This is mainly due to various benefits for switching to the others side, such as increased scalability and providing the files to the user to access these files anywhere in the world just with an internet connection and a device. This is highly convenient for the end-user as it allows them to streamline their organization by performing upgrades and maintaining the storage infrastructure. But this also leads to some privacy concerns which can be troublesome for the individual as well as the organizations. Therefore, the users encrypt their data before uploading which significantly reduces the chances of data leakage in the event of a breach. Therefore, an effective approach for the purpose of enabling search over encrypted data on the distributed blockchain platform.

REFERENCES

1. Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han, "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage", IEEE Transactions on Services Computing (Volume: 10, Issue: 5, Sept.-Oct. 1 2017), 16 March 2016.
2. Zhirong Shen, Jiwu Shu and Wei Xue, "Keyword Search with Access Control Over Encrypted Cloud Data", IEEE Sensors Journal (Volume: 17, Issue: 3, Feb.1, 1 2017), 01 December 2016.
3. Chang Liu, Liehuang Zhu and Jinjun Chen, "Graph Encryption for Top-K nearest Keyword Search Queries on Cloud", IEEE Transactions on Sustainable Computing (Volume: 2, Issue: 4, Oct.-Dec. 1 2017), 15 May 2017.
4. Rui Li and Alex X. Liu, "Adaptively Secure Conjunctive Query Processing over Encrypted Data for Cloud Computing ", 2017 IEEE 33rd International Conference on Data Engineering (ICDE), 18 May 2017.
5. Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang and Yingjiu Li, "Efficient and Expressive Keyword Search Over Encrypted Data in Cloud", IEEE Transactions on Dependable and Secure Computing (Volume: 15, Issue: 3, May-June 1 2018), 12 August 2016.
6. Boyang Wang and Xinxin Fan, "Search Ranges Efficiently and Compatibly as Keywords over Encrypted Data", IEEE Transactions on Dependable and Secure Computing (Volume: 15, Issue: 6, Nov.-Dec. 1 2018), 01 December 2016.
7. Xiaofeng Ding, Peng Liu, and Hai Jin, "Privacy-Preserving Multi-Keyword Top-k k Similarity Search Over Encrypted Data", IEEE Transactions on Dependable and Secure Computing (Volume: 16, Issue: 2, March-April 1 2019), 12 April 2017.
8. Meng Shen, Baoli Ma, Liehuang Zhu, Xiaojiang Du, and Ke Xu, "Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT", IEEE Internet of Things Journal (Volume: 6, Issue: 2, April 2019), 20 September 2018.
9. Hui Yin, Jixin Zhang, Yinqiao Xiong, Lu Ou, Fangmin Li, Shaolin Liao, and Keqin Li, "CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme", IEEE Access (Volume: 7), 03 January 2019
10. Hoang Giang Do and Wee Keong Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search", 2017 IEEE World Congress on Services (SERVICES), 14 September 2017.
11. Shan Jiang, Jiannong Cao, Julie A. McCann, Yanni Yang, Yang Liu, Xiaoqing Wang, and Yuming Deng, "Privacy-Preserving and Efficient Multi-Keyword Search over Encrypted Data on Blockchain", 2019 IEEE International Conference on Blockchain, 02 January 2020.
12. Yu Guo, Chen Zhang, and Xiaohua Jia, "Verifiable and Forward-secure Encrypted Search Using Blockchain Techniques", ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 27 July

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details