"Literature Review on a Streamlined Approach to Policy Updates in Cloud-Based Health Record Systems"

V.JAYAGANESH, B.KALPANA SATTU

MADHA ENGINEERING COLLEGE

ABSTRACT

In an attribute-based searchable encryption scheme, users can search for interesting keywords on keyword indexes by using a keyword search trapdoor. Data owners can encrypt their data with access policies for security considerations and encrypt keywords to obtain keyword index for privacy keyword search. Unfortunately, the majority of attribute-based encryption (ABE) systems now in use have large computational costs at the user side, and many searchable encryption schemes only offer single keyword searches. The practical implementation of attribute-based searchable encryption methods is severely restricted by these issues. In this research, we present an attribute-based encryption (VMKS-ABE) system for cloud storage that is verifiable and allows for multi-keyword searches while maintaining search privacy. In other words, the cloud server may perform a multi-keyword keyword searchsearch trapdoor, but it is unaware of the information included in the searched terms. The suggested plan significantly lessens the computing load at the user client by outsourcing a large number of computing operations to the cloud proxy server. Additionally, the approach facilitates the validation of the accuracy of the externalized private key. It is demonstrated that the suggested technique is secure in the sense that the ciphertext is selectively secure against selective plaintext attacks in the random oracle model, and the keyword index is indistinguishable under adaptive keyword assaults in the general group model. Our system is suitable for practical implementation, as demonstrated by the experimental and security findings.

Keywords :*Verifiable outsourcing, attribute-based encryption, multi-keyword search, and adaptive security.*

I. INTRODUCTION

These days, as cloud computing [1] advances, cloud storage is a new type of storage that allows users to store and retrieve data. Many businesses and individuals use these cloud services to store and manage shared data that they have outsourced. Cloud storage does, however, come with some drawbacks, including the possibility of user privacy disclosure and data security issues. This is because when a significant quantity of data is kept on a cloud server that is not physically under the data owners' control,long-term development of cryptographic technology that allows users to search for keywords in ciphertext. Meanwhile, it can benefit from the enormous computing capacity of CS and save a great deal of network and computational overhead for the user. The primary issue that SE technology addresses is how to use the server to finish the keyword search while the data is encrypted and kept in CS, yet CS cannot be fully trusted. It remains to be solved how to increase keyword search efficiency while lowering local computing burden. Single-word search is supported by the majority of current methods.The majority of attribute-based encryption (ABE) algorithms in use today are computationally expensive for the user client. The practical uses of ABE schemes are severely restricted by these issues. We provide an attribute-based encryption (VMKS-ABE) technique for cloud storage that is multi-keyword searchable and verifiable.

that addresses the issues of wasted network bandwidth and high computational costs. The scheme reduces the workload on local computers by outsourcing many computing tasks to a cloud proxy server and allows for the verification of the accuracy of the outsourced private keys. Our new approach protects search privacy and allows for multi-keyword searching, which can significantly increase keyword search accuracy.

II. LITERATURE REVIEW

[1].It is fundamental to a data sharing system that a user with the proper authority be able to retrieve encrypted documents from cloud storage using keywords. While data protection and retrieval capabilities can be achieved with typical searchable encryption technology, there are a few key concerns that should also in account. Initially, the majority of attribute-based searchable encryption methods that are currently in use only allow for single-keyword searches, which can provide a large number of useless search results and waste bandwidth and computer resources. Second, even if the user's qualities could change often, he frequently needs to get information about a specific keyword. Third, there are instances when a small percentage of incorrect search results are returned by the cloud server due to its lack of loyalty. Concentrate on these problems and develop a workable multi-keyword

searchable encryption system.is suggested to combine the auditing concepts with the ciphertext policy attribute-based encryption (CP-ABE) for data integrity verification and attribute revocation. By limiting the search scope, the scheme can prevent the cloud server from returning a large number of irrelevant documents. Additionally, by entrusting the powerful cloud server with the ciphertext updates, it can effectively implement attribute revocation and prevent access by unauthorized users. Verification algorithms are also used in third-party audits to guarantee the accuracy of search results and minimize the amount of work that end users must do. Most importantly, the technique demonstrated resilience against both selective keyword attacks and selective plaintext attacks using the generic group model.

[2]. Searchable Encryption techniques are used in cloud data sharing systems to guarantee data confidentiality during retrieval; nevertheless, in practice, they encounter a number of challenges. Initially, the majority of the earlier Ciphertext-Policy Attribute-Based term Search (CP-ABKS) systems allowed users to start search queries with just one term. This led to the return of numerous erroneous results, wasting bandwidth and computer power. Second, in order to reduce connection expense, untrusted cloud services might only return a tiny percentage of full search results. Furthermore, an unshared multi-owner setting is the only one supported by the majority of CP-ABKS systems, which results in significant computational and storage cost. Moreover, most of the prior techniques are vulnerable to offline keyword guessing attacks when the keyword space is a polynomial. To address these issues, we focus on a multi-keyword search method. Ciphertext Policy Attribute-Based Encryption (CP-ABE) technology is combined with a shared multi-owner system to give performance-preserving verification of search results. We show off our system's security, which protects against offline keyword guessing attacks and guarantees the unforgeability of signatures. It is superior to the most pertinent options in terms of functionality and utility, pursuant to the comparison of the trial data.

[3]. Data owners are incentivized to outsource their data to public clouds in order to lower the cost of management systems since the emergence of cloud computing. Sensitive data must be encrypted before outsourcing in order to safeguard data privacy. Thus, it is crucial to provide search functionality for encrypted data on cloud servers. Users may find it interesting to conduct a multi-keyword search and obtain the most relevant results given the vast quantity of data users stored in the cloud. In this work, we examine the multi word rank on search over encrypted cloud data proposed by Pasupuleti et al. Their plan contains issues with search processes, trapdoor creation, and index building. We tackle these issues and provide a multi-keyword ranked search over cloud storage encrypted data. The suggested By providing ranked searchable encryption strategy, which guarantees accurate file retrieval, it improves system usability by providing ranked results rather than merely undifferentiated ones. Additionally, we create a safe searchable index using reterival , and we encrypt sensitive file scores with additive order-preserving encryption. Moreover, our attribute-based encryption ensures user access control during data retrieval. Our plan for cloud storage is effective and safe, according to analysis. By providing ranked searchable encryption strategy, which guarantees accurate file retrieval, it improves system usability by providing ranked results rather than merely undifferentiated ones. Additionally, we create a safe searchable index using, and we encrypt sensitive file scores with additive order-preserving encryption. Moreover, our attribute-based encryption ensures user access control during data retrieval. Our plan for cloud storage is effective and safe, according to analysis.

[4].Nowadays, there is a lot of study being done on how to securely transmit medical data because of the increasing use of electronic medical technology and the quick development of cloud storage technology. The first step to achieving it is to conduct a quick and effective keyword search in the medical cloud. Untrusted service providers, however, could provide misleading search results or results pertaining to a particular business endeavor. The advantages enjoyed by consumers and primary data owners will also be harmed by privacy breaches involving medical data. In the medical sharing system, it is now crucial to guarantee fair and accurate searching of shared data and to safeguard the confidentiality of medical data. In order to address these issues, a search framework for a smart health system is put out in this study. Within the structure, two The user's trapdoor is matched with the index by smart contracts called search smart contract (SSC) and verify smart contract (VSC), which are built on the Ethereum blockchain and used to validate the accuracy of search results. We implement a ranking multi-keyword search that only provides the best pages that best satisfy the user's needs in order to increase search accuracy. Furthermore, a novel attribute-based encryption (ABE) is presented to maintain the sharing data's confidentiality and access authority. Additionally, the hiding policy which resolves the issue of privacy protection during data sharing is supported by the proposed ABE.

[5]. Attribute revocation is an extension of attribute-based encryption, which is a useful technique for achieving flexible and safe access control over data. Keyword search is also a crucial component of cloud storage. In cloud storage, the combination of both has a significant use. In this paper, we build an attribute-based searchable encryption scheme with attribute revocation for cloud storage. Our scheme uses attribute based keyword algorithm search with access control; if the search is successful, the cloud server provides the user with the

corresponding cipher text, which they can decrypt with certainty. Additionally, our approach allows for the search of numerous terms, which increases its usefulness. Let us assume that the Diffie-Hellman exponent is decisional and thus We demonstrate that our technique is secure using Diffie-Hellman under the selective security paradigm.

III .RESEARCH METHODOLOGY

A structured approach is used in the study methodology to ensure the efficacy, security, and feasibility of the suggested solution in the development of an attribute-based encryption (ABE) scheme for cloud storage that is verifiable and searchable using multiple keywords. First, a thorough literature analysis is done with an emphasis on current ABE schemes, especially those concerning searchable and verifiable ABE and cloud storage security. This review assists in identifying possible areas for development as well as gaps in present techniques. After that, the problem is stated precisely, including its goals, which include improving cloud storage security and facilitating effective, verified search functions. The next step in the design and implementation process is creating a conceptual foundation for the suggested scheme, putting it into practice with the right cryptographic methods, and making sure it is scalable and efficient enough for use in actual cloud environments. An To ensure confidentiality, integrity, and verifiability, the scheme is assessed against popular cryptographic attacks as part of a thorough security analysis that identifies vulnerabilities and risks. Next, by contrasting the suggested plan with current methods, performance evaluation experiments are carried out to evaluate compute overhead, storage needs, and communication overhead. To evaluate robustness and reliability, validation and testing entail simulations or prototype deployments in a cloud environment. Stakeholders and subject experts are consulted to identify usability issues. In a research paper that is submitted to pertinent conferences or journals for peer review and publishing, the thorough documenting of the research findings is referred to as reporting and documentation. Ultimately, reviewer feedback and iteration are integrated to improve the suggested plan and address any found flaws or restrictions, guaranteeing ongoing development and progress in cloud storage security.

IV. SYSTEMARCHITECTURE

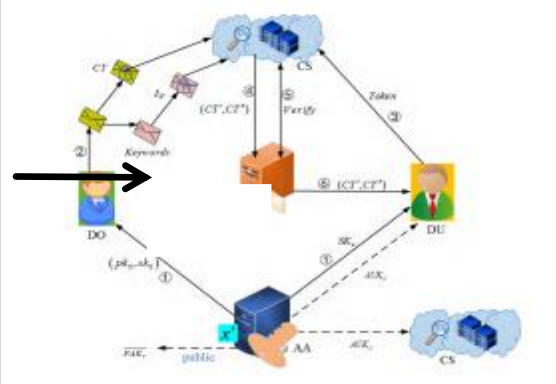


Fig1: System architecture

In order to address the issue of overhead and delay of earlier suggested PRE methods, we have developed a proxy re-encryption strategy for E-healthcare data exchange using fog computing.Our plan lowers the communication overhead and commutation cost of the Internet of Things devices with resource constraints.We can obtain significant performance by employing the proxy re-encryption strategy when we need to share encrypted data with numerous participants.

V. MODULES

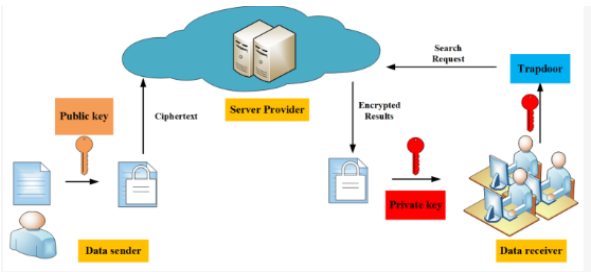


Fig 2: Modules architecture

A. Data User

B. Data Owner

C. Attribute authority

D. Cloud Proxy server

E. Cloud server

F.OKGSP

H.Attacker

A. DATA USER

The first step is the user registration procedure, which needs to be completed before users may access the system. Users must pass authentication at registration, and only those approved by the Attribute Authority are able to access their accounts. Users send keyword queries to the OKGSP (likely an external service or component) to start a file search. Entering the term and the right secret key grants access to the search functions. After that, users can examine the files in a decrypted format by conducting a file search using keywords and defined criteria (the "k" value). File retrieval requests are submitted to the OKGSP. Users can also see the status of their file requests and differentiate between those that are active and those that are not. Last but not least, individuals can safely log out of their accounts, concluding their usage of the platform.

B. DATA OWNER

Data Owners are first required to register as part of the system workflow's registration procedure. After registering, authentication takes place, and only Data Owners who have been given permission by the Attribute Authority can access their accounts and log in. After logging in successfully, Data Owners can upload files to the cloud. In order to encrypt the files, homomorphic techniques are used for both encryption and decryption. Fuzzy logic is used to produce the file private and trapdoor keys. Data Owners can then submit requests for file uploads to the cloud proxy server. Data Owners maintain control over their data after they are uploaded, including the right to view and remove any files that they so want. Lastly, after finishing their activities, Data Owners.

C. ATTRIBUTE AUTHORITY

One of the features of the system is a login process that only permits authorized users to access. After logging in, the system activates Data Owners' requests and allows them to be authorized. By going through this authorization process, Data Owners may be sure they have the right authorization to carry out their assigned tasks. In a similar vein, the system also grants authorization to Data Users, thereby triggering their requests and facilitating efficient interaction. Users can safely log out of the system after finishing their tasks, ending their session and maintaining system security. By taking these steps, the system effectively handles user requests and permissions while maintaining restricted access.

D.CLOUD PROXY SERVER

The system starts with the login procedure, which allows users to authenticate and receive access to the platform. The technology enables data owners to approve files for upload to the cloud server after a successful login. Transferring files in response to upload requests made by data owners is part of this permissions procedure. This transmission is facilitated by the proxy server, which also makes sure that files are approved before users can access them via the'search files' module. Users are also able to examine any file that has been approved for use in the system. Lastly, users have the option to safely log out to end their session after finishing their tasks. In addition to preserving the system's integrity and security, this procedure guarantees restricted access to files.

E.CLOUD SERVER

The system's gateway for authorized access is the login feature. Users can view all registered Data Owners and Data Users after logging in. They can also access other features including seeing all allowed files, which includes data that Data Owners have uploaded to the cloud and that the Cloud Proxy Server has approved. Users can also see the transactions that other users have done and see which files have been compromised by unapproved parties. In addition, the system has the ability to compute the throughput of all files transferred to the cloud, produce findings based on file request counts, and ascertain the upload delay time. Users can safely log out after finishing work to protect the integrity and security of the framework. The system's capabilities enable effective data management and analysis, offering valuable insights into security and system performance parameters.

F.OKGSP

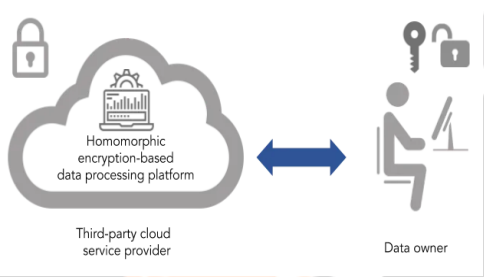
The login feature is the point of entry for users into the system. Users can access several functions after logging in. They have the ability to see requests for keyword keys and email the secret keyword key to the user's registered email address. Users can also email the decryption key—which contains the file secret key and trapdoor key—to the email address they registered with. Users can safely exit the system after finishing their tasks. This methodical technique improves the system's overall security by ensuring secure key management and communication.

H.ATTACKERS

Users can access the system and enjoy its different capabilities by logging in. Users have the ability to launch assaults on files that provider agents have uploaded. The purpose of this activity is to evaluate the system's resilience to prospective attackers and mimic security flaws. Users have the option to safely log off of the system after finishing their tasks, protecting its integrity. This method makes it possible to thoroughly examine and assess the security precautions the system takes against possible intrusions.

VI.ALGORITHM

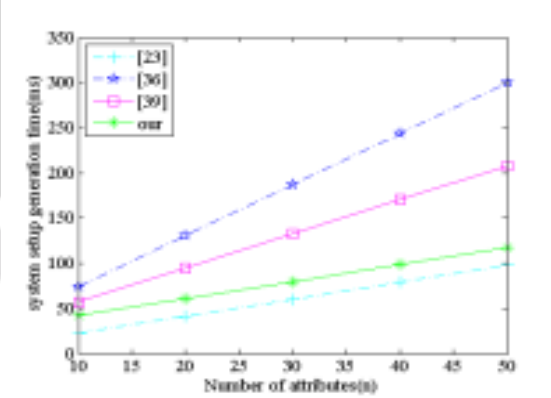
Homomorphic Algorithm



A cryptographic technique called homomorphic encryption enables mathematical operations on data to be performed on a cipher text rather than the data itself. The input data (also known as plain text) is encrypted and used as the cipher text. It is subsequently decrypted to get the intended result.

VII.RESULT

This section mostly compares the differences in performance between our approach and a few traditional re-encryption techniques displays the functional comparative results.



A major improvement in cloud security and data accessibility has been achieved by the implementation of an Attribute-based Encryption (ABE) Scheme for Cloud Storage that is Verifiable and Multi-keyword Searchable. Users can safely store and retrieve data from cloud storage using this system, which guarantees data confidentiality, integrity, and verifiability. The verifiability feature of the method facilitates user authentication and data integrity, offering a strong defense against tampering and unwanted access. Furthermore, the multi-keyword search function improves data accessibility by allowing users to look for files using several keywords, which expedites the process of retrieving data. An additional degree of protection is added by attribute-based encryption, which guarantees that only authorized individuals possessing particular traits can access encrypted data. In general, the effective execution of this plan signifies a noteworthy contribution to the security of cloud storage, providing users and organizations with improved privacy, data accessibility, and verifiability.

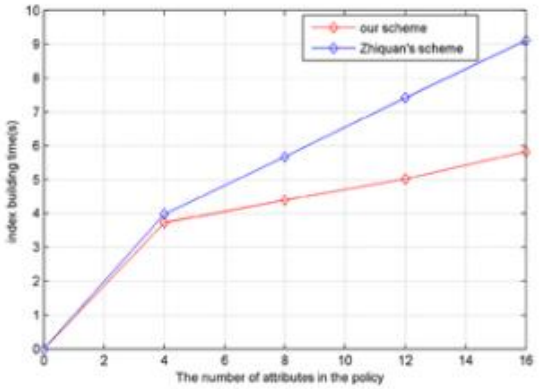


Fig2.(c) The number of attributes in policy and index building

VIII.FUTURE DISCUSSION

Additionally, using blockchain technology to build more secure, high-efficiency search methods that support dynamic dataset search is one of the difficulties that we need to be thinking about in light of the needs of actual applications and future research.

IX. CONCLUSION

We presented the VMKS-ABE system in this paper. In our system, we combine attribute-encrypted multi-keyword search with provable correctness of the outsourced private key. In contrast to the prior search encryption system, this work not only achieves multi-keyword search without compromising search performance, but it also introduces TPA to realize the function of user attribute revocation and validate the accuracy of the search results. Our method has demonstrated its security against targeted keyword assaults in the generic bilinear group model, as well as its resilience against targeted plaintext attacks. Our plan's viability was then confirmed by both theory and experiment. The keyword index's security is demonstrated in the generic group model. It is demonstrated that the ciphertext is selectively secure under the random oracle paradigm. It is worthwhile to build a verifiable, multi-keyword searchable scheme in the standard model since the security in the general group model is significantly less than in the standard model.

X .REFERENCES

[1] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ‘‘Enabling personalized search over encrypted outsourced data with efficiency improvement,’’ in IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[2] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, ‘‘A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing,’’ IEEE Trans. Inf. Forensics Secur., vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[3] K. Yang and X. Jia, ‘‘ABAC: Attribute-based access control,’’ in Security for Cloud Storage Systems. New York, NY, USA: Springer, 2014, pp. 39–58.

[4] H. Haiping, D. U. Jianpeng, H. Dai, and R. Wang, ‘‘Multi-sever multikeyword searchable encryption scheme based on cloud storage,’’ J. Electron. Inf. Technol., vol. 39, no. 2, pp. 389–396, Feb. 2017.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp.

[6]. M. Bellare, A. Boldyreva, and A. O’Neill, ‘‘Deterministic and efficiently searchable encryption,’’ in Advances in Cryptology (CRYPTO). Berlin, Germany: Springer, Aug. 2007, pp.

[7]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, ‘‘Fuzzy In cloud computing keyword search over encrypted data,’’ in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010,pp.

[8]. "Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," by W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li IEEE Trans.

[9]. Q. Dong, Z. Guan, and Z. Chen, ‘‘attribute-based keyword search efficiency enhancement via an online/offline approach,’’ in Proc. IEEE 21st Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2015, pp.

[10]. Y. Ye, J. Han, W. Susilo, T. H. Yuen, and J. Li, ‘‘ABKS-CSC: Attributebased keyword search with constant-size ciphertexts,’’ Secur. Commun. Netw., vol. 9, no. 18, pp.

[11]. Q. Chai and G. Gong, ‘‘Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp.

A Brief Author Biography

ER. B Kalpana is an Head of the Department of Computer Science and Engineering at Madha Engineering college, Chennai, Tamil Nadu, India. She received her Bachelor of Technology Degree in Information Technology from Sri Venkateswara College of Engineering Chennai with First Class and Distinction affiliated to Madras University in 2003 and She received her Master Degree in Computer Science and Engineering with First Class Distinction from Anna University, Chennai, Bachelor of Technology Degree in Information Technology from Sri Venkateswara College of Engineering Chennai with First Class and Distinction affiliated to Madras University in 2003 and Diploma Degree in Computer Science and Technology from Panimalar Polytechnic Chennai with First Class and Distinction with a Gold Medal affiliated to Directorate of Technical Education in 2000. She has several high level involvements in the area of Artificial Intelligence and Big data. She is the “EMC Academic Associate in Big Data Analytics and Data Science”. She is also awarded with "Senior Educator and Research Scholar Award‟ from National Foundation for Entrepreneurship Development, Tamil Nadu in the year 2015. She has nearly 15 years of academic experience in the field of Engineering and guided many research projects. She has published finite number of papers on Dependable and secure computing and in the area of Big data. She is an Associate Editor of Information Science & Engineering to the Editorial Review Board of esteemed International Journal of Entrepreneurship and Small & Medium Enterprises (IJESMES), Kathmandu, Nepal, from June 2015, Editor of International Journal of Advanced Research in Management, Engineering and Technology from March 2016 and Reviewer at International Journal of Advances in Engineering and Scientific Research from February 2016.

V.Jayaganesh is studying M..E. Computer Science Engineering in Madha Engineering college. and also he has completed B,E. Computer science and Engineering in Jeppiaar Institute of technology, Chennai, Tamil Nadu, India. Currently , he is working as a Software developer in H.C.L. Also he has published the journal in B.E. related to cloud computing topics such as” Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage” and also has secured the second rank in the state level football competition in UG