Sharing Data Based on Attribute Matching and Temporary Keyword Search on Cloud

Mangesh Bondre[1], Rohit Kumavat[2], Shubham Dhamdhere[3], Sayabanna Hegonde[4], Prof Bhagyashree Patle[5]
Sinhgad Institute of Technology Lonavala, PUNE

Abstract— Temporary keyword search on confidential knowledge in a very cloud atmosphere is the main focus of this analysis. The cloud suppliers aren't absolutely sure. So, it's necessary to source knowledge within the encrypted type. within the attribute-based keyword search (ABKS) schemes, the approved users will generate some search tokens and send them to the cloud for running the search operation. These search tokens are wont to extract all the ciphertexts that area unit created at any time and contain the corresponding keyword. Since this could cause some info run, it's safer to propose a theme within which the search tokens will solely extract the ciphertexts generated in a very specific amount. to the current finish, during this paper, we tend to introduce a replacement technique Sharing knowledge supported Attribute matching And Temporary Keyword Search on the cloud which gives this property. to judge the safety of our theme, we tend to formally prove that our projected theme achieves the keyword secrecy property and is secure against by selection chosen keyword attack (SCKA) each within the random oracle model. what is more, the owner shares access key with a time server that offers additional security for file access? User's views searched file rank wise. Performance analysis shows our scheme's usefulness.

Keywords—Searchable encryption, attribute-based encryption, provable security, temporary keyword search, cloud security, Time Server, Ranking

I. INTRODUCTION:

Public key cryptography with keyword search (PEKS) could be a cryptological primitive that was initially introduced by Boneh et al. to facilitate looking on the encrypted knowledge. In PEKS, every knowledge owner World Health Organization is aware of the general public key of the meant knowledge user generates a searchable ciphertext by means that of his/her public key, and outsources it to the cloud. Then, the info user extracts a hunt token associated with the associate capricious keyword by exploitation his/her secret key, and problems it to the cloud. The cloud service supplier (CSP) runs the search operation by exploitation the received search token on behalf of the info used to search out the relevant results to the meant keywords.

Motivated by this downside, Abdalla et al. introduced the notion of public-key cryptography with a temporary keyword search (PETKS) that restricts the validation of the token to a definite fundamental measure. They applied anonymous identity-based cryptography in their generic themes. additionally, Yu et al. projected another public key searchable cryptography within the context of a temporary keyword search. Despite the great options of their schemes, these schemes don't offer the power for knowledge homeowners to enforce their meant access policy. during this paper, we have a tendency to propose a completely unique notion of Key-Policy Attribute-Based Temporary Keyword Search (KP-ABTKS). In KP-ABTKS schemes, the info owner generates a searchable ciphertext associated with a keyword and also the time of encrypting in keeping with associate meant access management policy, and outsources it to the cloud. After that, every licensed knowledge user selects associate capricious measure and generates a hunt token for the meant keyword to search out the ciphertext. Then, he/she sends the generated token to the cloud to run the search operation. By receiving the token, the cloudy appearance for the documents contain the meant keyword. The search result on a ciphertext is positive, if (i) the info user's attributes satisfy the access management policy, (ii) the measure of the search token encompasses the time of encrypting, and (iii) the search token and also the ciphertext area unit associated with an equivalent keyword. to point out that the projected notion will be complete, we have a tendency to additionally propose a concrete internal representation for this new cryptological primitive supported linear map.

II. LITERATURE SURVEY:

Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement[1] Zhangjie Fu, Xinle Wu, Chaowen Guan, Xingming Sun, and Kui Ren

Keyword-based search over encrypted outsourced data has become an important tool in the current cloud computing scenario. The majority of the existing techniques are focusing on multi-keyword exact match or single keyword fuzzy search. However, those existing techniques find less practical

significance in real-world applications compared with the multi keyword fuzzy search technique over encrypted data. The first attempt to construct such a multi-keyword fuzzy search scheme was reported by Wang *et al.*, who used locality-sensitive hashing functions and Bloom filtering to meet the goal of multi-keyword fuzzy search. Nevertheless, Wang's scheme was only effective for a one letter mistake in keyword but was not effective for other common spelling mistakes. Moreover, Wang's scheme was vulnerable to server out-of-order problems during the ranking process and did not consider the keyword weight. In this paper, based on Wang *et al.*'s scheme, we propose an efficient multi keyword fuzzy ranked search scheme based on Wang *et al.*'s scheme that is able to address the aforementioned problems.

First, we develop a new method of keyword transformation based on the unigram, which will simultaneously improve the accuracy and creates the ability to handle other spelling mistakes. In addition, keywords with the same root can be queried using the stemming algorithm. Furthermore, we consider the keyword weight when selecting an adequate matching file set. Experiments using real-world data show that our scheme is practically efficient and achieve high accuracy.

A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data[2] Zhihua Xia, Xinhui Wang, Xingming Sun, Senior, and Qian Wang

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF _ IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly.
Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data[3] Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou, and Xuemin (Sherman) Shen
Using cloud computing, individuals can store their data on remote servers and allow data access to public users through the cloud servers. As the outsourced data are likely to contain sensitive privacy information, they are typically encrypted before uploaded to the cloud. This, however, significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. In this paper, we address this issue by developing the fine-grained multi-keyword search schemes over encrypted cloud data. Our original contributions are three-fold. First, we introduce the relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. Second, we develop a practical and very efficient multi-keyword search scheme. The proposed scheme can support complicated logic search the mixed “AND”, “OR” and “NO” operations of keywords. Third, we further employ the classified sub-dictionaries technique to achieve better efficiency on index building, trapdoor generating and query. Lastly, we analyze the security of the proposed schemes in terms of confidentiality of documents, privacy protection of index and trapdoor, and unlinkability of trapdoor. Through extensive experiments using the real-world dataset, we validate the performance of the proposed schemes. Both the security analysis and experimental results demonstrate that the proposed schemes can achieve the same security level comparing to the existing ones and better performance in terms of functionality, query complexity and efficiency.

Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the
Cloud[4] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li
Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset

can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi-contributor case. Inspired by attribute-based encryption (ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e. file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re-encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi-trusted cloud server. We formalize the security definition and prove the proposed ABKS-UR scheme selectively secure against chosen-keyword attack. To build confidence of data user in the proposed secure search system, we also design a search result verification scheme. Finally, performance evaluation shows that the efficiency of our scheme.

Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation[5] Yanfeng Sh,i Qingji Zheng, Jiqiang Liu, Zhen Han

Attribute-based encryption (ABE) enables an access control mechanism by specifying access control policies among decryption keys and ciphertexts. In this paper, we propose a novel ABE variant, dubbed directly revocable key-policy ABE with verifiable ciphertext delegation (drvuKPABE), which supports direct revocation and verifiable ciphertext delegation. The drvuKPABE offers the following features which are promising in the data sharing applications: (1) it allows the trusted authority to revoke users by solely updating the revocation list while mitigating the interaction with non-revoked users, which is unlikely to indirectly revokable ABE; (2) it allows the third party to update ciphertexts with public information so that those non-revoked users cannot decrypt them; and (3) it enables any auditor (authorized by data owners) to verify whether the untrusted third party updated ciphertexts correctly or not. We formalize the syntax and security properties for drvuKPABE, and propose the construction based on the multilinear maps. Our solution attains the security properties under the Multilinear Decisional Diffie–Hellman assumption in the random oracle model.

III. PROBLEM STATEMENT

In the recent days the storing the files on cloud is very complicated and insecure for all the users. When we are storing our data on cloud then there is a possibility that access data by attacker. For resolving the problem we developed the application. That set time server for access file when user download from server, furthermore we use ranking so users get files rank wise.

IV. PROPOSED SYSTEM:

We develop an associated application that has knowledge homeowners, users, TTP and cloud server. the info owner registers and sends an activation request to TTP. TTP activates the account of the owner and sends OTP to knowledge homeowner's mobile variety. The owner currently log in to the system. transfer file with a time server and keywords and inscribe victimization AES and ND5 rule severally. homeowners conjointly read and transfer files. Users register and send an activation request to TTP. TTP activates the user's account and send OTP to mobile variety. User search file victimization Keywords. get the file from cloud rank wise and look at files, then he requests to knowledge owner to send key. knowledge owner sends a key response with time server meaning specific cut-off date ar set for transfer image from cloud. Here we have a tendency to use time server by 2 ways that 1st is ready to time server for file, meaning once cut-off date ends then cloud mechanically delete the file from the cloud. and the second method is user transfer time victimization key and for that key owner set time for downloading.

V. ADVANTAGES:

- It achieves the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA)
- The search tokens can only extract the ciphertexts generated in a specified time interval so leakage is not possible.

VI. SYSTEM ARCHITECTURE:

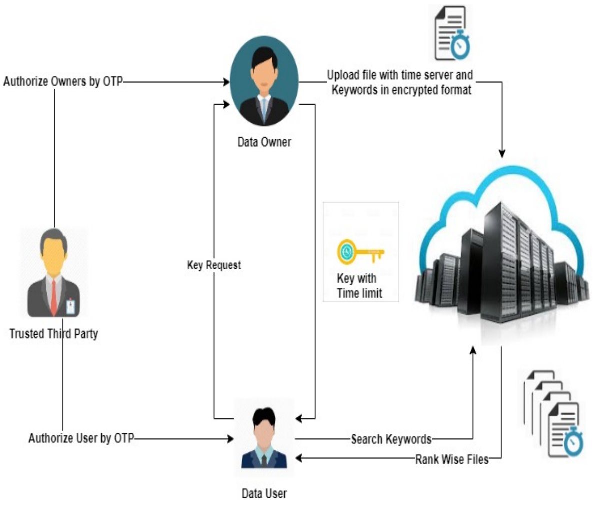


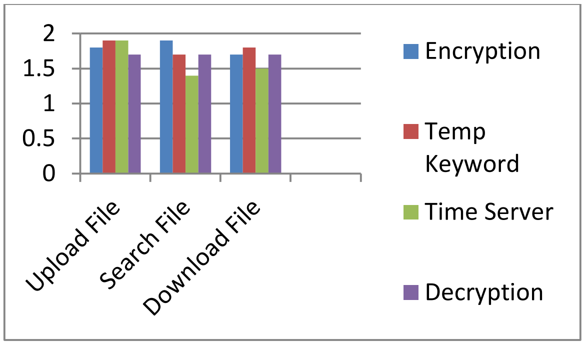
Figure 1 System Architecture

VII. ALGORITHM DETAILS:

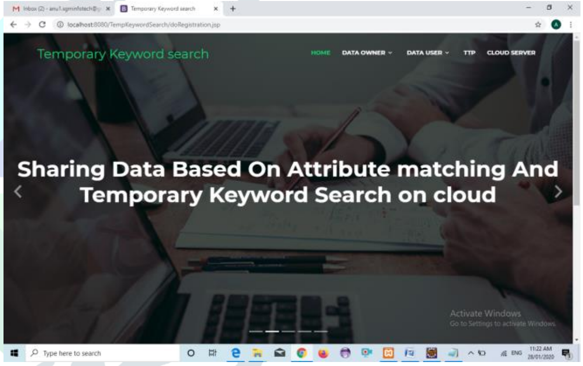
- AES Algorithm
  - Derive the set of round keys from the cipher key.
  - Initialize the state array with the block data (plaintext).
  - Add the initial round key to the starting state array.
  - Perform nine rounds of state manipulation.
  - Perform the tenth and final round of state manipulation.
  - Copy the final state array out as the encrypted data (ciphertext).
- MD5:

The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. In our project we use MD5 to store Keywords in encrypted format.

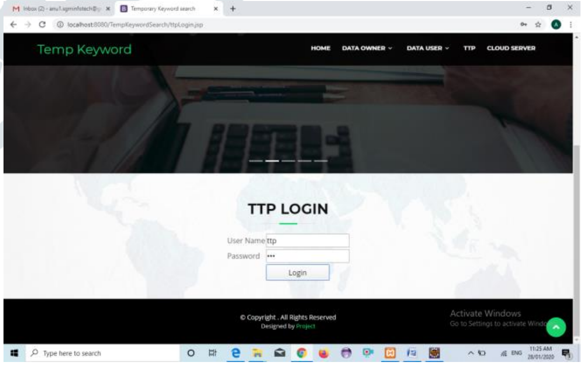
RESULTS AND SCREEN SHOTS



	Encryption	Temp Keyword	Time Server	Decryption
Upload File	1.8	1.9	1.9	1.7
Search File	1.9	1.7	1.4	1.7
Download File	1.7	1.8	1.5	1.7



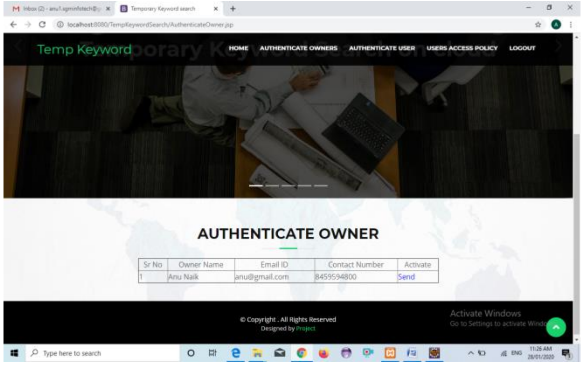
Sharing Data Based On Attribute matching And Temporary Keyword Search on cloud



TTP LOGIN

User Name ttp
Password •••

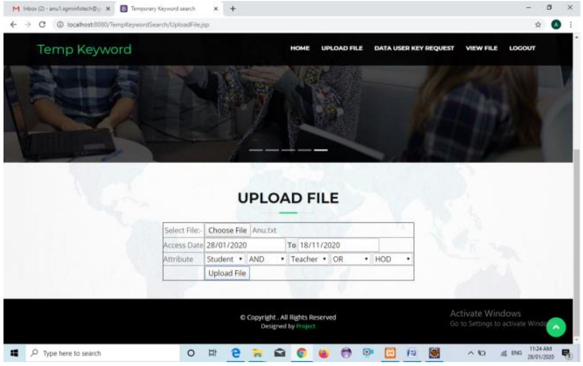
© Copyright . All Rights Reserved
Designed by Project



AUTHENTICATE OWNER

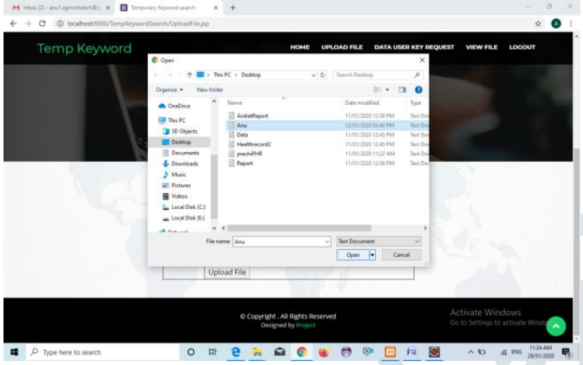
Sr No	Owner Name	Email ID	Contact Number	Activate
1	Anu Naik	anu@gmail.com	8459594800	Send

© Copyright . All Rights Reserved
Designed by Project



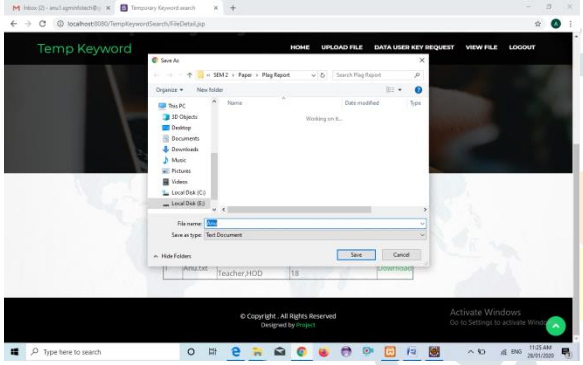
UPLOAD FILE

Select File:-	Choose File Anu.txt						
Access Date	28/01/2020	To	18/11/2020				
Attribute	Student	AND	Teacher	OR	HOD		



Name	Date modified	Type
AniketReport	11/01/2020 12:58 PM	Text Do
Anu	22/01/2020 03:40 PM	Text Do
Data	11/01/2020 12:45 PM	Text Do
Healthrecord2	11/01/2020 12:45 PM	Text Do
prachiPHR	11/01/2020 11:22 AM	Text Do
Report	11/01/2020 12:58 PM	Text Do

File name: Anu
Text Document



File name: Anu
Save as type: Text Document

1	Anu.txt	Teacher,HOD	18	Download

CONCLUSION:

Securing cloud storage is a vital downside in cloud computing. we tend to self-addressed this issue and introduced the notion of key-policy attribute-based temporary keyword search (KPABTKS). consistent with this notion, every knowledge user will generate a probe token that is valid just for a restricted amount. we tend to plan the primary concrete construction for this new science primitive supported linear map. we tend to formally show that our theme is incontrovertibly secure within the random oracle model. The quality of encoding algorithmic rule of our proposal is linear with relevancy to the quantity of the concerned attributes. additionally, the quantity of needed pairing within the search algorithms is freelance of the quantity of the supposed time units per the search token and it's linear with relevancy the number of attributes. Performance analysis of our theme in terms of each procedure price and execution time shows the sensible aspects of the planned theme.

REFERENCES:

[1] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, 2016.

[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.

[3] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[4] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187–1198, 2016.

[5] Y. Shi, Q. Zheng, J. Liu, and Z. Han, "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation," Information Sciences, vol. 295, pp. 221–231, 2015.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 53–70.

[8] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in International Colloquium on Automata, Languages, and Programming. Springer, 2008, pp. 579–591.

[9] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Information Sciences, vol. 275, pp. 370–384, 2014.

[10] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Information Sciences, vol. 276, pp. 354–362, 2014.

[11] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE Transactions on

Information Forensics and Security, vol. 10, no. 3, pp. 665–678, 2015.

[12] T. Okamoto and K. Takashima, “Fully secure functional encryption with general relations from the decisional linear assumption,” in Advances in Cryptology–CRYPTO 2010. Springer, 2010, pp. 191–208.

[13] A. Lewko and B. Waters, “New proof methods for attribute-based encryption: Achieving full security through selective techniques,” in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 180–198.

[14] J. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy-preserving decentralized key-policy attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2150–2162, 2012.

[15] M. Chase, “Multi-authority attribute based encryption,” in Theory of Cryptography. Springer, 2007, pp. 515–534.