Accessible Authentication Using Keyword Search through Homomorphic Encryption

Dr. Vipul Vekariya
Professor,
Department of CSE
PIET, Parul University,
Vadodara, Gujarat, India
vipul.vekariya18435@paruluniversity.ac.n

Manjunath.R
Assistant Professor,
Department of Data Science & Mathamatics
Jain (Deemed to be University), JC Road,
Bangalore, India.
r.manjunath@jaininiversity.ac.in

Dr. Jasmeen Gill
Associate Professor,
Department of CSE
RIMT University, Mandi, Godindgarh, India
jasmeengill@rimt.ac.in

Dr M Gopianand,
Assistant Professor,
Department of Computer Applications,
PSNA College of Engineering and Technology, Dindigul.
mgopianand@psnacet.edu.in

Avneesh Kumar
Professor,
Department of Computer Application
Galgotias University, Greater Noida,
Uttar Pradesh, India
avneesh.avn119@gmail.com

Dr Amaresh Jha
Associate Professor,
School of Modern Media,
UPES, Dehradun
amaresh.jha@ddn.upes.ac.in

2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC) | 978-1-6654-5687-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/IIHC55949.2022.10060417

ABSTRACT: Data storage presents substantial issues due to concerns about data security and privacy. In this study, we provide a search-based, interoperable, verified public key cryptography system. The searchability is significantly improved by our recommended method, which allows the cloud servers to create invert crypto indexes while needing a query trap and leveraging asymmetric cryptography developed by van Vries, Miller, Showing different, and Vaikuntanathan. Contrarily, the recommended method offers a brand-new permitted dataset built on the inversion decryption scheme and shows how it may be used to evaluate the thoroughness and correctness of serps. Additionally, using the provided method, many users may do encrypted searches on cryptography. Finally, it is shown that the offered technique is secure utilizing the approximate-GCD problem. The experiment's results showed that the proposed technique had less computational complexity than the methods currently in use.

1. INTRODUCTION

The plume has now been widely used by both people and companies because to its capacity to manage data easily and inexpensively. However, since then, difficulties have appeared. Although cloud service providers are generally reliable, outsourcing data have strong privacy protections and economic benefits. Before storing the data online, the material's owner encrypts it to stop data leakage. However, the encryption drastically restricts how effectively csps can fulfill user requests, such as browsing encrypted files.

Seriously damage et al. established the concept of public key cryptography with lookup to address this problem (PEKS). The PEKS system requires that writers submit a secure message and a word list to a private email. After getting the necessary keyword (also known as a trapdoor) from the recipient, the email server examines the encrypted emails to see whether it is there. Soon after, more recommendations to improve this design and use it with the cloud system were made. However, the majority of PEKS systems now in use can guarantee that the website's search results are comprehensive. If there is no guarantee that the results are thorough, the server may send incomplete search results in order to save computer resources. Making decisions based only on inadequate search engine results might have serious, even extreme, consequences.

Since the information or phrases included in the indexing are scrambled, the VM can readily store the encrypted messages and indexing in the order in which they have been collected. Since a file may contain numerous synonyms, data providers often encrypt and publish each keyword for every file. The runtime of the cloud is O(log n m), where n is the entire number of files on the server and m is the total number of keywords, since every time a user enters a query request, the cloud must visit all of the indexes in order to find the target assets. As a result, search is not very efficient, and the server may opt not to scan all indexes and just provide partial search results in order to save computational load. The generated should in fact be altered at the cloud server to improve search speed. The client must receive a query manhole from the user in the PEKS schemes in order to determine if one of the encryption indexes connected towards the files is equal to the query backdoor. Without a zipper, the server cannot check that possibly the phrases in the two decrypted indexes are same, therefore it is unable to alter the encoded index structure.

The owner of the data is willing to make it available to many users of the cloud storage system. In this situation, many users are supported by the lookup encryption. But the vast majority of PEKS systems in use today are designed for a single user. It is quite clear that the tactics recommended for use in 1% cannot be used directly and

978-1-6654-5687-6/22/$31.00 ©2022 IEEE

effectively in multi-user situations because to the latter's increased demands. Only one user is permitted to do an encrypted text search on encrypted files, and data providers are only permitted to share their information with one other user under one 15(15 scheme. In multi-user contexts like cloud services, data owners want to allow multiple users to perform encrypted keyword searches on encryption while still allowing them to share their information with a large number of users.

To overcome the aforementioned problems, we provide a validated public key authentication system with cross-context keyword searches based on encryption algorithms.

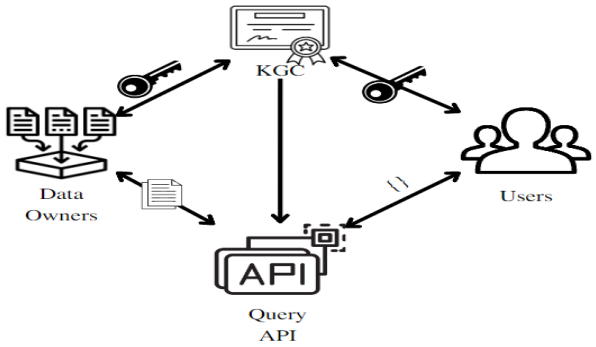

Fig 1: System model.

Briefly mentioned are the based solely. We cover a few important past works in this field in Part 2. The preparatory materials used in Section 3 of the study are then presented. In Section 4, we provide a secure framework, the theoretical underpinning of our strategy, and information on how to construct our system. Next, we show in Part 5 how our strategy fits with the security model. The effectiveness of the system is evaluated in paragraph 6. Finally, the article is concluded in Section 7.

2. PRIOR WORKS

Seriously damage et al. first developed public key cryptography with search term (PEKS) to enable users to look on encrypted cloud servers using keywords without decrypting the data. and its development makes advantage of ego security construction (IBE). Later, potentially harmful et al. proposed a more practical approach that could handle arbitrary conjunctive searches (such as comparison search, subset search, etc.). Baek et al. offered a PEKS technique using a specific server to get rid of a VPN tunnel. Camenisch et alconcept .'s in advised naive manufacture of the search terms trap in order to maintain the secrecy of the phrase from an inquisitive snare developer. Through encrypted cloud information, Cao et al. provided multi-keyword ranked searches and created a number of privacy requirements. Up until now, a lot of work has gone into making the PEKS program more secure and effective.

With the development of encryption technology, the risk of privacy leakage in the data owner has lessened. The following, in particular, may be used to summarize our significant contribution:

By using DGHV encryption technology (van Lange, Gold, Known to exhibit, and Value is assumed), we are able to improve overall encrypted access structure. Our system lets the cloud server to create an invert encryption indexes without utilizing a request trap, greatly enhancing performance.

Depending mostly on inversion encrypt data set, we suggest a novel certified database schema for confirming the accuracy and comprehensiveness of search engine results, and we utilize it to provide verification documentation.

Our system enables individuals to securely seek up secret key and seems to be necessary for pass usage Based here on Guesstimated issue, the security of our technique has been shown.

We assess our plan's effectiveness and compared it to the earlier designs in terms of timeline complexity and functionality. In our technique, the runtime of a keystroke query is lowered to O(m). Results from experiments show that our plan's query efficacy is greater than that of competing systems.

However, the problem of providing secure query services is still another recent challenge. As a result of a system failure or the cloud customer's potential to return insufficient search results in order to reduce computing costs, the beneficiary may start receiving some inaccurate and imperfect query results. This could cause the beneficiary to make an unfortunate mistake based on those insufficient and inaccurate serps. It might be devastating or very serious. The verifiability of the search result should be considered as a result. Currently, there are several initiatives in place to address this issue, including proposals through. There are a few approaches for searching through encryption keys that can be verified, however the bulk of existing systems focus mostly on data validation. The techniques are rendered worthless once they are shifted to it since the encryption procedure uses both the set of numbers and the secret keys of the data landlord. To the best of the researcher's knowledge, there aren't many search algorithms that can be validated via encryption, and those that can are often built to ensure that search keywords were appropriate for fixed contexts rather than multi-user situations. Chai and Gong offered the first text box in an asymmetric setting that had been confirmed. Systems that used natural quality encryption showed how to use good search algorithms. Sun et al. offered a search term crucial to figure 1 in the case of multiple cotext searches by turning the proposed secure indexing tree into a verified one. Guo et al. developed a multi-phrase rated search over encryption that can check the result of sorting and provide procedures for dynamic updating. The works mentioned above, in particular, were made for a specific user.

- *Key-generation center*. The creation of both public and private secrets and their transmission to network users, datacenters, and other customers is the responsibility of a center known as the vital center (KGC).
- *Data owners*. A certain group of clients are referred to as "data providers" since they create private information and then hire cloud storage providers to store it securely so that only authorized users may access it.
- *Cloud servers*. The capacity to handle and maintain data belonging to data owners is provided by the extensive storage and sophisticated processing capabilities of cloud services. The csps are in responsible of generating query results based on the search words entered by the clients, encrypting the search terms, and then sending the search terms to the users.
- *Users*. Users are sometimes referred to as those who joined to search for coded phrases in the restricted content. Please be aware that every user in this article has a public ID.

A. THREAT MODEL

We have used the word "frank," which is also used in other proposals for secure cloud-based data searches, to define KGC and authorized users. The clouds are described as being honest yet mysterious.

Homomorphic: For any two vectors b_1, b_2, and random integers r_1, r_2, then $H(r_1 b_1 \quad r_2 b_2) \quad H(b_1)^{r_1} H(b_2)^{r_2}$.

It is difficult to obtain b1, b2, b3, r1 y r2 (b3 /= r1b1 + r2b2) for just about any logarithmic time method that fulfils H (b3) = Nts (b1) r1 H (b2) r2)

3. A VERIFIABLE PUBLIC KEY ENCRYPTION SCHEME WITH KEYWORD SEARCH IN MULTI-USER SETTING

A. SYSTEM MODEL

The prototype system is shown in figure 4. The program's four primary parts are the crucial center, data owners, datacenters, and data consumers. Server follows the plan fairly and makes an attempt to enquiringly examine the data it gets in order to gain additional knowledge. Using the information that the cloud may collect, we estimate the security strategy to be as follows:

Model for Known Ciphertext. Under this paradigm, which is intended to protect the phrases from the public cloud, the device can only view the encrypted message. More specifically, cloud servers enable data users to do searches on encrypted communications. By employing the ciphertexts to invert the encryption of the data set, the server in our system creates a Z-index system, which can subsequently be used as a search term for confirmation. However, the server is unable to initially extract those words from encrypted data since it is blind to the user's secret key.

- *DEFINITION*

Before transmitting a document to a cloud server, a data owner would first decrypt it using a widely used conventional cryptographic approach. After adding each word to the decryption, the data owner will send the following answer to public cloud. PEKS (pk, wi):

$E(file)||PEKS(w_1, pk)||\ldots||PEKS(w_m, pk)$,
Where is a rudimentary kind of encryption with the above-mentioned properties. This study examined how the server scans all data including a hashtag query and how the user assesses the comprehensiveness and correctness of the return list (w1, w2,, wt). We exclude discussing individual r.e.

Definition 1: The preceding techniques make up a verified public-key encryption system featuring search query for many people:

- ***Setup***(1^{λ}): The Setup (1) method returns a pair of key sk and cryptographically pk after receiving a secure indicator,
- ***KeyGen***$(1^{\lambda}, id)$: The ***KeyGen*** algorithm takes as input a
- a search's outcomes are finished. Output 1 if the findings are accurate and comprehensive; alternatively, input 0.

PEKS (W_1)	E ($file_1$)	E ($file_2$)		
PEKS (W_2)	E ($file_1$)	E ($file_2$)	E ($file_3$)	
.....	...	...	...	...
PEKS (W_{m-1})	E ($file_1$)	E ($file_2$)	E ($file_3$)	
PEKS (W_m)	E ($file_1$)	E ($file_2$)		

Fig 2: An inverted encryption index structure

4. PRODUCTIVITY ANALYZER

This section evaluates the efficiency of our technique in terms of its characteristics, computational cost, the comparability of benchmark searching cryptographic protocols, and experimental results. Figures 2 assume that DO represents the number of authorized involved parties, n represents the number of data files, m represents the number of search phrases, t represents the number of aspects searched, and d represents the number of search results.

First, we assess the value and computational burden of our approach by comparing it with the other clustering techniques in figure 4.

In order to demonstrate the retrieval accuracy utilizing a data set, we evaluate several comparable searching encryption algorithms. The results are shown in Column 3. In general, folder and topic index structures—the former of which is sometimes referred to as the ir system—are the two major forms of index structures. Understanding methods is possible because of the index's structure, which makes our scheme less complex than methods. To ensure the precision and thoroughness of search engine results, we suggest the R t index in this scheme, which offers text search plus results validation. Comparatively, it shows that our approach is more successful when all of the components are included.

Fig 3: Keygen algorithm comparison.

To evaluate the computational efficiency of our strategy, we run comparison experiments utilizing VMKDO16 on only one data set, the Houston email collection. On a machine with an Intel Core i5 processor running at 2.6 GHz, the tests are conducted on Windows. We define E(Fq) as y2 x3 x, with G1 being merely a subgroup of E and q being a large prime number (Fq). G1 has a base field size of 512 bits and a unit structure size of 160 bits. Figures illustrate the study's results.

Figures show how the processing time of the Full crack approach in two ways is improved by DOs nearly continually (Here we set DO, 5000]). Furthermore, we can observe that our method uses less computational power than VMKDO16 since it just calls.

In order to create a set of data boss's keys, the VMKDO16 approach calls for two multiplication operations as well as the choice of two random numbers for each data subject. The secret keys are generated via a hashing process using the VMKDO16 method.

a process Before producing unique identities for the encrypted file set during the PEKS stage, VMKDO16 must first encrypt file set F using the common public key encryption method (Here we set m [1, 1000]). The complexity of the computation required to generate the signatures for each file system frame increases. The specified keyword set is then used to generate the index for the file set. The main components of the approach are a large number of bilinear pairings and exponential processes. Our method simply needs two multiplication operations, two additions, or a hash operation to finish the PEKS process. As a consequence, the calculation time of the PEKS technique in the VMKDO16 plan is much longer than that of our methods. Results of the study, which support our investigation. In essence, the keyword m affects the 15(15 methodology, and as m rises, so does the computing burden on the procedure. However, because adding and multiplying only need a little amount of computation, our method performs essentially the same

Figure from the testing phase shows that our technique is substantially less computationally intensive than the system VMKDO16 when there are fewer search words (Here we set t [150, 750]). The computation time for the VMKDO16 technique is essentially constant, however for our system, it rises linearly with t. This means that the quantity of search phrases may have a significant impact on the possible backdoor advantage.The attribute encryption method is used in the construction of the VMKDO16 system. Regardless of the quantity of phrases, the Testing approach just necessitates 3 strength exponent processes and 3 bilinear pairing activities throughout the Testing phase. Because the encoded indexes include words and our system is designed using the hmac encryption approach, it should expand linearly as the number of searched keywords increases. Therefore, when t is large enough, the VMKDO16 approach will perform better than our method. Fortunately, customers often note that few keyword terms are utilized. As a result, our method consistently performs better than VMKDO16 when there are fewer search terms.

CONCLUSION

In multi-user scenarios, it is advised to combine encryption techniques with verified encrypted public keys. Our technique enables the creation of an index structure for inversion decryption by the servers without the need for a question door, bringing the runtime of a specific search query down to O. (m). Data indicate that it clearly has an advantage over rivals. Our solution also allows a

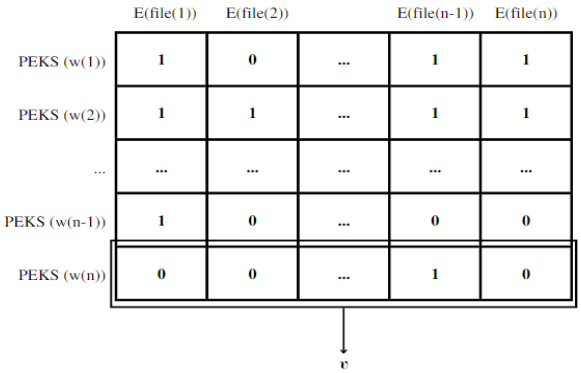

Fig 4: Index-based searchable encryption schemes comparison

large number of users to execute encrypted keyword searches while concurrently confirming the correctness and completeness of serps in multi-user scenarios. It is secure based on a security analysis utilizing the approximately problem with a random generator.

REFERENCES

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ''Public key encryption with keyword search,'' in *Advances in Cryptology— EUROCRYPT*. Berlin, Germany: Springer, 2004, pp. 506–522.

[2] D. Boneh and B. Water, ''Conjunctive, subset, and range queries on encrypted data,'' in *Theory of Cryptography*. Berlin, Germany: Springer, 2007, pp. 535–554.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ''Public key encryption with key- word search revisited,'' in *Computational Science and Its Applications— ICCSA*. Berlin, Germany: Springer, 2008, pp. 1249–1259.

[4] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, ''Blind and anony- mous identity-based encryption and authorised private searches on public key encrypted data,'' in *Public Key Cryptography—PKC*. Berlin, Germany: Springer, 2009, pp. 196–214.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ''Privacy-preserving multi- keyword ranked search over encrypted cloud data,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[6] M. Li, S. Yu, N. Cao, and W. Lou, ''Authorized private keyword search over encrypted data in cloud computing,'' in *Proc. IEEE 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2011, pp. 383–392.

[7] C. Gu, Y. Guang, Y. Zhu, and Y. Zheng, ''Public key encryption with keyword search from lattices,'' *Int. J. Inf. Technol.*, vol. 19, no. 1, pp. 1–10, 2013.

[8] C. Hou, F. Liu, H. Bai, and L. Ren, ''Public-key encryption with keyword search from lattice,'' in *Proc. IEEE 8th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC)*, Oct. 2013, pp. 336–339.

[9] B. Wang, W. Song, W. Lou, and Y. T. Hou, ''Inverted index based multi- keyword public-key searchable encryption with strong privacy guarantee,'' in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 2092–2100.

[10] J. Li, X. Lin, Y. Zhang, and J. Han, ''KSF-OABE: Outsourced attribute- based encryption with keyword search function for cloud storage,'' *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.

[11] K. Emura, G. Hanaoka, K. Nuida, G. Ohtake, T. Matsuda, and S. Yamada, ''Chosen ciphertext secure keyed-homomorphic public-key cryptosys- tems,'' *Des., Codes Cryptogr.*, vol. 86, no. 8, pp. 1623–1683, 2018.

[12] R. C. Merkle, ''A certified digital signature,'' in *Proc. Int. Conf. Adv. Cryptol.*, 1989, pp. 218–238.