SPS FOR INTELLIGENT PROCESSING OF ENCRYPTED DATA IN CLOUD

[1]Y.Amrutha ,[2]K.Arun Kumar, [3]K.Sreevani,
[4]K.Nandini, [5]M.Hareesh, [6]M.R Nilesh,
[1,2,3]Assistant Professor, Dept. of CSE, [4,5,6] B. Tech., (CSE)
Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

Abstract – Phrase search allows retrieval of documents containing an exact phrase, which plays an important role in many machine learning applications for cloud-based IoT, such as intelligent medical data analytics. In order to protect sensitive information from being leaked by service providers, documents (e.g., clinic records) are usually encrypted by data owners before being outsourced to the cloud. This, however, makes the search operation an extremely challenging task. In this paper, we propose **P3**, an efficient privacy-preserving phrase search scheme for intelligent encrypted data processing in cloud-based IoT. Our scheme exploits the homomorphic encryption and bilinear map to determine the location relationship of multiple queried keywords over encrypted data. It also utilizes a probabilistic trapdoor generation algorithm to protect users' search patterns. Thorough security analysis demonstrates the security guarantees achieved by **P3**. We implement a prototype and conduct extensive experiments on real-world datasets. The evaluation results show that compared with existing multi keyword search schemes, **P3** can greatly improve the search accuracy with moderate overheads.

Keyword: -Secure Search, Encrypted Data, Cloud. IoT

1. INTRODUCTION

PHRASE search, which allows users to search for sentences or documents containing a specific phrase that consists of a set of consecutive keywords [1], serves as an important building block in many machine learning applications for cloud-based IoT [7]. For instance, it can be applied to intelligent clinical data analytics collected from medical IoT devices, which retrieves medical records related to a certain disease (e.g., myocardial infarction) and feeds machine learning algorithms to obtain portent symptoms of the disease. It can also be applied to the

emerging entityoriented search [1], which identifies the records within which the exact description of an entity (e.g., person or event) occurs. The resulting records can be utilized for situation assessment and intelligent decision making. Another application scenario refers to the semantic search in knowledge graphs, which searches for entities with semantic similarity (e.g., titles, positions, and interests) and provides input signals to machine learning models for recommendation of products, news, and advertisements.

The combination of cloud computing and IoT enables powerful processing of data beyond individual IoT devices with limited capabilities. This, however, raises a great concern about the security and privacy of IoT data stored in the cloud, as untrusted cloud service providers may get access to sensitive data or even result in data leakage accidents . In order to protect data privacy, data owners can opt to encrypt their sensitive data before outsourcing the storage of the data to remote cloud servers. For instance, a healthcare company may store their encrypted patients' records in the cloud, and allow only the authorized users to perform phrase search over these records. This naturally imposes a requirement on the cloudbased search engine to perform phrase search operations over encrypted data.

Many schemes [2, 4, 5, 7, 8] have been proposed to enable efficient search operations over encrypted textual data, as summarized in Table I. Existing solutions to the single-keyword and multi-keyword search problems cannot be used to perform phrase search over encrypted documents, because they are unable to determine the positional1 relationship of the keywords composing a phrase in the encrypted environment. For instance, the conjunctive keyword search scheme [4] will return a document if it contains each keyword at least once, regardless of whether these keywords appear consecutively as a phrase. Therefore, if we use this scheme for phrase search, we would end with inaccurate results . There are a limited number of studies targeting the phrase search problem over encrypted data. These solutions, however, generally involve notable limitations as shown in Table I, e.g., by either requiring resource-consuming multiple rounds of client-server interactions, or relying on a behalf of the client. Since the client-side IoT devices usually have constrained computing and storage resources, we aim at developing a phrase search scheme that achieves all of the attributes. The main challenge is to enable cloud servers to make a judgement on whether the keywords occurring in an encrypted document are consecutive or not, without leaking sensitive information.

In this paper, we propose P3, a new Privacy-Preserving Phrase search scheme over cloud-based encrypted data. We take advantage of the inverted index structure to build a secure index that achieves greater flexibility and efficiency. The inverted index is one of the most popular and efficient index structures for plaintext search. Compared with the diverse self designed index structures [4, 5], the inverted index structure can improve retrieval efficiency and scalability in practice. To tackle the challenge of determining the positional relationship of queried keywords over encrypted data, we resort to the homomorphic encryption and bilinear map, which enables the client to obtain exact search results from a single interaction with the cloud server. As the phrase search is a special case of multi-keyword search, our solution can also perform conjunctive multi-keyword search efficiently.

1) We propose a secure single-interaction phrase search scheme that enables phrase search over encrypted data in cloud-based IoT, without relying on a trusted third-party.

2) We employ the combination of homomorphic encryption and bilinear map to determine the pairwise positional relationship of queried keywords on the cloud server side. It can be used as a building block in other relevant application scenarios.

3) We implement a prototype of P3 and conduct extensive experimental evaluation using real-world datasets. Results demonstrate that P3 greatly improves the search accuracy with moderate overheads.

2. RELATEDWORK

ExistingSystem

The secure searchable encryption problem was first addressed by Song et al., which was index-free and could merely support exact single keyword search. In order to extend the functionality and efficiency of searchable encryption, follow-ups have proposed various schemes that support single keyword search and exact or fuzzy multi-keyword search by using either self-designed indexes or the typical inverted index structure. Several attempts have been taken to extend the fuzzy multi-keyword search scheme to support phrase search, either by treating a pre-defined phrase (e.g., network security) as a single keyword [6] or introducing a TTP server on the client side.

Tang et al.proposed a phrase search construction over encrypted cloud data, but failed to implement and evaluate their proposal in real-world application scenarios. For each individual phrase

recognition, this construction needed two rounds of communications between the client and the server, and also required a large number of trapdoors generated by the client. The authors in [20] proposed a phrase search scheme with relatively low storage and computational overhead. However, they failed to present a complete threat model, a security definition, or a reasonable security proof. Therefore, it remains unclear about the privacy guarantees provided by the proposed method.

Disadvantages

In the existing work, phrase search construction over encrypted cloud data, but failed to implement and evaluate their proposal in real-world application scenarios due to lack of poor techniques methods.

Existing solutions to the single-keyword and multi-keyword search problems cannot be used to perform phrase search over encrypted documents, because they are unable to determine the positional1 relationship of the keywords composing a phrase in the encrypted environment.

In the proposed system, the system proposes P3, a new Privacy-Preserving Phrase search scheme over cloud-based encrypted data. We take advantage of the inverted index structure to build a secure index that achieves greater flexibility and efficiency. The inverted index is one of the most popular and efficient index structures for plaintext search. Compared with the diverse self designed index structures, the inverted index structure can improve retrieval efficiency and scalability in practice.

To tackle the challenge of determining the positional relationship of queried keywords over encrypted data, we resort to the homomorphic encryption and bilinear map, which enables the client to obtain exact search results from a single interaction with the cloud server. As the phrase search is a special case of multi-keyword search, our solution can also perform conjunctive multi-keyword search efficiently.

The system proposes a secure single-interaction phrase search scheme that enables phrase search over encrypted data in cloud-based IoT, without relying on a trusted third-party.

The system employs the combination of homomorphism encryption and bilinear map to determine the pair wise positional relationship of queried keywords on the cloud server side. It can be used as a building block in other relevant application scenarios.

The system implements a prototype of P3 and conduct extensive experimental evaluation using real-world datasets. Results demonstrate that P3 greatly.

Advantages

The system is more effective due to Index privacy Since the secure index can be regarded as a representation of the encrypted documents, any further information (e.g., keywords) should not be deduced from the index by the cloud server, except for the relationship between a trapdoor and its corresponding search results.

This scheme is more secured since it is protecting privacy associated with the phrase search operation, which consists of three types of privacy, namely the document set privacy, the index privacy and the trapdoor privacy to gather.

3. IMPLEMENTATION

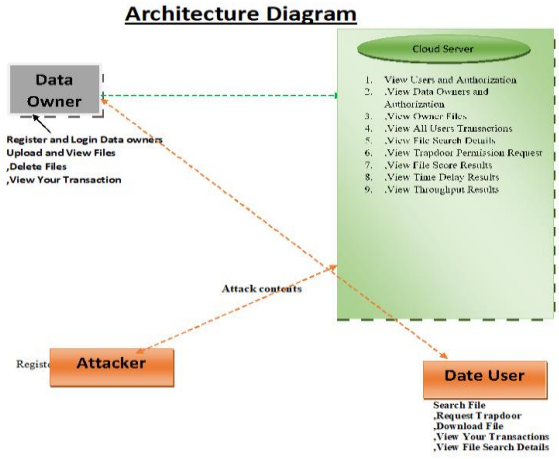


Fig 1. Architecture Diagram

Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the file and the index name and then store in the cloud. The data encryptor can have capable deleting of a specific file. And also he can view the transactions based on the files he uploaded to cloud and will do the following operations like **Upload**, View Files, Delete Files, and View Your Transaction.

Data User

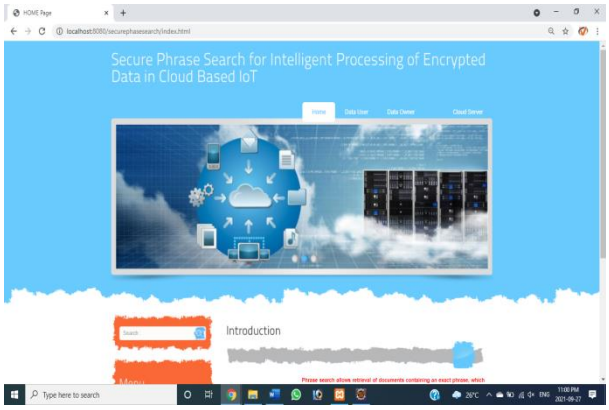
In this module, user logs in by using his/her user name and password. After Login user requests search control to cloud and will Search for files based on the index keyword with the Score of the searched file and downloads the file. User can view the search of the files and also do some operations like Search File, Request Trapdoor, Download File, View Your Transactions, View File Search Details

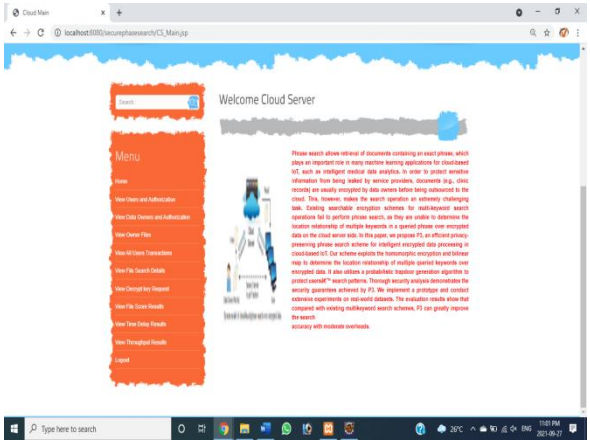
Cloud Server

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with Remote User. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.The cloud server authorizes the data owner and the data user and es the search requests sent from the users. Also in this module it shows personalized search model and the interest search model. Can View Users and Authorization, View Data Owners and Authorization ,View Owner Files ,View All Users Transactions ,View File Search

Details ,View Trapdoor Permission Request, View File Score Results ,View Time Delay Results, View Throughput Results

4. EXPERIMENTAL RESULTS





5. CONCLUSION

In this paper, we presented a novel scheme, P3, which tackled the challenges in phrase search for intelligent encrypted data processing in cloud-based IoT. The scheme exploits the homomorphic encryption and bilinear map to determine the pairwise location relationship of queried keywords on the cloud server side. It eliminates the need of a trusted third party and greatly reduces communication overheads. Thorough security analysis illustrated that the proposed scheme provides the desired security guarantees. The experimental evaluation results demonstrated the effectiveness and efficiency of the proposed scheme. In future work, we plan to further improve the flexibility and efficiency of the scheme.

6. REFERENCES

[1] A. Anand, I. Mele, S. Bedathur, and K. Berberich. Phrase queryoptimization on inverted indexes. In Proc. of ACM CIKM, pages 1807–1810. ACM, 2014.

[2] S. Ananthi, M. S. Sendil, and S. Karthik. Privacy preserving keywordsearch over encrypted cloud data. Communications in Computer &Information Science, 190:480–487, 2011.

[3] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-dnf formulas onciphertexts. In TCC, pages 325–341. Springer, 2005.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou. Privacy-preserving multikeywordranked search over encrypted cloud data. In IEEE INFOCOM,pages 829–837, April 2011.

[5] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Y. Zomaya.An efficient privacy-preserving ranked keyword search method. TPDS,27(4):951–963, 2016.

[6] M. Chuah and W. Hu. Privacy-aware bedtree based solution for fuzzymulti-

keyword search over encrypted data. In Workshops of IEEEICDCS, pages 273–281, June 2011.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky. Searchablesymmetric encryption: Improved definitions and efficient constructions.In Proc. of ACM CCS, pages 79–88, New York, NY, USA, 2006. ACM.

[8] B. Dan, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public keyencryption with keyword search. In EUROCRYPT 2004, pages 506–522.Springer, 2004.

[9] X. Du, M. Guizani, Y. Xiao, and H. Chen. Transactions papersa routing-driven elliptic curve cryptography based key managementscheme for heterogeneous sensor networks. IEEE Transactions onWireless Communications, 8(3):1223–1229, March 2009.

[10] X. Du, Y. Xiao, M. Guizani, and H. H. Chen. An effective keymanagement scheme for heterogeneous sensor networks. Ad HocNetworks, 5(1):24–34, 2007.

[11] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren. Toward efficient multikeywordfuzzy search over encrypted outsourced data with accuracyimprovement. IEEE Transactions on Information Forensics & Security,11(12):2706–2716, 2017.

[12] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren. Ablockchain-based privacy-preserving payment mechanism for vehicleto-grid networks. IEEE Network, pages 1–9, 2018.

[13] X. Hei, X. Du, S. Lin, and I. Lee. Pipac: Patient infusion patternbased access control scheme for wireless insulin pump system. In 2013Proceedings IEEE INFOCOM, pages 3030–3038, April 2013.

[14] S. Kamara, C. Papamanthou, and T. Roeder. Dynamic searchable symmetric encryption. In Proc. of ACM CCS, pages 965–976, NewYork, NY, USA, 2012. ACM.

[15] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen. Enabling efficientmulti-keyword ranked search over encrypted mobile cloud data throughblind storage. IEEE Transactions on Emerging Topics in Computing,3(1):127–138, 2015.