A ES

ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021

https://doi.org/10.5281/zenodo.12726549

SPS FOR INTELLIGENT PROCESSING OF ENCRYPTED DATA INCLOUD

K VISWANATH, VIJAYA BHASKAR MADGULA, D SNEHA
Assistant Professor [1,2,3]
viswanath.k003@gmail.com, vijaya.bhaskar2010@gmail.com, sneha.dharmavaram@gmail.com
Department of CSE, Sri Venkateswara Institute of Technology,
N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:

Secure Search, Encrypted Data, Cloud. IoT

ABSTRACT

Intelligent medical data analytics is only one of several cloud-based IoT machine learning applications that rely on phrase search to retrieve documents that include an exact term. Data owners often encrypt documents (such as medical records) before outsourcing them to the cloud to prevent the leakage of sensitive information. On the other hand, this makes the search operation a very difficult process. Smart encrypted data processing in the cloud is the focus of this article, where we provide P3, a privacy-preserving phrase search strategy that is both efficient and effective. We find the geographical association of numerous requested keywords over encrypted data by using the homomorphic encryption and bilinear map in our technique. In addition, it safeguards users' search habits by use of a probabilistic trapdoor creation method. A comprehensive evaluation of P3's security features reveals the benefits of these enhancements. We put a prototype into action and do comprehensive tests using datasets from the real world. P3 significantly outperforms state-of-the-art multi-keyword search algorithms in terms of search accuracy while imposing only minor overheads, according to the assessment findings.

A ES

ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021

https://doi.org/10.5281/zenodo.12726549

INTRODUCTION

Many machine learning applications for cloud-based IoT rely on PHRASE search, which enables users to search for phrases or documents that include a specified phrase made up of consecutive keywords [1]. Intelligent clinical data analytics derived from medical IoT devices, for instance, may gather patient records linked to a certain illness (like myocardial infarction) and input them into machine learning algorithms to predict when the patient would experience particular symptoms. Moreover, it is applicable to the

An entity-oriented search [1], which finds the records where an entity's (person's or event's) precise description appears. Situation evaluation and rational decision making may be aided by the records that result. One such use case is knowledge graphs' semantic search, which looks for entities that are similar in meaning (such as jobs, interests, or titles) and feeds that information into machine learning models that then propose content (such as news articles, items, or ads).

With cloud computing and the Internet of Things (IoT), data may be processed powerfully, beyond the capability of individual IoT devices. However, this does bring up serious concerns about the privacy and security of IoT data kept in the cloud, as data leakage incidents or access to sensitive information by unreliable cloud service providers are real possibilities. If data owners are concerned about the privacy of their sensitive information, they have the option to encrypt it before entrusting it to distant cloud servers for storage. For instance, a healthcare provider might encrypt patient data before storing them in the cloud, ensuring that only authorised individuals can access them via keyword searches. Because of this, it is essential that the cloud-based search engine be able to do phrase searches across encrypted data.

Table I summarises the many techniques that have been suggested[2,4,5,7,8] to facilitate effective search operations over encrypted textual material. Phrase searches over encrypted documents are infeasible with current methods for single-keyword and multi-keyword searches because to their inability to decipher the positional1 connection between the keywords that make up a phrase in an encrypted setting. If a document includes each keyword at least once, even if they don't exist in a phrase, the conjunctive keyword search scheme [4] will return it. Thus, we would get erroneous results if we do phrase searches using this approach. Few research have focused on the term search issue with encrypted data. Table I shows that these solutions often have significant constraints, such as the need for resource-intensive client-server exchanges or the client's reliance on another party. We intend to build a word search method that accomplishes all of the features, as the computational and storage capabilities of client-side IoT devices are often restricted. Without disclosing sensitive information, the biggest obstacle is making it possible for cloud servers to determine whether the keywords in an encrypted document are sequential.

We provide P3, a novel privacy-preserving phrase search algorithm for encrypted data stored in the cloud, in this article. In order to construct a safe index that is both more flexible and efficient, we use the inverted index structure. When it comes to plaintext searches, the inverted index is a popular and effective index structure. In fact, the inverted index structure may increase retrieval efficiency and scalability compared to the different self-designed index structures [4, 5]. By using homomorphic encryption and bilinear maps, we are able to overcome the difficulty of deciphering the spatial connection of searched keywords over encrypted data. This allows the client to get precise search results within a single communication with the cloud server. Since phrase searches are a subset of multi-

A ES
ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021
https://doi.org/10.5281/zenodo.12726549

RELATED WORK

Existing System

In their first attempt to solve the safe searchable encryption challenge, Song et al. relied only on specific single term searches and did not include any indexes. Subsequent works have suggested a number of techniques to improve the efficiency and utility of searchable encryption; these include self-designed indexes, the conventional inverted index structure, and systems that enable precise or fuzzy multi-keyword searches as well as single-keyword searches. A number of initiatives have our technology is able to quickly conduct conjunctive multi-keyword searches as well.

To facilitate phrase search over encrypted data in cloud-based IoT, we provide a safe single-interaction phrase search method that does not depend on a trusted third party.
2) To find the pairwise positional connection of the searched keywords on the server side of the cloud, we use a mix of homomorphic encryption and bilinear map. Other applicable application scenarios may use it as a building component.
3) We put a P3 prototype into action and test it extensively using real-world datasets. The findings show that P3 significantly enhances search accuracy with relatively low overheads. initiatives have been made to augment the fuzzy multi-keyword search scheme with phrase search capabilities, either by including a TTP server onto the client side or by interpreting pre-defined phrases as individual keywords, such as "network security" [6]. Although Tang et al. suggested building keyword searches over encrypted cloud data, they never got around to testing and implementing their idea in actual use cases. With respect to every single term It was necessary for the client to produce a significant number of trapdoors and for there to be two rounds of communications between the server and the client for this structure to be recognised. A word search strategy with little computational and storage cost was suggested by the authors in [20]. But neither a comprehensive threat model nor a plausible security proof were provided. That is why the suggested method's privacy assurances are still up in the air.

Disadvantages

Previous research attempted to build phrase searches over encrypted cloud data, but they lacked the proper tools to test and refine their ideas in practical settings.
Phrase searches over encrypted documents are infeasible with current methods for single-keyword and multi-keyword searches because to their inability to decipher the positional1 connection between the keywords that make up a phrase in an encrypted setting.
P3, a novel Privacy-Preserving Phrase search strategy over encrypted data stored in the cloud, is offered by the system. In order to construct a safe index that is both more flexible and efficient, we use the inverted index structure. Reversed indexing is among the standard and most effective index formats for plaintext searches. The inverted index structure has the potential to enhance retrieval efficiency and scalability in comparison to the many self-designed index structures.
By using homomorphic encryption and bilinear maps, we are able to overcome the difficulty of deciphering the spatial connection of searched keywords over encrypted data. This allows the client to get precise search results within a single communication with the cloud server. Our method is capable of effectively doing conjunctive multi-keyword searches as well, as phrase searches are a subset of multi-keyword searches.
Without depending on a trusted third party, the system offers a safe single-interaction phrase search strategy that allows phrase search over encrypted data in cloud-based IoT.
On the server side of the cloud, the system uses a mix of bilinear maps and homomorphism encryption to find the pair-wise positional connection of the searched keywords. Other applicable application scenarios may use it as a building component.
By using real-world datasets, the system performs thorough experimental assessment and applies a P3 prototype. The results show that P3 significantly.

A ES
ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021
https://doi.org/10.5281/zenodo.12726549

Advantages

Index privacy makes the system more efficient. The cloud server should not infer any additional information (such as keywords) from the secure index, which can be seen as a representation of the encrypted documents. The only exception to this rule is the connection between a trapdoor and its associated search results.
The phrase search operation involves three kinds of privacy—document set privacy, index privacy, and trapdoor privacy to gather—and our technique is more secure since it protects all three.

1. IMPLEMENTATION

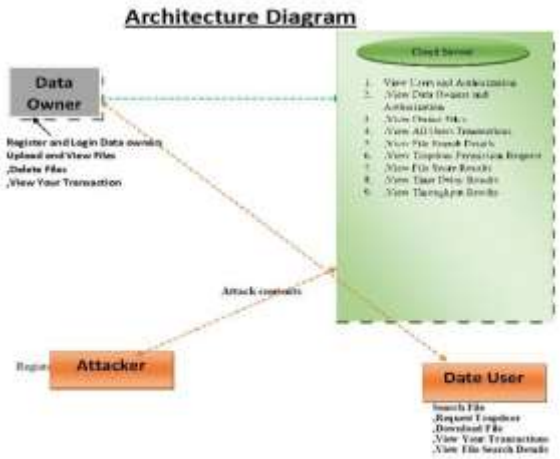

Fig 1. Architecture Diagram

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 alsohe 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

Users are able to access this module by entering their login credentials. Once logged in, users may request search control to the cloud, which will then search for files using index keywords and the search score before downloading them. The user may see the results of their file searches and do activities like as searching, downloading, seeing their transactions, and requesting a trapdoor.

Cloud Server

The cloud server manages a cloud toprovide data storage service. Data ownersencrypt their data files and store them inthe cloud for sharing with Remote User.To access the shared data files, dataconsumers download encrypted data filesof their interest from the cloud and thendecrypt them.The cloud server authorizesthe data owner and the data user andes the

ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021

https://doi.org/10.5281/zenodo.12726549

search requests sent from the

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 PermissionRequest, View File Score Results ,ViewTime Delay Results, View Throughput Results

2. EXPERIMENTAL RESULTS

3. CONCLUSION

Our innovative P3 approach was introduced in this study to address the difficulties of phrase search for intelligent encrypted data processing in cloud-based IoT. The method uses bilinear maps and homomorphic encryption to find the pairwise location relationship of searched keywords on the server side of the cloud. By doing away with the need for a reliable third party, it significantly lowers communication overheads. Full examination of safety measures shown that the suggested plan offers the required security assurances. The efficiency and efficacy of the suggested strategy were proven by the experimental assessment findings. We want to increase the scheme's efficiency and adaptability in further work.

4. REFERENCES

[1] Anand, Anand, Mele, Bedathur, and Berberich, Kishore. Phrase queryoptimization on inverted indexes. Sections 1807–1810 of the proceedings of the ACM Conference on Information and Knowledge Management. published by ACM in 2014.
S. Karthik, **M. S. Sendil, and **S. Ananthi**.Secure keyword search using

ISSN: 2096-3246
Volume 53, Issue 03, Aug 2021

https://doi.org/10.5281/zenodo.12726549

secured cloud storage. Publications in the field of computer and information science, volume 190, pages 480–487, 2011.
P. Nissim, E.-J. Goh, and D. Boneh [3]. On ciphertexts, we evaluate 2-dnf formulas. See TCC, sections 325–341. Published by Springer in 2005.

(4) Cao, N., Wang, C., Li, M., Ren, K., and Lou, W.multi-keyword ranked search with privacy protection using encrypted cloud data. Pages 829–837, published in April 2011 by IEEE INFOCOM.
X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Y. Zomaya are the authors of the fifth point.An effective ranked keyword search algorithm that retains user privacy. TPDS, 2016; 27(4): 951–963.
[6]Chuah M. and Hu W. Fuzzy multi-objective privacy-aware bed-tree

search using keywords on encrypted data. Pages 273–281, June 2011, in Workshops of IEEEICDCS.
By R. Ostrovsky, J. Garay, S. Kamara, and R. Curtmola [7]. Findable symmetric encryption: Enhanced descriptions and effective builds.Proceedings of the 2006 ACM Conference on Computational Support Systems, New York, NY, USA, pages 79–88. ACM.
G. Persiano, R. Ostrovsky, G. D. Crescenzo, and B. Dan [8] conducted the study. Secure key exchange via keyword query. Between pages 506 and 522 of EUROCRYPT 2004.April 2004: Springer.
It was written by X. Du, M. Guizani, Y. Xiao, and H. Chen. A key management strategy for heterogeneous sensor networks that is driven by routing and based on elliptic curve cryptography is presented in the articles. 2008 March issue of IEEE Transactions on Wireless Communications, volume 8, issue 3, pages 1223–1229.
This is according to [10] X. Du, Y. Xiao, M. Guizani, and H. H. Chen. Key management for heterogeneous sensor networks that works. Published in 2007 in the journal Ad HocNetworks, volume 5, issue 1, pages 250–34.
Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren; referenced in [11].Aiming for an improved accuracy rate in multikeyword fuzzy search using encrypted outsourced data. Published in 2017 by the IEEE Transactions on Information Forensics & Security, volume 11, issue 12, pages 2706–2716.

[12] Fermat Gao, Liang Zhu, Min Shen, Khalid Sharif, Zeyn Wan, and Karol Ren. Vehicle-to-grid networks using a privacy-preserving payment mechanism built on blockchain. Pages 1–9, 2018 on the IEEE Network.
Citation: [13] Hei, X., Du, X., Lin, S., and Lee, I. Pipac is a wireless insulin pump device that uses patient infusion patterns as an access control technique. Presented in April 2013 at the IEEE INFOCOM conference, pp 3030–3038.
[14]With contributions from S. Kamara, C. Papamanthou, and T. Roeder. Dynamic searchable symmetric encryption. New York, NY, USA, 2012, pp 965–976, in Proceedings of the ACM Conference on Computational Speech (CCS). ACM.
[15]H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen (researchers). Improving the efficiency of multi-keyword ranked search using blind storage on encrypted mobile cloud data. Published in 2015 in the IEEE Transactions on Emerging Topics in Computing, volume 3, issue 1,, pages 127–138.