ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726595

FPSE: Encrypted Cloud Computing Fast Print Search

C SOUNDARYA, D SNEHA, JANGILI RAVI KISHORE
Assistant Professor [1,2,3]
soundarya.chittepu@gmail.com, sneha.dharmavaram@gmail.com, jangiliravi.kishore1@gmail.com
Department of CSE, Sri Venkateswara Institute of Technology,
N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:

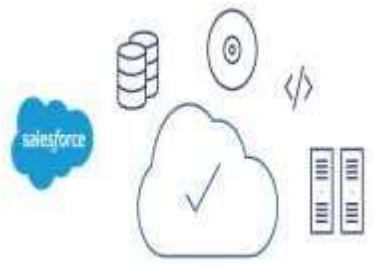
ABSTRACT

The research network has lately seen a surge in interest in distributed computing due to its many advantages; nevertheless, this trend has also brought up concerns about privacy and security. The availability and storage space for sensitive information has been a major issue for the zone. In particular, several researchers combed through encrypted files kept on remote servers in the cloud for answers. There have been a number of approaches to conjunctive catch-all searches, but less research into targeted system searches. With storage and communication costs that are either equal to or better than prior arrangements, we demonstrate a Bloom-based expression search procedure in this study that is much quicker. Using a succession of n-gram channels, our strategy enhances the utility. The approach is flexible enough to withstand consideration connection assaults, and it shows a trade-off between capacity and false positive rate. Also shown is a structural approach that takes an application's objective false positive rate into account.

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

INTRODUCTION

What is cloud computing?



All People ds Talking Approximately "The Cloud." But What Does It Suggest?

More and more, generation is migrating to the cloud. The trend of moving away from traditional software development practices and towards the web has been steadily increasing over the last decade. Future plans for CC in the next decade include innovative ways to work together on the go using mobile devices.

So what is cloud computing? In its most basic form, it is an online method of outsourcing application development. One benefit of computers is that it allows users to access software and apps from any location thanks to the cloud, which stores these programmes on the servers of an external party. This implies that consumers may focus on enjoying the final product rather than worrying about issues like energy storage.

Lifestyles Earlier Than CloudComputing

Costly and intricate, traditional business software has been a constant. To install, setup, test, operate, relax, and update them, you need a whole team of experts.
The largest organisations with the best IT teams aren't obtaining the applications they need, and when you scale that effort over dozens or thousands of apps, it becomes clear why. Organisations of a smaller or medium scale are not at danger.

Cloud Computing: A Better Way

Because you are no longer tasked with managing hardware and software, the hassles associated with preserving your own information are eliminated with cloud computing.

program— that will be handled by a knowledgeable sales team or dealer. You pay for only the resources you use, and any upgrades are automatically applied, thanks to the application-like nature of the shared infrastructure.

They cost less and may be up and running in a matter of days or weeks when built using cloud computing. When you use a cloud app, all you have to do is launch the browser.

Numerous business applications, such as customer relationship management (CRM), human resources (HR), accounting, and many more, are being developed and deployed on the cloud. After extensive testing, several of the biggest companies' sales forces relocated their apps to the cloud.

Many companies are essentially renaming their non-cloud services and products to reflect the popularity of cloud computing. Be sure to do your homework while assessing cloud services, and bear in mind that cloud computing affects both software and hardware.

A ES

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726595

1. TYPES OF SERVICES

Infrastructure-as-a-Service

2 To put it simply, it is the simplest kind of computing functions. Infrastructure such as servers, virtual machines (VMs), storage, networks, and working structures may be installed on a pay-as-you-go basis via a cloud provider. Cloud-Based Platform Software development, testing, distribution, and management environments provided by these services on demand. Platform as a service (PaaS) aims to alleviate developers' concerns about the installation and management of servers, storage, networks, and databases, allowing them to focus on creating internet or mobile applications more quickly.

2.1 Software as a Service

3 In this model, users pay a regular fee in exchange for access to a library of software applications made available over the internet. Software as a service allows cloud providers to take care of hosting, managing, and updating software and underlying infrastructure, including security patches and upgrades. A web browser is often used by clients to access the programme online.

4 their telephone, pill or pc.

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

Adaptable

Cloud computing permits for adaptable applications and programs which are customizable, whilst permitting ownersmanage over the middle code.

Multitenant

Cloud software presents an opportunity to provide personalized packages and portals for number of clients or tenants.

Reliable

Due to the fact it's miles hosted via a third birthday celebration, companies and other users have extra warranty of reliability, and while there are troubles, smooth get admission to to customer service.

Scalable

With the internet of things, it is critical thatsoftware capabilities across each tool and integrates with other applications. cloud applications can offer this.

Comfy

Cloud computing can also assure a greatersecure environment, thanks to multiplied assets for security and centralization ofinformation.

2. LITERATURE SURVEY

1) Public Key Encryption with keywordSearch

2) the term "urgent" in order for the email to be directed appropriately. But Alice would rather not let the gateway decipher all of her communications. Without knowing anything more about the email, we establish and build a system that allows Alice to provide the gateway a key that allows it to check whether the term "urgent" is a keyword in the message. We call this system Public Key Encryption with Search as a keyword. Think of another scenario where Alice receives communications encrypted for her by others and stored on a mail server. With our method, Alice may teach the mail server to recognise mails with a certain keyword, but it will not inform her of anything else. We provide many architectures and a definition of public key encryption using keyword search.

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

3) Building an Encrypted andSearchable Audit Log

A well-designed audit log may faithfully portray previous system activity and is therefore an integral component of any secure system. This is particularly important when there are potential threats whose actions might compromise the audit logs. Even though auditors need access to audit logs in order to evaluate system activity in the past, unauthorised individuals should not have access to the sensitive information that may be included in audit logs. A challenge arises when trying to encrypt audit logs such that only authorised auditors can decipher them, while yet making them easily searchable. In this paper, we detail a method for building searchable encrypted audit logs that may be mixed and matched with several current methods for making tamper-proof logs. To be more specific, we integrated a database query audit log that safeguards data integrity using hash chains and allows querying the encrypted log using extracted keywords via identity-based encryption. Beyond searchable audit logs, our method for keyword searching on encrypted data has extensive applicability.

Secure Conjunctive KeywordSearches for Unstructured Text:

There are a number of searchableencryption schemes that allow secure conjunctive keyword searches over encrypted data, but all of them assume thatthe position of the keywords is known. This is a pity, since in unstructured text,

e.g. the body of an e-mail, this position is unknown and one has to construct O(mn) search tokens for n keywords in a text of length m. In this paper we present a searchable encryption scheme that allows conjunctive keyword searches without specifying the position requiring only one search token with constant ciphertext length. We prove the security of our scheme using the external Diffie-Hellman assumption in the random oracle model.

4) Achieving effective cloud search services: multi-keyword ranked searchover encrypted cloud data supporting synonym query

Abstract: In recent years, consumer-centriccloud computing paradigm has emerged asthe development of smart electronic devices combined with the emerging cloud is achieved. For consumers, they want to find the most relevant products or data,which is highly desirable in the "pay-as- you use" cloud computing paradigm. As sensitive data (such as photo albums,emails, personal health records, financial records, etc.) are encrypted before outsourcing to cloud, traditional keyword search techniques are useless. Meanwhile, existing search approaches over encrypted cloud data support only exact or fuzzy keyword search, but not semantics-based multi-keyword ranked search. Therefore,how to enable an effective searchable system with support of ranked search remains a very challenging problem. This paper proposes an effective approach tosolve the problem of multi-keyword ranked search over encrypted cloud datasupporting synonym queries. The main contribution of this paper is summarized intwo aspects: multi-keyword ranked search to achieve more accurate search results andsynonym-based search to support synonymqueries. Extensive experiments on real- world dataset were performed to validate the approach, showing that the proposed solution is very effective and efficient for multikeyword ranked searching in a cloud environment.

A ES

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726595

Conjunctive Keyword Search Schemes

3. By encrypting data on an untrusted server and providing a database manager with the ability to search for encrypted data containing a certain term, users may implement a keyword search scheme. This method ensures that the database manager cannot expose the user's password. With a conjunctional keyword search method, a user may get results that include many terms with only one query. The inability of a malevolent attacker to construct new legitimate capabilities from the observed ones is one of the security criteria of conjunctive keyword search methods. Conjunctive keyword search algorithms are shown to be insecure in this work. Given two sets of keywords and two sets of capabilities, an attacker may create a new set of capabilities equal to the difference between the two sets of keywords.

4. PROBLEM STATEMENT

- Boneh et al. proposed one of the earliest works on keywordsearching. Their scheme uses public key encryption to allowkeywords to be searchable without revealing data content.
- Waters et al. investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches.
- Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords.
- Other interesting problems, such as the ranking of search results and searching with keywords that might contain errors termed fuzzy keyword search, have also been considered. The ability to search for phrases was also recently investigated.
- Some of the existing system hasexamined the security of the proposed solutions and, where flaws were found, solutions wereproposed
- The cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in caseof data breach.
- By recognizing the almostexponential distribution of keywords, the entries in the keyword location tables are split into pairs to achieve normalization without the high cost of storing unused random data. However, the use of encrypted indexes and theneed to perform client-side encryption and decryption may stillbe computationally expensive in certain applications.
- Its space-efficiency comes at the cost of requiring a brute force location verification during phrase search. Since all potential locationsof the keywords must be verified, the amount of computation required grows proportionally to the file size. As a result, thescheme exhibits a high processing time.

5. PROPOSED SCHEME

- In this paper, we present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme isalso scalable, where documents caneasily be removed and added to thecorpus. We also describe modifications to the scheme tolower storage cost at a small cost in

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

response time and to defend againstcloud providers with statistical knowledge on stored data.

- Although phrase searches are processed independently using our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches. Therefore, we describe both the basic conjunctive keyword search algorithm and the basic phrase search algorithm alongwith design techniques.

MODULES:

- System Framework
- Data Owner
- Data User
- Cloud Server

- **MODULES DESCRIPTION:**

System Framework:

Our standardised approach for keyword searches is housed in this framework. In order to perform hashing and encryption operations, the data owner must first create the necessary encryption keys during setup. The next step is to examine each document in the database for relevant keywords. Hashed keywords and n-grams are connected to bloom filters. Before being uploaded to the server in the cloud, the documents undergo symmetric encryption. The data owner parses the files during setup and then uploads them to the cloud server with Bloom filters applied to add them to the database. When a data owner wants to delete a file and any associated Bloom filters, they only need to make a request to the cloud server. The user inputs data in order to do a search. keyword then it computes and sends a trapdoor encryption of the queried keywords to the cloud to initiate a protocoland returns accurate file. Here weimplement some modules they are DataOwner, Data User and Cloud Server.

Data Owner:

After logging into the Data Owner module, the first step is for the Data Owner to register their details. Once they've done so, they'll need to authenticate their login using an OTP. After that, the data owner may use hashing techniques and encrypted keywords to upload files to the cloud server. Any files saved to the cloud may be seen by this person. The file requests issued by data consumers might be approved or rejected by the data owner.

Data User:

Before they may use the cloud, data users must first register their details in the data user module. All files uploaded by data owners may be searched by data users. The request may be sent to the files, which will

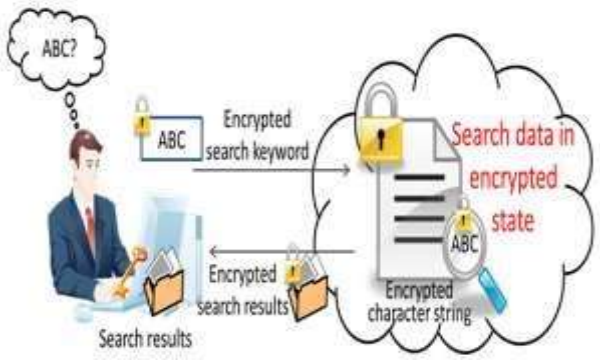
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

subsequently be sent to the data owners. The decryption key will be sent to the registered mail of the data owner after the request has been approved.

Cloud Server:

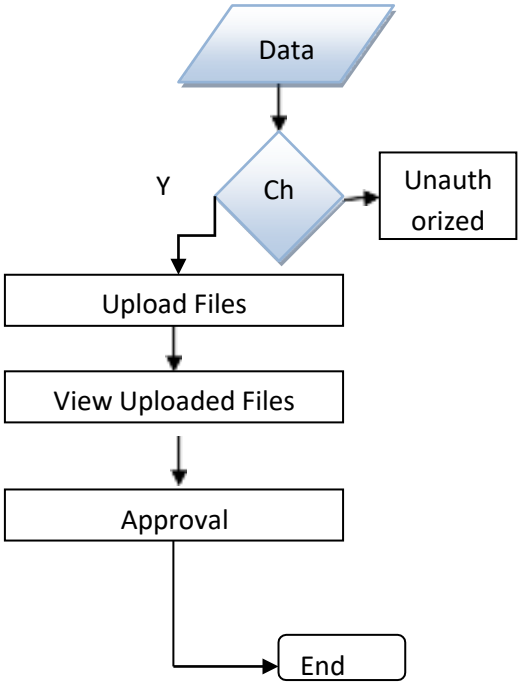
In this module, we develop Cloud Server module. In Cloud Server module, CloudProvider can view all the Data owners and data users' details. CP can able see thefiles in cloud uploaded by the data owners.

6. SYSTEM ARCHITECTURE



6.1 SYSTEM DESIGN

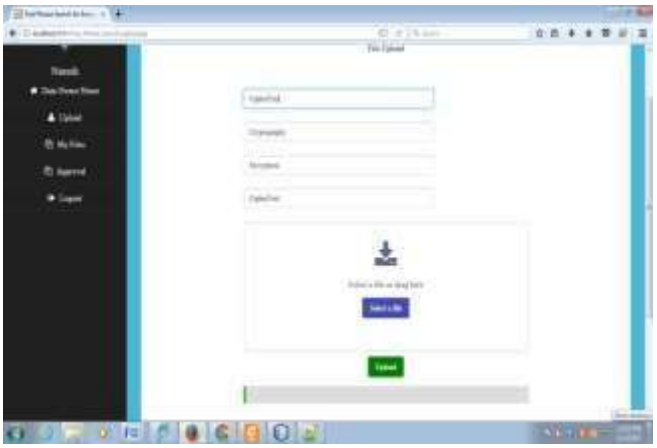
6.2 DFD:

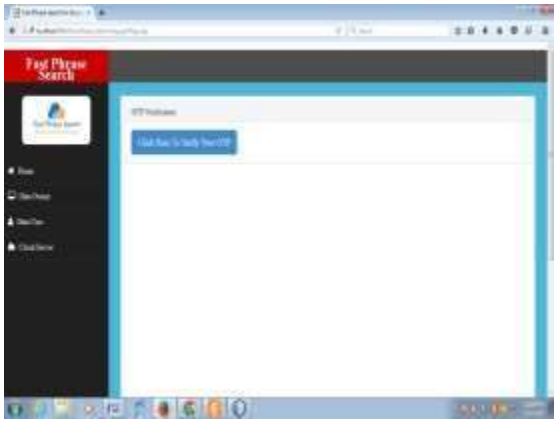


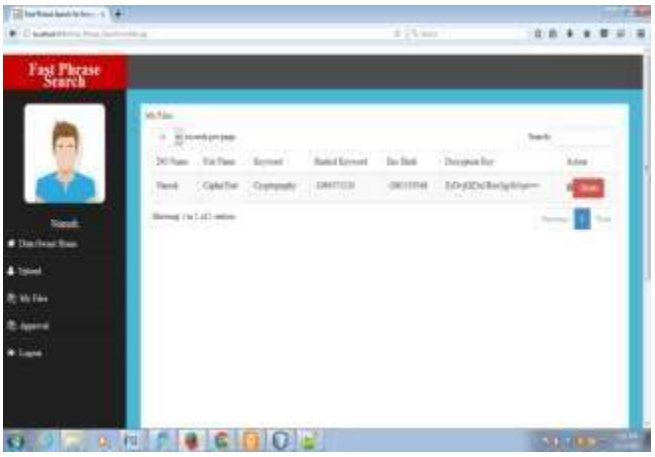
6.1 SAMPLE SCREEN

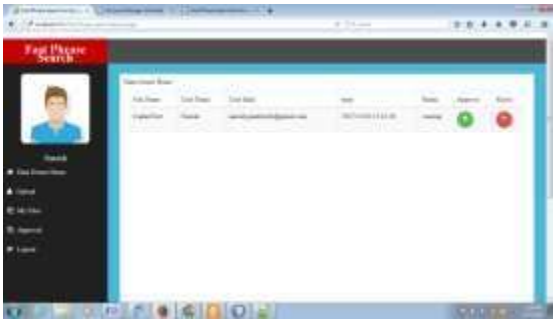
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726595









A ES

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726595

7. CONCLUSION

Our Bloom filter–based phrase search methodology, detailed in this work, outperforms state-of-the-art methods with a single communication round and testing of the filter. Instead of using a location search or a sequential chain verification, the approach reformulates phrase search as n-gram verification, which reduces the computational cost. Without knowing where a sentence is, our algorithms simply take its presence into account. Our techniques are parallelizable, have a reasonable storage demand, and do not necessitate sequential verification. Also, unlike previous methods, ours allows phrase search to operate autonomously, without the need for a conjunctive keyword search to find potential documents. Building a Bloom filter index is a method for quickly verifying Bloom filters that works similarly to indexing. Our experiments also show that it achieves lower storage costs than all preexisting systems, with the exception of those that trade off greater computational costs for lower storage costs.While the suggested solution has a communication cost that is comparable to top current solutions, it may be tuned to obtain high speed or maximum speed with appropriate storage cost, depending on the application. Additionally, a method is detailed for modifying the strategy to prevent inclusion-relation assaults. In order to back up our design decisions, we addressed a number of security and efficiency concerns, including the impact of lengthy words and accuracy rate.

REFERENCES

[1] "Public key encryption with keyword search," in In proceedings of Eurocrypt, 2004, pp. 506–522, by D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano.
An encrypted and searchable audit log was built by Waters, Balfanz, Durfee, and Smetters in 2004 at the Network and Distributed System Security Symposium.

In the 2012 IEEE International Conference on Network Infrastructure and Digital Content, M. Ding, F. Gao, Z. Jin, and H. Zhang presented "An efficient public key encryption with conjunctive keyword search scheme based on pairings," which can be found on pages 526–530.

In the 2011 International Conference on Network and System Security, F. Kerschbaum presented a paper titled "Secure conjunctive keyword searches for unstructured text" (pp. 285-289).
Public key encryption with ranked multikeyword search was presented by C. Hu and P. Liu at the 2013 International Conference on Intelligent Networking and Collaborative Systems (pp. 109-113).
"Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," published in 2014 in the IEEE Transactions on Consumer Electronics, was written by Z. Fu, X. Sun, N. Linge, and L. Zhou.
In their article "Relevance ranking for one to three term queries" published in January 2000 in Information Processing and Management: an International Journal, C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope discuss this topic.
8. "An effective fuzzy keyword search scheme in cloud computing," by H. Tuo and M. Wenping, published in 2013 in the International Conference on Intelligent Networking and Collaborative Systems, pages 786–789.
Presented at the 2013 International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing, the paper "An efficient attack on a fuzzy keyword search scheme over encrypted data" by M. Zheng and H. Zhou is cited as reference [9].

[10] "Encrypted phrase searching in the cloud," in 2012's IEEE Global Communications Conference (pp. 764-770), by S. Zittrower and C. C. Zou.
The paper "Phrase search over encrypted data with symmetric encryption scheme" was presented at the 2012 International Conference on Distributed Computing Systems Workshops and can be found on pages 471-480. The authors are Y. Tang, D. Gu, N. Ding, and H. Lu.

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726595

IEEE International Conference on Cloud Computing, 2015, "An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems" [12] H. Poon and A. Miri. "A low storage phrase search scheme based on bloom filters for encrypted cloud services," in the 2015 IEEE International Conference on Cyber Security and Cloud Computing, [13] published. Referenced in the paper "Difference set attacks on conjunctive keyword search schemes" by H. S. Rhee, I. R. Jeong, J. W. Byun, and D. H. Lee, which was published in 2006 at the Third VLDB International Conference on Secure Data Management, pages 64–74.
[15] "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in 2013's IEEE International Conference on Cloud Computing Technology and Science, pp. 339-346, by K. Cai, C. Hong, M. Zhang, D. Feng, and Z. Lv.