www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Dual server keyword search with public key exchange using keyword mapping technique

N.Giridharan[1], L.Sangavi[2], T.A.Sastinath[2], M.Sharmila Devi[2]

Assistant Professor Department of Computer Science and Engineering K S Rangasamy College of Technology, Tiruchengode- India.

Students, Department of Computer Science and Engineering K S Rangasamy College of Technology, Tiruchengode- India.

ABSTRACT

The advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. It defines and solve the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. This mechanism that reduces the cost of encrypted matching, in the form of a pre-filtering operator using Bloom filters and simple randomization techniques. propose containment obfuscation techniques and provide a rigorous security analysis of the information leaked by Bloom filters in this case. Among various multi-keyword semantics, choose the efficient principle of "Enhanced Association Rule Mining coordinate matching", i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use "inner product similarity" to quantitatively formalize such principle for similarity measurement. First propose a basic EARM scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models.

INTRODUCTION

Cloud computing concept

Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network it's provided for you *as a service* by another company and accessed over the internet, usually in a completely seamless way. exactly where the hardware and software is located and how it all works doesn't matter to you, the user-it's just somewhere up in the nebulous "cloud" that the internet represents.

TYPES OF CLOUD SERVICES

Infrastructure as a service (IAAS)

Means you're buying access to raw computing hardware over the Net, such as servers or storage. Since you buy what you need and pay-as-you-go, **this** is often referred to as utility computing. Ordinary web Hosting is a simple example of IaaS: you pay a monthly subscription or a per-megabyte/gigabyte fee to have a hosting company serve up files for your website from their servers.

Author for correspondence:
Department of Computer Science and Engineering K.S.R College of Engineering (Tiruchencode)

Software as a service (SAAS)

Means you use a complete application running on someone else's system. Web-based email and Google Documents are perhaps the best-known examples. Zoho is another well-known SaaS provider offering a variety of office applications online.

Platform as a service (PAAS)

Means you develop applications using Web-based tools so they run on systems software and hardware provided by another company. So, for example, you might develop your own ecommerce website but have the whole thing, including the shopping cart, checkout, and payment mechanism running on a merchant's server.

TYPES OF CLOUD COMPUTING

Public cloud

Public clouds are owned and operated by third-party cloud service providers, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Private cloud

A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site data center. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud

Hybrid cloud combines public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, a hybrid cloud gives your business greater flexibility, more deployment options, and helps optimize your existing infrastructure, security, and compliance.

USES OF CLOUD COMPUTING

Create new apps and services

Quickly build, deploy, and scale applications-web, mobile, and API on any platform. Access the resources you need to help meet performance, security, and compliance requirements.

Back up and recover data

Protect your data more cost-efficiently and at massive scale by transferring your dataover the Internet to an offsite cloud storage system that's accessible from any location and any device.

Analyze data

Unify your data across teams, divisions, and locations in the cloud. Then use cloud services, such as machine learning and artificial intelligence, to uncover insights for more informed decisions.

Stream audio and video

Connect with your audience anywhere, anytime, on any device with high-definition video and audio with global distribution.

Deliver software on demand

Also known as software as a service (SaaS), on-demand software lets you offer the latest software versions and updates around to customers anytime they need, anywhere they are.

Test and build applications

Reduce application development cost and time by using cloud infrastructures that can easily be scaled up or down.

Embed intelligence

Use intelligent models to help engage customers and provide valuable insights from the data captured.

EXISTING SYSTEM

The large number of data users and documents in cloud, it is crucial for the search service to allow

multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. The searchable encryption focuses on single keyword search or Boolean keyword search, and rarely differentiates the search results.They investigate the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. To address this security vulnerability, we propose a new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, it defines a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF).

In a PEKS system, using the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS cipher texts) with the encrypted data. The receiver then sends the trapdoor of a to-be-searched keyword to the server for data searching. Given the trapdoor and the PEKS cipher text, the server can test whether the keyword underlying the PEKS cipher text is equal to the one selected by the receiver. If so, the server sends the matching encrypted data to the receiver.

PROPOSED SYSTEM

We define and solve the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching". It has been proposed the problem of Secured Multikeyword search (SMS) over encrypted cloud data (ECD), and construct a group of privacy policies for such a secure cloud data utilization system. From number of multi-keyword semantics, we select the highly efficient rule of coordinate matching, i.e., as many matches as possible, to identify the similarity between search query and data, and for further matching we use inner data correspondence to quantitatively formalize such principle for similarity measurement. First propose a basic Secured multi keyword ranked ontology keyword mapping and search scheme

Using secure inner product computation, and then improve it to meet different privacy requirements. The Ranked result provides top k retrieval results. Also propose an alert system which will generate alerts when un-authorized user tries to access the data from cloud, the alert will generate in the form of mail and message.

MODULE DESCRIPTION

Cloud setup module

This module enhances the schemes which allow multi-keyword query and provide result similarity ranking for effective data retrieval, instead of returning undifferentiated results. Privacy-Preserving. To prevent the cloud server from learning additional information from the dataset and the index, and to meet privacy. Efficiency above goals on functionality and privacy should be achieved with low communication and computation over head.

Earm coordinate matching

"Coordinate matching" is an intermediate similarity measure which uses the number of query keywords appearing in the document to quantify the relevance of that document to the query. When users identify the exact subset of the dataset to be regained, Boolean queries achieve well with the exact search necessity stated by the user. It is more elastic for users to identify a list of keywords indicating their concern and regain the most relevant documents with a rank order.

Data privacy, the data owner can resort to the traditional symmetric key cryptography to encrypt the data before outsourcing, and effectively prevent the cloud server into the outsourced data. Index privacy, if the cloud server infers any association between keywords and encrypted documents from index. Therefore, the searchable index should be built to prevent the cloud server from acting such kind of association attack.

Keyword Privacy, as users generally wish to have their search from existence showing to others

like the cloud server, the most vital concern is to hide what they are searching, i.e., the keywords specified by the corresponding trapdoor. The trapdoor can be generated in a cryptographic way to protect the query keywords.

Prefiltering and security management module

This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database.

Finally, the matched word list from the database and the user gets the file from that list. The search query is also described as a binary vector association rule each bit means whether corresponding keyword appears in this search request.the similarity could be exactly measured by inner product of query vector with data vector.

ENCRYPT AND CLIENTMODULE

This module is used to help the server to encrypt the document using TRIPLE DES Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.

This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail from the "customerservice404" email before enter the activation code. After user can download the Zip file and extract that file.

MULTI-KEYWORD MODULE

This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list. The search query is also described as a binary vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by inner product of query vector with data vector.

However, directly outsourcing data vector or query vector will violate index privacy or search privacy. To meet the challenge of supporting such multi-keyword semantic without privacy breaches, we propose a basic SMS scheme using secure inner product computation, which is adapted from a secure k-nearest neighbor (KNN) technique, and then improve it step by step to achieve various privacy requirements in two levels of threat models.

Admin module

This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

Ranking result

When any User request for the data then Ranking is done on requested data using k-nearest neighbour algorithm. For Ranking co-ordinate matching‖ principle is used. After ranking user gets the expected results of the query.

CONCLUSION

The problem of multi-keyword ranked ontology keyword mapping and search over encrypted cloud data, and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching", i.e., as many matches as possible, to effectively capture similarity between query keywords and outsourced documents, and use "inner product similarity" to quantitatively formalize such a principle for similarity measurement.

For meeting the challenge of supporting multi-keyword semantic without privacy breaches, we first propose a basic EARM scheme using secure inner product computation, and significantly improve it to achieve privacy requirements in two

levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset show our proposed schemes introduce low overhead on both computation and communication. As our future work, we will explore supporting other multi-keyword semantics (e.g., weighted query) over encrypted data, integrity check of rank order in search result and privacy guarantees in more stronger threat model.

REFERENCES

[1]. Armbrust M., Fox A., Griffith R., Joseph A. D., Katz R.H., Konwinski A., Lee G., Patterson D.A., Rabkin A., Stoica I. and Zaharia M.,"An Efficient And Privacy-Preserving Semantic Multi- Keyword Ranked Ontology Keyword Mapping And Search Over Encrypted Cloud Data", university of California, berkeley, tech,. 67(4), 2012, 8-54.

[2]. Bellare.M, Boldyreva.A, and ONeill.A (2013),"Privacy-Preserving Ranked Multi-Keyword Search Leveraging Polynomial Function In Cloud Computing", in proceeding. of CRYPTO, 5(1), 2013, 1-21.

[3]. Boneh.D, Crescenzo.G.D, Ostrovsky.R, and Persiano.G, "Secure Ranked Keyword Search Over Encrypted Cloud Data", 7(5), 2014, 22-56.

[4]. Curtmola.R, Garay.J.A, Kamara.S, and Ostrovsky.R, "Searchable symmetric encryption", 34(1), 2016, 1-11.

[5]. Dolev.D, Naor.M,"Privacy Preserving Keyword Searches On Remote Encrypted Data",in SIAM Journal on Computing, Earlyversion in proceedings of STOC '91, 2(1), 2010, 125-137.

[6]. Goh.E.J, "Secure indexes", CryptologyPrint Archive, "Privacy-Preserving Multi-Keyword Ranked Ontology Keyword Mapping And Search Over Encrypted Cloud Data", ACNS, 5(2), 2013, 1-22.

[7]. Goldreich.O and Ostrovsky.R,"Authorized Private Keyword Search over Encrypted Data in Cloud Computing", Journal of the ACM, 23(6), 2014, 4-78.

[8]. Kamara.S and Lauter.K, "Cryptographic cloud storage", in RLCPS, Springer, Heidelberg, 25(10), 2010, 74-82.

[9]. Kilian.J, "Enabling Efficient Fuzzy Keyword Search Over Encrypted Data In Cloud Computing", in Proceedings of ACMSTOC'88, 56(1), 20–31, 2011.

[10]. Kushilevitz.E and Ostrovsky.R, "Privacy Preserving Multi-Keyword Ranked Ontology Keyword Mapping And Search With Anonymous Id Assignment Over Encrypted Cloud Data", in Proceedings of IEEE FOCS'97, 2012, 364–373.

[11]. Sheridan.D, "Privacy-Preserving Multi-Keyword Text Search In The Cloud Supporting Similarity-Based Ranking", in Proceedings of vol. 6(2), 2014, 6-78.

[12]. Singhal.A, "Achieving Secure, Scalable, and Fine-Grained Data", IEEE Data Engineering Bulletin, vol. 24(4), 2011, 35–43.

[13]. Song.D, Wagner.D, and Perrig.A, "Efficient and Secure Multi-Keyword Serach On Encrypted Cloud Data" in Proceedings of S&P, 2(8), 2010, 813-819.

[14]. Vaquero.L.M, Rodero-Merino.L, Caceres.J, and Lindner.M, "Practical Techniques for Searches on Encrypted Data", ACM SIGCOMM Computer Communication. Rev., 39(1), 2015, 50–55.

[15]. Witten.I. H., Moffat.A, and Bell.T.C, "Public Key Encryption with Keyword Search", Morgan Kaufmann Publishing, 56(7), 2016, 128-140.