A SURVEY ON SECURE AND EFFICIENT FEATURE BASED PRODUCT INFORMATION RETRIEVAL FROM CLOUD

[1]**Dr. Sateesh Nagavarapu**, professor, Dept of CSE, Mallareddy Institute of Technology, Post Via Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

[2]**R. Manthru Naik**, Asst. Prof, , Dept of CSE, Mallareddy Institute of Technology, Post Via Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

[3]**D Narahari Asst. Prof.**, Asst. Prof, Dept of CSE, Mallareddy Institute of Technology, Post Via Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

ABSTRACT: When it comes to managing a big number of IT resources in an effective and adaptable way, cloud computing is an exciting new IT method to watch. Companies are increasingly moving their data management systems to the cloud and storing their product information on cloud servers. As an additional problem, how to keep commercially private data secure while yet allowing for the capacity to search it is a major one. An identifier-based and feature-based product search strategy is suggested in this work to ensure privacy. This is done by creating two new index trees that can be searched without having access to the plaintext data. Analysis and simulation findings show that our system is both secure and efficient.

Key Words: Product Information Retrieval; Cloud Computing; Information Security.

1. INTRODUCTION

China's whole industrial chain has to be restructured in light of the recent information technology revolution and the slowdown in the country's economic development. Efforts have been made to further integrate China's e-commerce market with its conventional economy as part of the country's "Internet +" industrial upgrading plan in recent years. As ecommerce has grown in breadth and depth, as well as in the number of sectors it has penetrated, it has helped to alter and upgrade businesses, making it easier for them to compete in today's global economy and society. Chinese ecommerce transactions in 2016 totaled 3.5 trillion dollars, an annual growth rate of around 25.5 percent, according to the Monitoring Report on the Data of China's Ecommerce Market [1]. Ecommerce big data has emerged as a result of the increasing volume of online transactions. Companies' local data storage systems are being stretched to their limits as more and more data files are being kept there. Local hardware failures may cause significant data loss or destruction, which can have a significant impact on a business's day-to-day operations. Because of this, cloud storage systems were developed. Cluster applications, network technologies, and distributed file systems may all be used to aggregate and organise a huge number of different kinds of storage devices in the cloud. Amazon Web Services [2], Microsoft Azure [3], I Cloud [4], and App Engine [5] are just a few of the well-known cloud service offerings available both domestically and internationally.

2. LITERATURE SURVEY

Practical Techniques for Searches on Encrypted Data

To avoid security and privacy issues, it is preferable to keep data on data storage servers such as mail servers and file servers in encrypted form. However, this sometimes necessitates a

trade-off between utility and security. For example, it was previously unknown how to allow the data storage server to do the search and answer the question without compromising the secrecy of the stored data. Our cryptographic algorithms for searching encrypted data are described in this work and guarantees of security are provided for the resultant crypto systems. Because they provide proof-of-concept encryption, an untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that an untrusted server cannot learn anything about the plaintext other than what the search results reveal; and they provide controlled searching, so that an untrusted server cannot look up any random word without the user's permission. They are therefore demonstrably secure. The encryption and search algorithms we provide are simple, fast (only O(n) stream cypher and block cypher operations are required for a document of length), and introduce essentially no space and communication overhead, so they may be used right now.

Functional Encryption for Inner Product Predicates from Learning with Errors

Our functional encryption technique for inner product predicates relies on the complexity of the learning with errors (LWE) issue, which makes it more secure. With this design, we can perform operations on encrypted data such as range and subset searches, polynomial evaluation, and CNF/DNF formulae. Inner products are supported across tiny fields, unlike prior efforts that used bilinear maps. Using lattice-based encryption methods, we have developed the first practical system that goes beyond simple identity-based encryption. Identity-based encryption developed by Agrawal, Boneh, and Boyen is reimagined in our system in a new way (Eurocrypt 2010). Compared to the standard model, ours is a weak form of attribute concealment.

Our lattice predicate encryption approach for inner product predicates is secure due to the complexity of the learning with errors (LWE) issue, which we have demonstrated. Applications like range and subset searches, polynomial evaluation, and CNF/DNF formulae may all be instantiated on encrypted data using our system. Please refer to the complete work for a more in-depth examination of these applications. Using lattice-based encryption methods, we have developed the first practical system that goes beyond simple identity-based encryption.

Secure Conjunctive Keyword Ranked Search over Encrypted Cloud Data

In the cloud computing concept, a shared pool of customizable computing resources (e.g., networks, servers, storage, applications and services) may be supplied and released with minimum administration effort or service provider involvement. For data protection reasons, critical information must be encrypted before being outsourced, which means that standard keyword-based data mining is out of date. It is required to enable numerous keywords in a search request and return documents in the order of their relevance to these keywords due to the enormous number of cloud data users and documents. In other studies on searchable encryption, the search results are seldom sorted, and only a single keyword or Boolean keyword search is used. Defining and solving the difficult challenge of securing conjunctive keyword ranked search over encrypted cloud data is the focus of our research in this article.

Multi-keyword ranking search over encrypted cloud data is addressed in this study, and a number of security needs are outlined. We selected the efficient principle of coordinate matching and annotation-based query from a variety of multi-keyword notions (Weighted query). As a starting point, we suggest an annotation-based query and safe inner data processing. In addition, the k-nearest neighbour method yields good ranking results.

3. METHODOLOGY

Using the second and third forms of data, we devise a safe and effective way to search for information. To make things easier to understand, here is some background information. We begin by assuming that every product in the firm has a unique identification and a description file. Design flow, standard design, features and market position are all included in this file. If the product is launched sooner than its competitors, the firm will be able to occupy a larger market share and gain a significant advantage over its rivals. Because the items are time-sensitive, all of the information should be concealed from rivals and the general public. Product information expands in tandem with the company's expansion.

Moving a local data management system to the cloud is a simple way to increase a storage system's stability and durability. Because of its extensive capabilities, cloud computing is largely regarded as a potential IT infrastructure. Because it has the ability to rearrange a vast amount of storage, compute, and application resources, it enables consumers to receive IT services in an on-demand and flexible way. An further difficulty is how to keep the data private while yet making it searchable.

An encrypted product information retrieval system is designed in this study. This system contains two index structures: an IDAVL tree, which has a hash value index tree, and a PRF tree, which has a height-balanced index tree. Two data search techniques are offered based on the two index trees, namely the identifier or feature vector search by the data users of the desired product. The ID-AVL tree may be immediately outsourced to the cloud since the hash values of the product IDs are used instead of the plaintext data. Meanwhile, the plaintext data components in the PRF tree are encrypted using the safe kNN method before being outsourced. An extensive depth-first product search method for the PRF tree is also devised. The results of the simulations reveal that the recommended strategy is both successful and efficient.

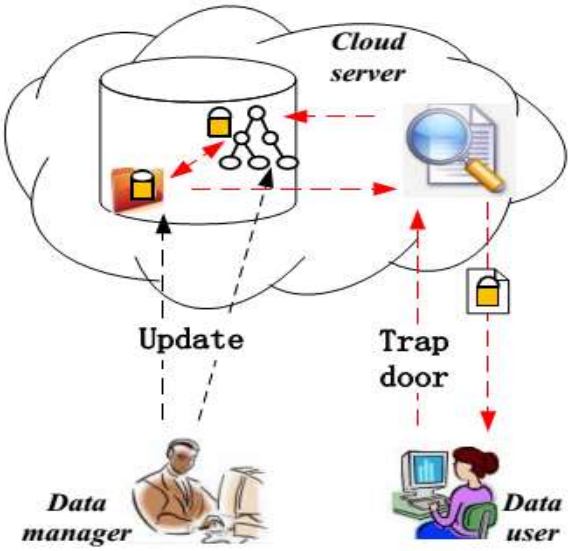

Fig. 1. Encrypted product information retrieval system model

The data manager, the cloud server, and the data user form the core of the product retrieval system paradigm. Following is a breakdown of the key tasks of each of these three organisations.

Data manager: It is the job of the data manager to keep track of the product and its data. Before sending the data to the cloud server, the data manager must also use symmetric encryption to secure the product information file.

Data user: Decrypting the returned files using the symmetric secret keys gives the data user access to the plaintext files. The data manager provides these secret codes.

Cloud server: The data manager's uploads are stored on the cloud server. An initial trapdoor is generated by a user who wants to explore cloud data. This is then submitted to the server. The cloud server employs a search engineer to serve as a conduit between the encrypted data and the data consumers.

4. EVALUATION OF THE CLASSIFICATION EXPERIMENT

Here, The data owner is person who is responsible for all information regarding the data that is stored in the cloud server. Data owner upload the data to cloud server and the Data users will search the related data by identifier based and Product based type of searches.

The data user is the person only view the type of data that is provided by the data owner. Here, a similarity matches score that is given about the accuracy of the search value that is given by the user.

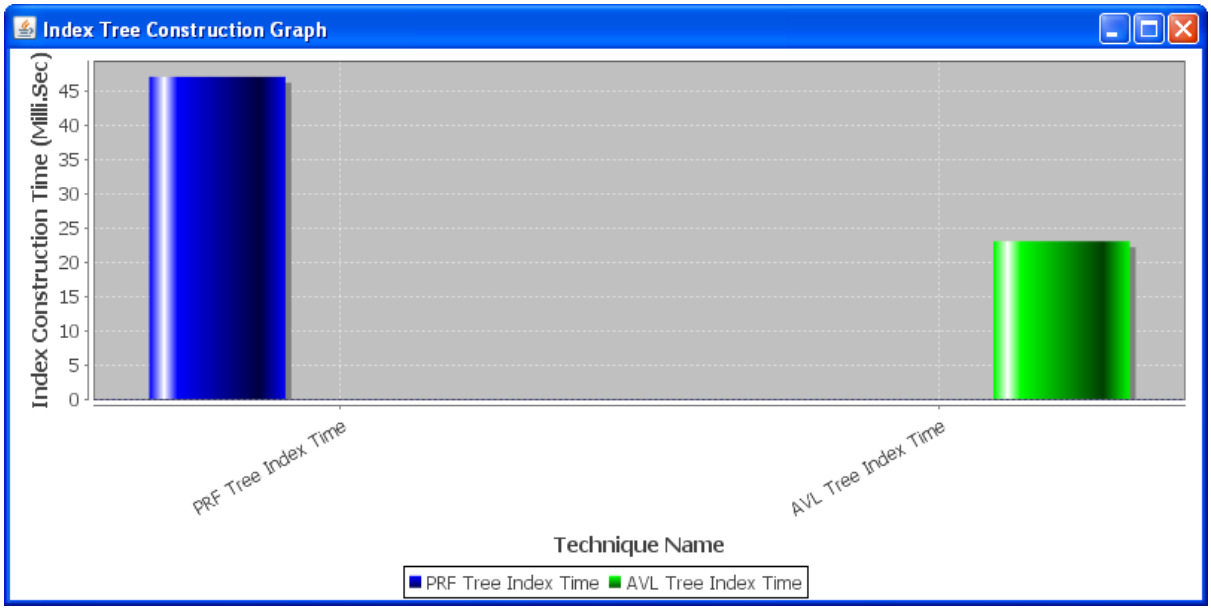

Fig. 2. Index Tree Construction Graph

Index construction time in milliseconds is shown on the x-axis of the above graph, which shows 'PRF tree Index time and AVL tree Index time'.

5. CONCLUSIONS

In this work, we provide a cloud-based system for retrieving product information that is both safe and fast. A hash value AVL tree, which supports identifier-based product search, and a

product vector retrieval tree for feature-vector-based product search, are created. In order to search the two trees, two different search algorithms have been developed. All outsourced data is encrypted in order to safeguard the privacy of product information. A set of separate secret keys is used to encode the product information, and the product vectors are encrypted using the safe kNN technique. The suggested scheme's security and efficiency are shown via security analysis and simulation results.

REFERENCES

[1] www.100EC.cn. 2016 Monitoring Report on the Data of China's Ecommerce Market [EB/OL]. http://www.100ec.cn/zt/16jcbg/,2017- 05-24
[2] Amazon. Amazon S3. http://aws.amazon.com/s3/
[3] Windows azure. http://www.microsoft.com/windowsazure/
[4] Apple i Cloud. http://www.icloud.com/
[5] Google App Engine. http://appengine.google.com/
[6] Golle P.Staddon J,Waters B. Secure Conjunctive Keyword Search over Data[C]. Springer, 2004.
[7] Song D X,Wanger D.Perrig A. Practical Techniques for Searched on Encrypted Data[C].IEEE,2000.
[8] Boneh D,Di Crescenzo G,Ostrovsky R. et al. Public Key Encryption with Keyword Search: EUROCRYPT[C].Springer,2004.
[9] Rhee H S.Park J K,Susilo W. et al. Trapdoor Security in A Searchable Public-Key Encryption Scheme with A Designated Tester[J].Journal of Systems and Software,2010,83(5):763-771
[10] Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." IEEE Internet Computing 16.1 (2012): 69-73.
[11] Song, Dawn Xiaoding, David Wagner, and Adrian Perrig. "Practical techniques for searches on encrypted data." Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000.
[12] Goh, Eu-Jin. "Secure indexes." IACR Cryptology ePrint Archive 2003 (2003): 216.
[13] Curtmola, Reza, et al. "Searchable symmetric encryption: improved definitions and efficient constructions." Journal of Computer Security 19.5 (2011): 895-934.
[14] Swaminathan, Ashwin, et al. "Confidentiality-preserving rankordered search." Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007.
[15] Wang, Cong, et al. "Enabling secure and efficient ranked keyword search over outsourced cloud data." IEEE Transactions on parallel and distributed systems 23.8 (2012): 1467-1479.
[16] Zerr, Sergej, et al. "Zerber+ r: Top-k retrieval from a confidential index." Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009.
[17] Jarecki, Stanislaw, et al. "Outsourced symmetric private information retrieval." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.
[18] Chang, Yan-Cheng, and Michael Mitzenmacher. "Privacy preserving keyword searches on remote encrypted data." International Conference on Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2005.
[19] Wang, Cong, et al. "Secure ranked keyword search over encrypted cloud data." Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010.

[20] Boneh, Dan, et al. "Public key encryption with keyword search." International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2004.

