A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage & Detect Malicious user

Prof. Vishal Walunj, Yasir Abulkalam Mulla, Aniket Navnath Sabale, Akshay Pratap Deshmukh
Computer Engineering ,DY Patil School of Engineering Ambi, Talegaon Pune.

Abstract:
Temporary keyword search on confidential data in a cloud environment is the main focus of this research. The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form. In the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. These search tokens can be used to extract all the ciphertexts which are produced at any time and contain the corresponding keyword. Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the ciphertexts generated in a specified time interval. To this end, in this paper, we introduce a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property. To evaluate the security of our scheme, we formally prove that our proposed scheme achieves the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA) both in the random oracle model and under the hardness of Decisional Bilinear Diffie-Hellman (DBDH) assumption. Furthermore, we show that the complexity of the encryption algorithm is linear with respect to the number of the involved attributes. Performance evaluation shows our scheme's practicality.

Introduction:

In, cloud computing plays an important role in our daily life, because it provides efficient, reliable and scalable resources for data storage and computational activities at a very low price. However, the direct access of the cloud to the sensitive information of its users threatens their privacy. A trivial solution to address this problem is encrypting data before outsourcing it to the cloud. However, searching on the encrypted data is very difficult. Public key encryption with keyword search (PEKS) is a cryptographic primitive which was first introduced by Boneh et al. [1] to facilitate searching on the encrypted data. In PEKS, each data owner who knows the public key of the intended data user generates a searchable cipher text by means of his/her public key, and outsources it to the cloud. Then, the data user extracts a search token related to an arbitrary keyword by using his/her secret key, and issues it to the cloud. The cloud service provider (CSP) runs the search operation by using the received search token on behalf of the data user to find the relevant results to the intended keywords. Zheng et al. [2] introduced the notion of attribute-based keyword

search (ABKS) to allow a data owner to control the access of data users for searching on his/her outsourced encrypted data. They used attribute-based encryption (ABE) [3] to construct a searchable cryptographic primitive in the multi-sender/multi receiver model. In their work, the legitimate data users can enlist the cloud to run the search operation on behalf of them without requiring any interaction with the data owner. In a secure ABKS scheme, a data owner cannot obtain any information about the keywords which the data users intend to look for. However, in all of the PEKS and ABKS schemes, once the cloud receives a valid search token related to a certain keyword, the cloud can investigate the keyword's presence in the past and any future cipher text. So, if the adversary realizes the corresponding keyword of the target search token, then she will be able to get some information about the next

documents which will be outsourced to the cloud. Therefore, it will be more secure to limit the time period in which the search token can be used.

Motivated by this problem, Abdalla et al. [4] introduced the notion of public key encryption with temporary keyword search (PETKS) which restricts the validation of the token to a certain time period. They applied anonymous identity-based encryption [5] in their generic scheme. In addition, Yu et al. proposed another public key searchable encryption in the context of temporary keyword search. Despite the good features of their schemes, these schemes do not provide the facility for data owners to enforce their intended access policy. In this paper, we propose a novel notion of Key-Policy Attribute-Based Temporary Keyword Search (KP-ABTKS). In KP-ABTKS schemes, the data owner generates a searchable ciphertext related to a keyword and the time of encrypting according to an intended access control policy, and outsources it to the cloud. After that, each authorized data user selects an arbitrary time interval and generates a search token for the intended keyword to find the ciphertext. Then, he/she sends the generated token to the cloud to run the search operation. By receiving the token, the cloud looks for the documents contain the intended keyword. The search result on a cipher text is positive, if (i) the data user's attributes satisfies the access control policy, (ii) the time interval of the search token encompasses the time of encrypting, and (iii) the search token and the cipher text are related to the same keyword. To show that the proposed notion can be realized, we also propose a concrete instantiation for this new cryptographic primitive based on bilinear map.

LITERATURE SURVEY

Paper Name: Public Key Encryption with keyword Search

Author Name: Dan Boneh Giovanni, Di Crescenzo, Rafail Ostrovsky

Descriptions: Suppose user Alice wishes to read her email on a number of devices: laptop, desktop, pager, etc. Alice's mail gateway is supposed to route email to the appropriate device based on the keywords in the email. For example, when Bob sends email with the keyword "urgent" the mail is routed to Alice's pager. When Bob sends email with the keyword "lunch" the mail is routed to Alice's desktop for reading later. One expects each email to contain a small number of keywords. For example, all words on the subject line as well as the sender's email address could be used as keywords. The mobile people project [24] provides this email processing capability. Now, suppose Bob sends encrypted email to Alice using Alice's public key. Both the contents of the email and the keywords are encrypted. In this case the mail gateway cannot see the keywords and hence cannot make routing decisions. As a result, the mobile people project is unable to process secure email without violating user privacy. Our goal is to enable Alice to give the gateway the ability to test whether "urgent" is a keyword in the email, but the gateway should learn nothing else about the email. More generally, Alice should be able to specify a few keywords that the mail gateway can search for, but learn nothing else about incoming mail. We give precise definitions in section

Paper Name: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data

Author Name: Qingji Zheng, Shouhuai Xu , Giuseppe Ateniese

Descriptions: Cloud computing allows data owners to use massive data storage and vast computation capabilities at a very low price. Despite the benefits, data outsourcing deprives data owners of direct control over their outsourced data. To alleviate concerns, data owners should encrypt their data before outsourcing to the cloud. However, encryption can hinder some useful functions such as searching over the outsourced encrypted data while enforcing an access control policy. Moreover, it is natural to outsource the search operations to the cloud, while keeping the outsourced data private. There is a need to allow the data users to verify whether the cloud faithfully executed the search operations or not. To the best of our knowledge, existing solutions

cannot achieve these objectives simultaneously and Our Contributions We propose a novel cryptographic primitive, called verifiable attribute-based keyword search (VABKS). This primitive allows a data owner to control the search, and use of, its outsourced encrypted data according to an access control policy, while allowing the legitimate data users to outsource the (often costly) search operations to the cloud and verify whether or not the cloud has faithfully executed the search operations. In other words, a data user with proper credentials (corresponding to a data owner's access control policy) can

(i) search over the data owner's outsourced encrypted data,

(ii) outsource the search operations to the cloud, and

(iii)verify whether or not the cloud has faithfully executed the search operations. We formally define the security properties of VABKS and present a scheme that provably satisfies them. The scheme is constructed in a modular fashion, by using attribute-based encryption, bloom filter, digital signature, and a new building-block we call attribute-based keyword search (ABKS) that may be of independent value. Experimental evaluation shows that the VABKS solutions are practical. B. Related Work To the best of our knowledge, no existing solution is adequate for what we want to achieve. In what follows we briefly review the relevant techniques.

Paper Name: Towards Privacy-Preserving Storage and Retrieval in Multiple Clouds

Author Name: Jingwei Li, Dan Lin, Anna Squicciarini, Jin Li and Chunfu Jia

Descriptions: —Cloud computing is growing exponentially, whereby there are now hundreds of cloud service providers (CSPs) of various sizes. While the cloud consumers may enjoy cheaper data storage and computation offered in this multi-cloud environment, they are also in face of more complicated reliability issues and privacy preservation problems of their outsourced data. Though searchable encryption allows users to encrypt their stored data while preserving some search capabilities, few efforts have sought to consider the reliability of the searchable encrypted data outsourced to the clouds. In this paper, we propose a privacy-preserving Storage and Retrieval (STRE) mechanism that not only ensures security and privacy but also provides reliability guarantees for the outsourced searchable encrypted data. The STRE mechanism enables the cloud users to distribute and search their encrypted data across multiple independent clouds managed by different CSPs, and is robust even when a certain number of CSPs crash. Besides the reliability, STRE also offers the benefit of partially hidden search pattern. We evaluate the STRE mechanism on Amazon EC2 using a real world dataset and the results demonstrate both effectiveness and efficiency of our approach.

Paper Name: An Efficient Search Scheme over Encrypted Data on Mobile Cloud

Author Name: Jian Li, Member IEEE/ACM, Ruhui Ma, Haibing Guan

Descriptions: Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. In this paper, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval, meanwhile the network traffics during

the file retrievals are also significantly reduced.

Paper Name: Identity-Based Private Matching over Outsourced Encrypted Datasets
Author Name: Shuo Qiu, Jiqiang Liu, Yanfeng Shi, Ming L
Descriptions: With wide use of cloud computing and storage services, sensitive information is increasingly centralized into the cloud to reduce the management costs, which raises concerns about data privacy. Encryption is a promising way to maintain the confidentiality of outsourced sensitive data, but it makes effective data utilization to be a very challenging task. In this paper, we focus on the problem of private matching over outsourced encrypted datasets in identity-based cryptosystem that can simplify the certificate management. To solve this problem, we propose an Identity-Based Private Matching scheme (IBPM), which realizes fine-grained authorization that enables the privileged cloud server to perform private matching operations without leaking any private data. We present the rigorous security proof under the Decisional Linear Assumption and Decisional Bilinear Diffie-Hellman Assumption. Furthermore, through the analysis of the asymptotic complexity and the experimental evaluation, we verify that the cost of our IBPM scheme is linear to the size of the dataset and it is more efficient than the existing work of Zheng [30]. Finally, we apply our IBPM scheme to build two efficient schemes, including identity-based fuzzy private matching as well as identity-based multi-keyword fuzzy search.

Problem statement:

We develop an application that has data owners, users, TTP and cloud server. The Data owner registers and send activation request to TTP. TTP activate account of owner and send OTP to data owners mobile number. Owner now login to the system. upload file with time server and keywords and encrypt using AES and ND5 algorithm respectively. owners also view and download les. Users register and send activation request to TTP. TTP activate users account and send OTP to mobile number. User search file using Keywords. Get file from cloud rank wise and view files, then he request to data owner to send key. data owner send key response with time server that means specific time limit are set for download image from cloud. Here we use time server by two ways first is set time server for le , that means when time limit ends then cloud automatically delete file from the cloud. and second way is user download time using key and for that key owner set time for downloading. Advantage of proposed System

• It achieves the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA)
• The search tokens can only extract the cipher texts generated in a specified time interval so leakage is not possible.
• To store the data in Encryption Format.

Existing system:

In existing the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. These search tokens can be used to extract all the cipher text which are produced at any time and contain the corresponding keyword. Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the ciphertexts generated in a specified time interval. However, in all of the PEKS and ABKS schemes, once the cloud receives a valid search token related to a certain keyword, the cloud can investigate the keyword's presence in the past and any future ciphertext. So, if the adversary realizes the corresponding keyword of the target search token, then she will be able to get some information about the next documents which will be outsourced to the cloud.

Proposed system:

In this project YOLO (You Only Look Once) object detection system which uses convolution neural networks for object detection. It is one of the faster algorithms that performs without much degradation in accuracy.

The proposed experiment employs You Only Look Once (YOLO) v3 model, which is a deep learning framework based on Darknet, an open-

source neural network in C. YOLOv3 is the best choice as it provides real-time detection without losing too much accuracy. The architecture used is darknet53 which consists of 53 convolutional layers each followed by Leaky ReLu activation and batch normalization layers, making it a fully convolutional network (FCN).

Advantages:

Real-time frame-based efficient fire and gun detection deep learning model has been presented with a high accuracy metric.

The Darknet53 model might be bulky but has a good detection capability. The detections per frame are appropriate for real-time monitoring and can be deployed on any GPU based system.

System Architecture Diagram:

CLOUD techniques make it possible to utilize information technology resources into business domain. The cloud provides variety of scalable services on-demand, such as online databases, program interface, storage and computing resources, etc. Users can obtain services through phones, laptops, and desktops as shown in Fig. 1. Cloud storage provides remote data storage and management services. It is also helpful in data analyzing and computing, which is quite simple as it can provide a variety of services at the same time. Cloud has many advantages in data storage, such as decreasing communication cost and maintenance charge, saving resources, allowing remote access, and so on. However, people might not be willing to store

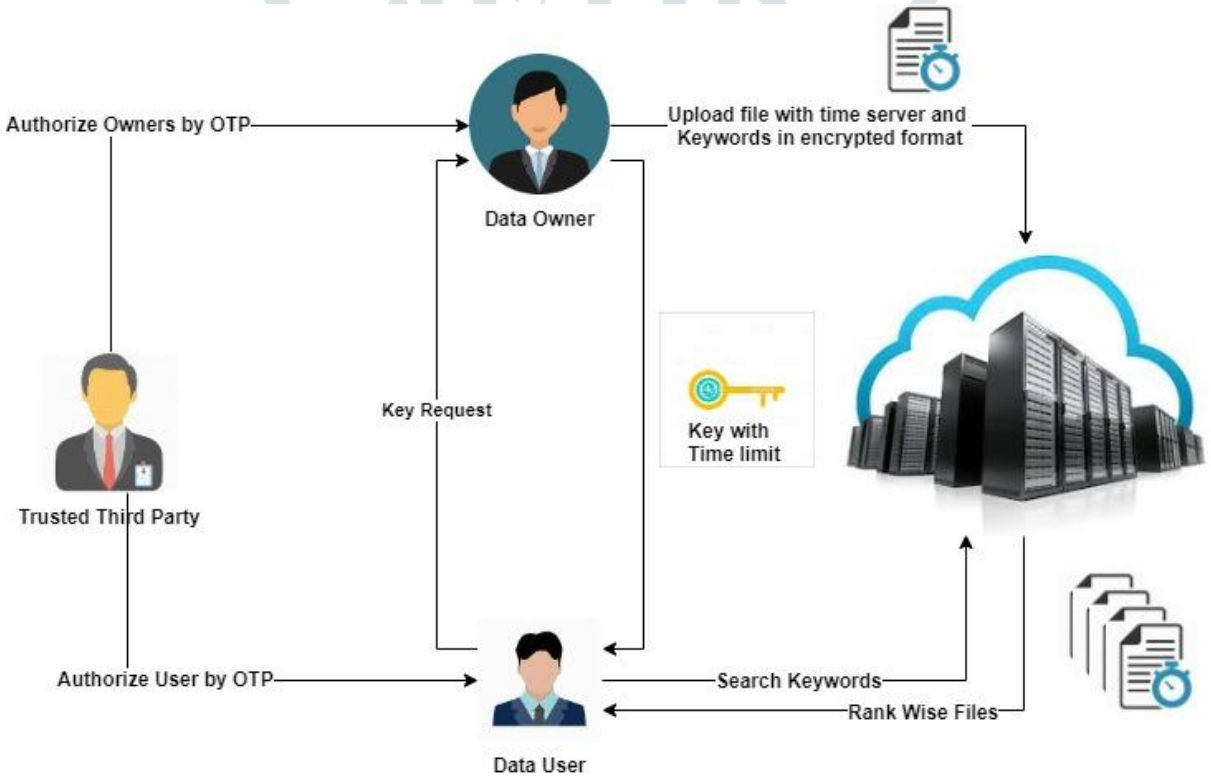

Figure: System Architecture

Their data in the cloud, even though it provides so many benefits because of the data confidentiality and privacy problems. The cloud server (CS) may be untrusted, in other words, if data is uploaded to cloud, the cloud service provider may obtain and disclose users' personal privacy, and even access and share the data illegally

CONCLUSION

Securing cloud storage is an important problem in cloud computing. We addressed this issue and introduced the notion of Sharing Data Based On Attribute matching And Temporary Keyword Search on cloud. According to our scheme, each data owner can generate a secret key which is valid only for a limited time interval for downloading. View Files Rank wise to the users.

REFERENCES

[1] Mohammad Hassan Ameri, Mahshid Delavar, Javad Mohajeri, Mahmoud Salmasizadeh, "A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage", IEEE Transactions on Cloud Computing, 2168-7161 (c) 2018 IEEE

[2] A. Awad, A. Matthews, Y. Qiao, and B. Lee, "Chaotic searchable encryption for mobile cloud storage," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[3] J. Li, D. Lin, A. C. Squicciarini, J. Li, and C. Jia, "Towards privacypreserving storage and retrieval in multiple clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 499–509, July 2017.

[4] J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 126–139, Jan 2017.

[5] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, "Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[6] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi keyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, 2016.

[7] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.

[9] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[10] A. Awad, A. Matthews, Y. Qiao, and B. Lee, "Chaotic searchable encryption for mobile cloud storage," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[11] J. Li, D. Lin, A. C. Squicciarini, J. Li, and C. Jia, "Towards privacy preserving storage and retrieval in multiple clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 499–509, July 2017.

[12] J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 126–139, Jan 2017.

[13] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM journal on computing, vol. 32, no. 3, pp. 586–615, 2003.

[14] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in International Conference on Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.