e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

A-KEY POLICY ATTRIBUTE BASED TEMPORARY KEYWORD SEARCH SCHEME FOR SECURE CLOUD STORAGE

Gayathri S*1

*1Student, Computer Science Engineering, AVS Engineering College,

Salem, Tamil Nadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS45065

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.

I. INTRODUCTION

TODAY, 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 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 ciphertext 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 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) 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.

II. METHODOLOGY

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

VABKS: Verifiable attribute-based keyword search over outsourced encrypted data

It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS).

Fuzzy Identity Based Encryption

We introduce a new type of Identity Based Encryption (IBE) scheme that we call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a ciphertext encrypted with another identity id if and only if the identities id an did are close to each other as measured by some metric (eg. Hamming distance). A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement. In this paper we present a construction of a Fuzzy IBE scheme that uses groups with efficiently computable bilinear maps. Additionally, our construction does not use Random Oracles. We prove the security of our scheme under the Selective-ID security model.

III. MODELING AND ANALYSIS

The software requirement specification is produced at the culmination of the analysis task. The function and performance allocated to software as part of system engineering are refined by establishing a complete information description as functional representation, a representation of system behavior, an indication of performance requirements and design constraints, appropriate validation criteria.

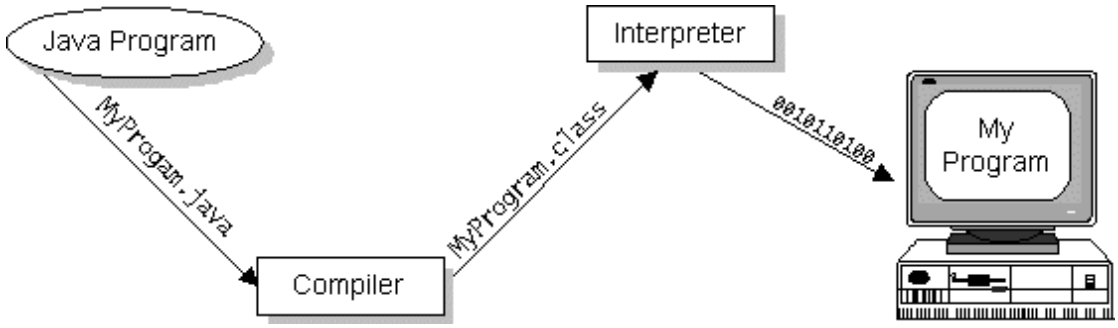

Figure 1: JAVA

A platform is the hardware or software environment in which a program runs. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other, hardware-based platforms. Most other platforms are described as a combination of hardware and operating system.

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries (*packages*) of related components.

The following figure depicts a Java program, such as an application or applet, that's running on the Java platform. As the figure shows, the Java API and Virtual Machine insulates the Java program from hardware dependencies.

IV. RESULTS AND DISCUSSION

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

V. CONCLUSION

Securing cloud storage is an important problem in cloud computing. We addressed this issue and introduced the notion of key-policy attribute-based temporary keyword search (KPABTKS). According to this notion, each data user can generate a search token which is valid only for a limited time interval. We proposed the first concrete construction for this new cryptographic primitive based on bilinear map. We formally showed that our scheme is provably secure in the random oracle model. The complexity of encryption algorithm of our proposal

is linear with respect to the number of the involved attributes. In addition, the number of required pairing in the search algorithms is independent of the number of the intended time units specified in the search token and it is linear with respect to the number of attributes. Performance evaluation of our scheme in term of both computational cost and execution time shows the practical aspects of the proposed scheme.

VI. REFERENCES

[1] Y. Yu, J. Ni, H. Yang, Y. Mu, and W. Susilo, "Efficient public key encryption with revocable keyword search," Security and Communication Networks, vol. 7, no. 2, pp. 466–472, 2014.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings.2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[3] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol.2003, p. 216, 2003.

[4] 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.