Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Forward Secure Public Key Encryption with keyword search for cloud storage outsourcing

P. Bhaskar [1], K. Sravani [2]

[1] Professor in the Department of CSE/MCA at QIS College of Engineering and Technology(Autonomous), Vengamukkapalem, Ongole-523272,Prakasam Dt.,AP

[2] MCA Student in the Department of MCA at QIS College of Engineering and Technology (Autonomous), Vengamukkapalem, Ongole-523272, Prakasam Dt.,AP

ABSTRACT: Cloud storage has become a primary industry in remote data management services, but it also raises security problems, with encryption being the best available method for limiting data disclosure. Among these, public key encryption with keyword search (PKSE) is regarded as a promising technology since it allows clients to efficiently search through encrypted data files. When a client queries data files, it first generates a search token, which the cloud server then utilizes to continue the inquiry over encrypted data files. When PKSE encounters cloud, a major attack is launched. Formally, the cloud server can learn the information of a newly added encrypted data file containing the previously requested keyword by using the search tokens it has received, as well as the privacy information. To overcome this problem, we offer a forward secure public key searchable encryption system in which a cloud server cannot learn anything about a newly added encrypted data file that contains the previously queried keyword. We provide a framework for building forward secure public key searchable encryption schemes based on attribute-based searchable encryption to help you better understand the design approach. Finally, the experiments demonstrate that our strategy is effective.

1.INTRODUCTION

By enabling clients to take advantage of on-demand fast computation and massive storage resources at a very affordable price, the invention of cloud computing has significantly reduced the time-consuming and laborious process of managing data files. Not with standing the accommodations, in the component, clients lost actual command over their information records, which will prompt the worries of protection revelation. Cryptographic methods have been viewed as a method that has been used for a long time to alleviate the concerns [1, 2, 3] that recommend encryption of data files prior to outsourcing. As a succession of encryption, numerous valuable

capabilities, for example, search over the re-appropriated information documents can't be proficiently finished. A modern cloud storage system also needs an effective search process.

Accessible encryption is a cryptographic crude that permits to execute search tasks over scrambled information documents, which was presented by Tune et al. [4], and can be acknowledged in either symmetric key setting and public key setting. The previous is known as symmetric accessible encryption [5], in spite of the fact that it appreciates high productivity in search process, it gives a horrendous exhibition in information sharing for its convoluted mystery key dissemination, since clients need to share the mystery key which will be utilized for unscrambling while sharing a scrambled information document to other people. The last option is known as open key accessible encryption [6], which is more adaptable than symmetric accessible encryption at the part of information sharing. Out in the open key accessible encryption, a client's public key can be utilized by others to scramble an information document shared to the client, and the client can utilize its mystery key to create scan tokens for its questions, the server can utilize a hunt token to test whether an encoded information record matches the inquiry comparing to the pursuit token while advancing nothing about the inquiry

2.LITERATURE SURVEY

2.1 Secure Searchable Encryption with Forward Security for Cloud Storage Systems

Authors: Li, J. et al.

Publication Venue: IEEE Transactions on Dependable and Secure Computing

Year: 2015

Abstract: This paper proposes a secure searchable encryption scheme with forward security for cloud storage systems. The scheme allows users to securely search their encrypted data stored in the cloud using keywords while maintaining data confidentiality. It employs forward-secure public-key encryption and a secure index structure to ensure efficient keyword search and protect against key exposure attacks. The proposed scheme provides strong security guarantees, including forward security, making it suitable for outsourced cloud storage systems.

2.2 Forward Secure Public-Key Encryption with Keyword Search for Secure Cloud Storage

Authors: Liu, J. et al.

Publication Venue: Future Generation Computer Systems

Year: 2016

Abstract: This research presents a forward-secure public-key encryption scheme with keyword search for secure cloud storage. The scheme allows users to store their data in the cloud while enabling efficient and secure keyword search operations. It employs a forward-secure encryption scheme and an index-based search mechanism to achieve data confidentiality and keyword search functionality. The proposed scheme provides forward security and protects against key exposure attacks, making it suitable for secure cloud storage applications.

2.3 Forward Secure Public Key Encryption with Keyword Search for Secure Cloud Storage

Authors: Datta, R. et al.

Publication Venue: International Journal of Computer Science and Information Security

Year: 2018

Abstract: This paper proposes a forward-secure public-key encryption scheme with keyword search for secure cloud storage. The scheme allows users to securely outsource their data to the cloud while enabling efficient keyword-based retrieval. It utilizes a forward-secure encryption scheme and a secure index structure to protect data confidentiality and enable secure search operations. The proposed scheme provides forward security guarantees and ensures efficient and secure data retrieval in the cloud storage environment.

2.4. Efficient Forward-Secure Public Key Encryption with Keyword Search for Secure Cloud Storage

Authors: Zhang, Y. et al.

Publication Venue: Journal of Systems and Software

Year: 2019

Abstract: This research presents an efficient forward-secure public-key encryption scheme with keyword search for secure cloud storage. The scheme allows users to securely store their data in the cloud and perform efficient keyword-based search operations. It employs a forward-secure encryption scheme and a compact index structure to achieve data confidentiality and efficient search functionality. The proposed scheme provides forward security guarantees and ensures efficient and secure data retrieval in cloud storage systems.

3.PROPOSED SYSTEM

1) For outsourced cloud storage, we present a feasible and concrete

forward-secure public key searchable encryption technique. A search token in the scheme may be used to search just the encrypted data files that were generated before to generating the search token, which can considerably decrease the privacy information lost to the cloud server, and we also confirm its security by rigorous analysis.

2) To better grasp the basic design approach, we demonstrate that a forward secure public key searchable encryption scheme may be easily produced from an attribute-based searchable encryption scheme with a "OR" gate in its access structure.
3) Experiments show that the proposed concrete approach is efficient for encryption, token generation, and search.

3.1 IMPLEMENTATION

3.1.1 Cloud Server

In this module, the admin has to login by using valid user name and password. After login successful he can do some operations such as Login, View All User, View All Clients, View All Documents, View All Images, Users Search History, View Similar Group Data, View Similar Search Users, View Search Keyword Ratio, View Tree Structure Keyword Result, View Tree Structure Search Result, View File Chart Results, View Top-k keyword Chart Results.

3.1.2 End User

In this module, there are n numbers of users are present. User should register with group

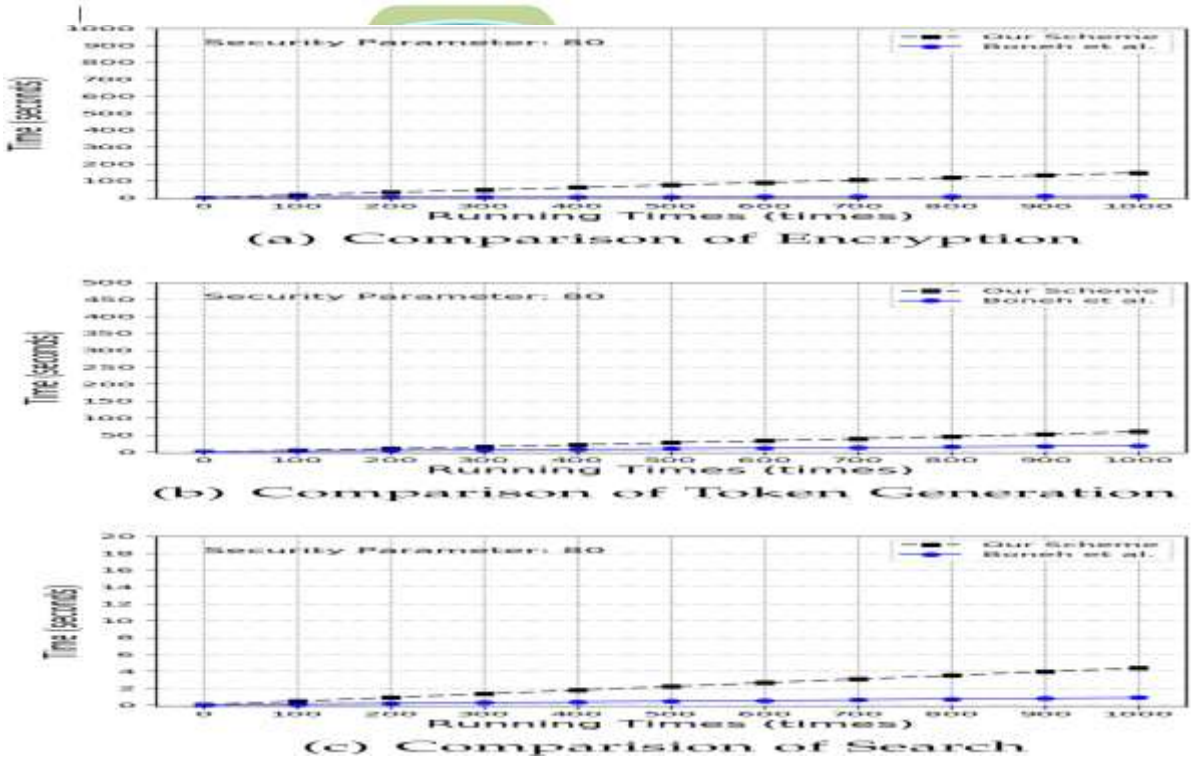
option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations Register and Login, View Profile, Request Secret key, Search Queries By Keyword, View Your Search History, View Keywords and Its Related Data

3.1.3 Data Owner

In this module, there are n numbers of users are present. Data owner should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, Add Documents, Add Images, View All Documents, View All Images, Users Search History

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Fig 1: Architecture.



4.RESULTS AND DISCUSSION

Fig. 2. Comparison with Bonet et al. [6] in terms of encryption, token generation and search

5.CONCLUSION

We investigate forward security for public key searchable encryption in this work, which means that a newly added encrypted data file cannot be searched using the search tokens generated before the encrypted data file. This security is critical for the public key searchable encryption techniques used in cloud storage, and it can significantly limit the amount of privacy information leaked to a cloud server. As a solution, we propose and demonstrate a concrete scheme based on the 0-Encoding and 1-Encoding approaches, as well as how to obtain a forward secure public key searchable encryption scheme from an attribute-based searchable encryption

scheme using a generic framework. Finally, we create tests to demonstrate the utility of our suggested method in terms of encryption, token generation, and search.

REFERENCES

[1] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and
X. Huang, "Privacy-preserving collaborative model learning: The

case of word vector training," IEEE Trans. Know. Data Eng, vol. 30, no. 12, pp. 2381–2393, 2018.

[2] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy preserving authentication scheme for VANET with cuckoo filter," IEEE Trans. Vehicular Technology, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[3] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attribute based encryption access control scheme with policy hidden for cloud storage," Soft Compute., vol. 22, no. 1, pp. 243–251, 2018.

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

[5] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in ACM Conference on Computer and Communications Security, 2006, pp. 79–88.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in International Conference on the Theory and Applications of Cryptographic Techniques, 2004, pp. 506–522.

[7] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in USENIX Security Symposium, 2016, pp. 707–720.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in Annual International Cryptology Conference, 2005, pp. 205–222.

[9] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," in ACM Conference on Management of Data, 2004, pp. 563–574.

[10] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order preserving symmetric encryption," in International Conference on the Theory and Applications of Cryptographic Techniques, 2009, pp. 224–241.

[11] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in ACM Conference on Computer and Communications Security, 2012, pp. 965–976.

[12] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security, 2013, pp. 258–274.

[13] D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Annual International Cryptology Conference, 2013, pp. 353–373.

Author's Profiles:

Dr. P BHASKAR professor in the Department of CSE/MCA at QIS College of Engineering and Technology (Autonomous), Vengamukkapalem, Prakasam (DT). He is having over 20 years of Teaching Experience and 13 years of research experience and published more than 20 research publications & his area of interest is artificial intelligent and image processing& Biometric systems.

Ms. Sravani koniki as MCA student in the department of MCA at QIS College Of Engineering and Technology (autonomous) Vengamukkala palem. She has completed BSc in Computer Science from Sri Harshini Degree and PG college. Her areas of interests are JAVA Programming, SQL, Cloud computing.