A PARALLEL AND FORWARD PRIVATE SEARCHABLE PUBLIC KEY ENCRYPTION FOR CLOUD BASED DATA SHARING

KUNTAPALLI JAYACHANDRAREDDY[1], S.V.S. GANGA DEVI[2]

PG Research Scholar, Dept. of Computer Applications, Madanapalle Institute of Technology and Science
Professor, Dept. of Computer Applications, Madanapalle Institute of Technology and Science, Andhra Pradesh, India

---

ABSTRACT

With the advancement of cloud computing technologies, data exchange over the cloud is becoming more common. New technology bring new security concerns, particularly when it comes to data privacy in cloud-based sharing services. One of the finest way for balancing data privacy and usability is searchable encryption. Due to the lack of some essential features such as parallel search and forward security, most existing searchable encryption systems do not match the requirements for both high search capacity and robust security at the same time. To address this issue, we propose parallel and forward private searchable public-key encryption as a variation searchable encryption with parallel and forward privacy (PFP-SPE). At the tradeoff of slightly increased storage costs, the PFP-SPE system accomplishes both parallelism and forward privacy. PFP-SPE provides a similar search functionality to various other programmes.

Keywords: *Security ,Encryption ,Decryption ,Data sharing.*

1. INTRODUCTION

Cloud-based data sharing has emerged as a viable alternative for easy access to massive amounts of data on demand. Its multiple advantages, such as cheaper costs, better resource utilisation, and higher agility, have industrial and academic interest. Cloud-based data sharing solutions are already in use across a wide range of industries, including education, logistics, healthcare, and finance. Diagram 1 depicts the traditional cloud-based data sharing application scenarios. However, as security issues (such as celebrity images being leaked in Cloud) continue to arise, people are becoming increasingly concerned about privacy protection while appreciating the convenience of cloud storage. To promote the widespread use of cloud-based data sharing, secure procedures balancing privacy and data consumption are urgently needed.

To promote the widespread use of cloud-based data sharing, secure procedures balancing privacy and data consumption are urgently needed.

2. LITERATURE SURVEY

The concept of Public-key Authenticated Encryption with Keyword Search (PAEKS) to address the problem of a data sender who not only encrypts but also authenticates a keyword so that a verifier is convinced that the encrypted keyword can only be generated by the sender. The authors present a concrete and efficient architecture of PAEKS and show its security under the stated security models using simple and static assumptions in the random oracle model [1]

The purpose of searchable encryption (SE) is to allow a client to search encrypted data on an untrusted server while maintaining some level of privacy for both the encrypted contents and the search queries. Recent research has concentrated on establishing effective SE techniques at the risk of allowing some minor, well-defined "(information) leakage" about files and/or queries to the server. However, the practical significance of this leakage is unknown. On the query privacy of single keyword and conjunctive SE schemes, the authors investigate file-injection attacks in which the server transmits files to the client, which the client subsequently encrypts and saves. they show that even with only a few injected files, such attacks can leak the client's requests [2].

The industrial Internet of Things is thriving, thanks to the extraordinary rapid growth of wireless sensor networks (WSNs) with cloud computing aid. New cyber security threats will emerge as a result of the new generation of technology, including data confidentiality in cloud-assisted WSNs (CWSNs). SPE (searchable public-key encryption) is a promising solution to this issue. In theory, sensors can post public-key cipher texts to the cloud, and its owners can safely delegate a keyword search to the cloud and obtain the desired data while retaining data secrecy. However, in terms of creating cipher texts and searching keywords, all existing and semantically safe SPE techniques have high costs. As a result, this research presents an LSPE (lightweight SPE) scheme[3].

3. PROPOSED METHOD

We present a version searchable encryption with parallel and forward privacy in the suggested system, namely parallel and forward private searchable public-key encryption with parallel and forward privacy (PFP-SPE). At the slightly increased storage costs, the PFP-SPE system accomplishes both parallelism and forward privacy.

4. System Architecture

Fig 1 shows the Architecture diagram. Admin login with the valid username and Password. After that he can add and view Categories, Products, Service Providers. While adding Service Providers the admin must give the location of the Service Providers. Admin can also have the access to view the feedback from the user about service provider and he can also block him. The user must be registered and login with their Email and Password. After logging, the user will select the Category and Service and send a query to the Service Provider. After the query is sent, the user will wait for the service provider solution and if he satisfies that is okay if not he can give feedback to admin. Service Provider login with their Email and Password. After logging, Servicer view the User queries or requests based on that he responds and provides a Solution to the User.

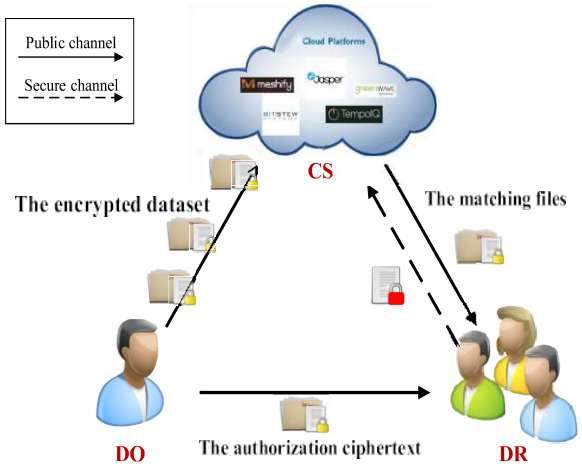

Fig 1. Architecture diagram

5. Result

During the research, the respondents were first presented with phrases regarding the perception of trust which allowed them to present their opinions on the meaning of this concept .The main aim of the this paper is the data owner send the data by using the cloud sharing. In this he will encrypt the data and the key code is given to the data receiver. The data receiver will decrypt the code and he/she will access the data.

6. CONCLUSION

We study a new architecture for a practical dynamic searchable encryption system that is both efficient and secure in this work. Fortunately, we also provide a realistic construction for a new cryptographic primitive, parallel and forward private searchable public-key encryption. The star-chain data structure in our scheme improves search efficiency and provides forward privacy. Our system is more suitable for practical application.

REFERENCES

[1] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," *Inf. Sci.*, vols. 403–404, pp. 1–14, Sep. 2017.

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

[3] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight search- able public-key encryption for cloud-assisted wireless sensor net- works," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3712–3723, Aug. 2018.

[4] H. Li, Q. Huang, J. Shen, G. Yang, and W. Susilo, "Designated-server identity-based authenticated encryption with keyword search for encrypted emails," *Inf. Sci.*, vol. 481, pp. 330–343, May 2019.

[5] R. Bost, "Σοφος forward secure searchable encryption," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 1143–1154.

[6] K. S. Kim, M. Kim, D. Lee, J. H. Park, and W.-H. Kim, "Forward secure dynamic searchable symmetric encryption with efficient updates," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2017, pp. 1449–1463.

[7] X. Song, C. Dong, D. Yuan, Q. Xu, and M. Zhao, "Forward private searchable symmetric encryption with optimized i/o efficiency," *IEEE Trans. Dependable Secure Comput.*, to be published.

[8] M. Ma, D. He, N. Kumar, K.-K.-R. Choo, and J. Chen, "Certifi- cateless searchable public key encryption scheme for industrial Inter- net of Things," *IEEE Trans. Ind. Inf.*, vol. 14, no. 2, pp. 759–767, Feb. 2018.

[9] L. Wu, B. Chen, K.-K.-R. Choo, and D. He, ‘‘Efficient and secure search- able encryption protocol for cloud-based Internet of Things,’’ *J. Parallel Distrib. Comput.*, vol. 111, pp. 152–161, Jan. 2018.

[10] M. Ma, D. He, H. Wang, N. Kumar, and K.-K.-R. Choo, ‘‘An effi- cient and provably secure authenticated key agreement protocol for fog- based vehicular ad-hoc networks,’’ *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, Oct. 2019.

[11] R. Bost and P.-A. Fouque, ‘‘Security-efficiency tradeoffs in searchable encryption,’’ *on Privacy Enhancing technol.*, vol. 2019, no. 4, pp. 132–151, Oct. 2019.

[12] L. Liu, J. Su, X. Liu, R. Chen, K. Huang, R. H. Deng, and X. Wang, ‘‘Toward highly secure yet efficient KNN classification scheme on out- sourced cloud data,’’ *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9841–9852,Dec. 2019.