LIGHTWEIGHT FINE-GRAINED SEARCH OVER ENCRYPTED DATA IN FOG COMPUTING

V. Priyadharshini,
Department of Computer Applications,
Krishnasamy College of Engineering and Technology, Cuddalore.

Mrs. R.Vijayalakshmi, MCA., M.Phil., (Ph.D),
Associate Professor,
Department of Computer Applications,
Krishnasamy College of Engineering and Technology, Cuddalore.

ABSTRACT:

Fog is another layer of a distributed network environment and is closely associated with cloud computing and the internet of things (IoT). Public infrastructure as a service (IaaS) cloud vendors can be thought of as a high-level, global endpoint for data; the edge of the network is where data from IoT devices is created.Fog computing can create low-latency network connections between devices and analytic endpoints.Both cloud computing and fog computing provide storage, applications, and data to end-users. However, fog computing is closer to end-users and has wider geographical distribution.

Fog computing, as an extension of cloud computing, outsources the encrypted sensitive data to multiple fog nodes on the edge of Internet of Things (IoT) to decrease latency and network congestion. However, the existing cipher text retrieval schemes rarely focus on the fog computing environment and most of them still impose high computational and storage overhead on resource-limited end users. In this paper, we first present a Lightweight Fine-Grained cipher text Search (LFGS) system in fog computing by extending Cipher text-Policy Attribute-Based Encryption (CP-ABE) and Searchable Encryption (SE) technologies, which can achieve fine-grained access control and keyword search simultaneously. The LFGS can shift partial computational and storage overhead from end users to chosen fog nodes. Furthermore, the basic LFGS system is improved to support conjunctive keyword search and attribute update to avoid returning irrelevant search results and illegal accesses. The formal security analysis shows that the LFGS system can resist Chosen-Keyword Attack (CKA) and Chosen-Plaintext Attack (CPA), and the simulation using a real-world dataset demonstrates that the LFGS system is efficient and feasible in practice.

INTRODUCTION:

The promising cloud computing paradigm can provide on-demand services with elastic resources and enable cloud clients to relieve the high storage and computation costs locally. However, the prevalence of Internet of Things (IoT) applications poses a huge challenge to the centralized cloud computing paradigm which incurs unbearable transmission latency and degraded services between user requests and cloud responses. Besides, large amounts of data generated from the IoT applications are often stored in the cloud. To decrease latency and network congestion, a fog computing paradigm which is an extension of cloud computing services to network edge has been a relatively recent research topic. In fog computing, the fog nodes inserted into the middle of cloud and end users (or IoT devices) can provide various services (i.e., data computation, data storage, etc.) for resource-limited end users (i.e., sensor nodes, mobile terminals, etc.), note that fog nodes are much closer to end users than cloud, When sensitive data (i.e., text, image, video, etc.), are outsourced to honest-but-curious fog nodes which are similar to public cloud platform, the data security and privacy concerns still impede

Fine-grained keyword search- LFGS system gains one-to-many rather than one-to-one encryption and specifies flexible access control over shared data, which eliminates some inherent drawbacks of

Lightweight computation on end users- With the help of fog nodes, LFGS system reliefs the large computational burden from data owners or end user's, which means that partial computation including files encryption, trapdoor generation and ciphertexts decryption is offloaded to fog nodes without any loss of data confidentiality.

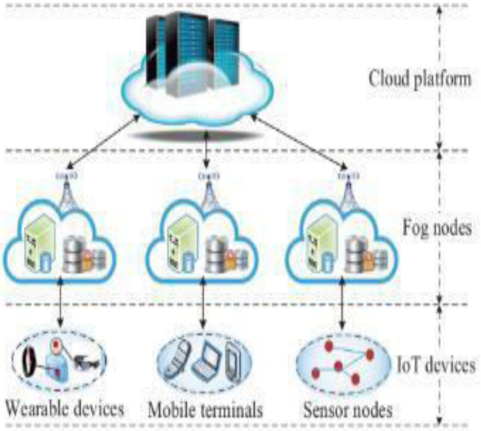
Attribute update- The extended LFGS system sup-ports attribute update and just needs to update the keys and ciphertexts associated with the updated at-tributes, which not only avoids illegal accesses using outdated keys but also imposes less computational overhead on this system.

Conjunctive keyword search-The extended LFGS system allows end users to issue multiple keywords in a single search query so that it can improve the user search experience as the conjunctive keyword search can narrow down the search scope and quickly locate the results of interest.

Security and practicability- Formal security shows that LFGS system is selectively secure against Chosen-Keyword Attack (CKA) and Chosen Plain- text Attack (CPA). The extensive experiments demonstrate that LFGS system is efficient and feasible in a broad range of applications.

the adoption of fog computing as data owners lose the physical control over their data in fog nodes or cloud.

existing public key cryptography schemes. Besides, LFGS system enables end users to search ciphertexts of interest according to queried keyword.



Infrastructure of fog computing

PROPOSED SYSTEM:

Lightweight Fine-Grained Search (LFGS) system for the resource-limited in fog computing. On the one hand, the basic LFGS system could greatly reduce the computational and storage burden of by outsourcing partial computation and storage to the honest-but-curious FNs without leaking sensitive information; on the other hand, the extended LFGS system could support conjunctive keyword search and attribute update to further narrow down the search scope and avoid unauthorized accesses, respectively.

Lightweight Fine-Grained Search over Encrypted Data in Fog Computing. Furthermore, the formal security analysis showed that the LFGS system is selectively secure against CKA and CPA, and the empirical experiments using a real-world dataset illustrated the efficiency and feasibility of LFGS system in fog computing.

MODULES

User authentication

This module used to create user authentication based on the user identity and sensitive data based the database created and the user can create security by login.

User's personal(sensitive data) details received through a registration process.

The data stored on the database when we login the username, password or key checked on the database if the details correct then the system allow for further.

Key generation

The proposed system basically focused on encryption and decryption the third party who create key for accessing the data on the server

In Cryptography the encryption of text (file or user details) encrypted by different types of technique and algorithm steps

The key act as part to encrypt or decrypt the data its like numbers,special characters, text based wordings, etc.

Fog mode

Fog computing extends the concept of cloud computing to the network edge, making it ideal for applications that require real-time interactions.

Fog is another layer of a distributed network environment and is closely associated with cloud computing

The process of service providing by the server through search engine, cloud the speed of data request and recieving service is important for reducing buffering on service provider.

Data on cloud

The data provider adding on the cloud by using the account after the authentication process

The data maintained on the cloud still access by the user and the data provider

Cloud is a online storage wherever and whenever can access those data by internet

In future overall applications possible to implement cloud to avoiding data thefting and data losing.

Accessing data

The user can getting data by the key which is created by the third party.

The accessing process based on the key generated by the third party. Who generating key without knowledge about the requester, data receiver and data provider.

It generate key random based on the instructions added into the algorithm

Which provide another step of security to accessing data from the cloud server.

Related work

In cloud computing environment, SE provides a fundamental solution to issue search queries over encrypted data according to specified keywords. Song et al. gave the first SE scheme which required litter communication, but the computational overhead was linear in the size of search query. To tackle this problem, Boneh et al. presented a Public key Encryption with Keyword Search (PEKS) scheme. After that, many SE schemes enriched with different features had been proposed, such as single keyword search, multiple keywords search, fuzzy keyword search, verifiable keyword search, ranked keyword search. Compared with single keyword search multiple keyword search can quickly locate the results of interest and greatly decrease the waste of computation and bandwidth resources. As there is no tolerance of minor types and format inconsistencies in exact keyword search queries, fuzzy keyword search enhances the system usability by leveraging Wildcard, Locality-Sensitive

Hashing (LSH) or Bloom Filter (BL) techniques.

As the cloud is a semitrusted third-party which will execute a fraction of search operations and return a fraction of search results to save computation resources or hide data corruption accidents, verifiable keyword search can verify whether the results are correct or not. To further narrow down the search results, ranked keyword search can return the results in the order of relevance scores to keyword.

CONCLUSIONS

In this paper, to demonstrated a Lightweight Fine-Grained Search (LFGS) system for the resource-limited EUs in fog computing. On the one hand, the basic LFGS system could greatly reduce the computational and storage burden of EUs by outsourcing partial computation and storage to the honest-but-curious FNs without leaking sensitive information; on the other hand, the extended LFGS system could support conjunctive keyword search and attribute update to further narrow down the search scope and avoid unauthorized accesses, respectively. Furthermore, the formal security analysis showed that the LFGS system is selectively secure against CKA and CPA, and the empirical experiments using a real-world dataset illustrated the efficiency and feasibility of LFGS system in fog computing. As a part of our future work, These also will continue to concentrate on expressive search including fuzzy keyword search, semantic keyword search, and so on. Besides, the secure channel utilized in our LFGS system should be eliminated as secure channel will incur high communication burden. Hence, They still need to further improve the efficiency of LFGS system so that it can be applied in various schemes.

References

[1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and finegrained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, 2017.

[2] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 78–88, 2017.

[3] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of iot and cloud computing," Future Generation Computer Systems, vol. 78, pp. 964–975, 2018.

[4] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," Future Generation Computer Systems, vol. 78, pp. 825– 837, 2018.

[5] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," Future Generation Computer Systems, 2017.

[6] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships