Comparison of Security and Performance Issues in Fog Enabled Cloud Computing

C. Nagarani
Reasearch scholar, Department of Computer Science, Dr.NGP Arts & Science College, Coimbatore, India

R. Kousalya, PhD
Assistant Professor,Department of Computer Science, Dr.NGP Arts & Science College, Coimbatore, India

ABSTRACT
Fog computing is a paradigm that extends the cloud computing and services to the edge of the network. Similar to services to end users. However, several challenges are addressed in fog computing in terms of security, authentication and authorization, privacy, revocation handling and data auditing techniques. This paper reviews various existing research work based on authentication, dynamic updation , access control in fog computing and provides merits and demerits of each system.

Keywords
Fog Computing, Cloud Computing, Cloud Service Provider, Authentication, Access Control

1. INTRODUCTION
Fog computing is a decentralized computing infrastructure whereby a data is processed and stored between the source of origin and a cloud architecture. This results in the reduction of data transmission overheads and subsequently, improves the cloud computing performance by reducing the requirement for processing and storing huge number of superfluous data. The fog computing paradigm is mostly motivated by a continuous growth in Internet of Things (IoT) devices. IOT devices provide rich functionality like connectivity and the development of new functionality. These devices require computing resources for processing the acquired data. However, the fast decision processes are also needed for maintaining a high-level of functionality. This can make scalability and reliability issues when using a standard client-server framework, where data is sensed by the client and processed by the server. If a server was to become overloaded in the conventional client-server framework, then many devices could be rendered unusable.

The fog paradigm has the objective for providing the scalable decentralized solution for this issue. This is achieved by providing a new hierarchically distributed and local platform between the cloud system and end-user devices. This platform has the ability of filtering, aggregating, processing, analysing and transmitting the data and will result in saving time and communication resources. This new paradigm is called as Fog computing and introduced by Cisco. Cisco pioneered the delivery of the Fog computing model that extends and brings the Cloud platform closer to end-user's device to resolve aforementioned issues. Fog system has the following characteristics:

- It will be placed at the edge of network with rich and heterogeneous end-user support.
- It provides support to a broad range of industrial applications due to instant response capability and has its own computing, storage and networking services.
- It is a highly virtualized platform and operates locally.
- It offers inexpensive, flexible and portable deployment in terms of both hardware and software.

However, there are no standard security certifications and measures defined for the fog computing. Also, it could be stated that a fog platform has relatively smaller computing resources due to their nature and hence it would be complex for executing a full suite of security solutions that are having the ability of detecting and preventing sophisticated, targeted and distributed attacks. It is an attractive target for cyber-criminals due to huge number of data throughput and likelihood of being able to obtain sensitive data from both cloud and IoT devices and also it is more accessible depending on the network configuration and physical location which increases the probability of an attack occurrence. Moreover, authentication and authorization solutions are not suit for fog computing since fog devices are operating at the edge of networks. The working surroundings of Fog devices will face with many threats that do not exist in a well-managed Cloud.

One of the most important issues in cloud computing is data security. Private data of users are stored in the data center of CSP (Cloud Service Provider) to release the storage and computing burden of personal devices. Typical data examples are social security records and health statistical data monitored by wearable sensors. However, the CSP could be curious on personal privacy. Thus, critical personal data stored in CSP are generally encrypted and their access is controlled. Obviously, these personal data could be accessed by other entities in order to satisfy a cloud service. Hence, a practical issue is how to control personal data access at CSP. A number of solutions have been proposed for protecting data access in the cloud. But, the drawback of such solutions is that computation complexity grows linearly with the number of data-groups or number of users. In addition, the time spent on data encryption, decryption and key management is more than symmetric key or asymmetric key encryptions.

When adversaries gain control over the cloud server, they have the capability to launch forge attack or replay attack which is aimed at breaking the linear independence among encoded data by replacing the data stored in the corrupted cloud server with old encoded data. Therefore, the integrity of users' data stored on the remote cloud server is vulnerable to internal and external attacks. Therefore, a more efficient technique is required to remotely verify the integrity of the outsourced data in the cloud. To address the issue of data integrity in cloud computing, researchers have developed different data auditing techniques such as integrity-based, recovery-based and deduplication-based techniques. However, the applied data structures in the data auditing methods are unable to effectively support dynamic data update operation

for large-scale data efficiently, especially frequent data update. Hence, it is imperative to design a new data structure to support dynamic update for large-scale data.

2. AUTHENTICATION IN FOG COMPUTING

2.1. Mutual Authentication Mechanism

Mutual authentication mechanism for the Edge-Fog-Cloud network framework for mutually authenticating Fog users at the Edge of the network with the Fog servers at the Fog layer. This mechanism requires the user-roaming randomly in the network for holding only one long-lived master secret key allowing him to communicate with any of the Fog servers in the network in a fully authenticated manner. The fog users are having the ability for mutually authenticating with new fog servers connecting with the network, without the need for re-registering and without any extra overheads. Furthermore, the servers on the fog are required for storing only one secret key for each fog user. On the other hand, the Fog users are totally unrelated to any public-key infrastructure. The scheme requires the Fog user for performing very few hash invocations and symmetric encryptions/decryptions. Therefore, the scheme is suitable to be efficiently implemented on the Fog user's smart card/device.

Demerits: This mechanism is only suitable for small scale networks where it is easy to reset and reinitialize the system when DoS attacks are detected.

2.2 Anonymous and Secure Aggregation Scheme (ASAS)

In the ASAS model, a fog node aggregates the data from terminal nodes and forwards the aggregated data to the public cloud server. By using the ASAS scheme, the fog node can help terminal devices upload their data to PCS. By using the data aggregation technique, the ASAS scheme can save bandwidth between the fog node and PCS. At the same time, the ASAS scheme not only protects the identities of terminal devices by using pseudonyms but it also guarantees data secrecy through a homomorphic encryption technique.

Demerits: Communication overhead is moderately high.

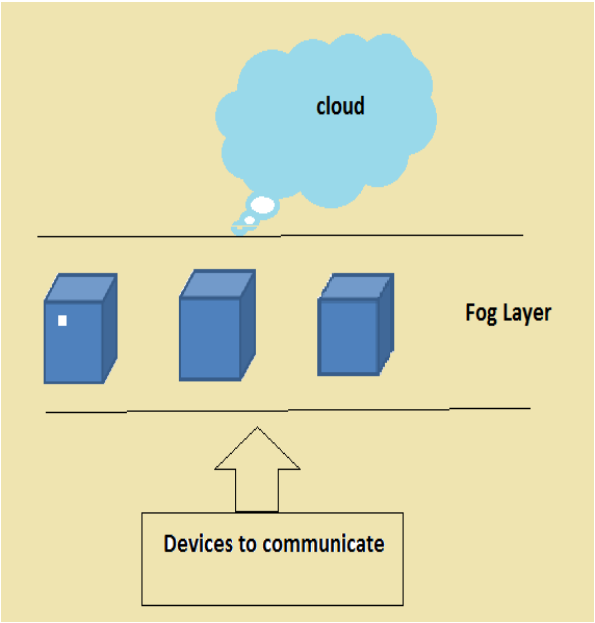

Fig 1: Fog enabled cloud computing

2.3 Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) against key-delegation abuse in fog computing. Initially, they observed that if a user can generate a new private key for a portion of his/her access right, this could potentially lead to some undesirable situations, which violates the access control policy. In this scheme, the property of bilinear groups is utilized. A user private key consists of components for all attributes, of which each is constructed based on either set of group elements according to if the user owns this attribute or not. Subsequently, the secret sharing scheme is applied on all attributes, and the bilinear map of key components and corresponding ciphertext components for all attributes are forced so that the key cannot be split nor combined with other private keys. The security properties of the scheme are proved in standard selective model.

Demerits: Computation cost is high during encryption process.

Table.1 Comparison of Authentication Techniques in Fog Computing

Title	Methods	Merits	Demerits
An Edge-Fog Mutual Authentication Scheme	Edge-Fog layer mutual authentication	Computationally efficient.	Only suitable for small scale networks where it is easy to reset and reinitialize the system when DoS attacks are detected.
Anonymous and secure aggregation scheme in fog-based public cloud computing	Anonymous and secure aggregation scheme, Homomorphic encryption	Secure and efficient.	Communication overhead is moderately high.
An Attribute-Based Encryption Scheme to Secure Fog Communications	Ciphertext-Policy Attribute Based Encryption (CP-ABE)	More desirable and feasible.	Computation overhead is high and also an efficiency of access structure is less.

3. FLEXIBLE ACCESS CONTROL

3.1 F2AC(Fine-grained Flexible Access Control)

Fine-grained, and flexible access control scheme for file storage in mobile cloud computing. F2AC can not only achieve iterative authorization, authentication with tailored policies, and access control for dynamically changing accessing groups, but also provide access privilege transition and revocation. A new access control model called directed tree with linked leaf model is proposed for further implementations in data structures and algorithms. F2AC can create, add, and delete users in a group (and a subgroup iteratively), authorize a user as a group leader who can

authorize privileges to other group users iteratively, and revoke privileges for a user in the group. F2ACcan manage access control such as merge, delete, and retrieve user or privileges in a lightweight manner via a proposed access control model, directed tree with linked leaf model. F2ACcan permit users to define various access control rules as they demand and separate the access control for system users and file users, which simplifies user experiences and management flows in cloud.

Demerits: The user with Authorize privilege cannot add more users for current files, namely, non-additive users.

3.2 CP-AB Based Access Control

In this scheme, the original decryption keys are spilt into a control key, a secret key and a set of transformation keys. The private cloud managed by the organization administrator takes charge of updating the transformation keys using the control key. It helps to handle the situation of flexible access management and attribute alteration. Meanwhile, the mobile user's single secret key remains unchanged as well as the cipher text even if the data user's attribute has been revoked. In addition, the access control list is modified through adding the attributes with corresponding control key and transformation keys so as for managing user privileges depending upon the system version.

Demerits: Computation load for key and data management is heavy.

3.3 Hierarchical Attribute-Set-Based Encryption

It extends cipher text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. The proposed scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing.

Demerits: The computation cost of this solution is generally high due to the complexity of attribute structure. The time spent on data encryption, decryption and key management is more than symmetric key or asymmetric key encryptions.

Table.2 Comparison of Flexible Access Control

Title	Methods	Merits	Demerits
F2AC: Fine-Grained, and Flexible Access Control	Fine-grained, and flexible access control scheme, Iterative authorization, authentication, directed tree with linked leaf model	Energy consumption and storage are less.	The user with Authorize privilege cannot add more users for current files, namely, non-additive users.
Flexible CP-ABE Based Access Control	Attribute-based access control, Outsourcing computing, attribute alteration, data verification	Secure, flexible and efficient.	Computation load for key and data management is heavy.
HASBE: A Hierarchical Attribute-Based Access Control in Cloud Computing	Access control, Ciphertext-Policy Attribute-Set-Based Encryption (CP-ASBE)	High security and flexibility.	Computation cost and time consumption are high.

4. DYNAMIC UPDATING MECHANISM

4.1 Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud

They focussed on the problem of data-integrity verification for the client's data residing on the Cloud Storage Server (CSS). Here, an existing third party auditing protocol is optimized and created it to replace, replay and forge attacks launched by malicious insiders at CSS. In this protocol, CSS-response size is optimized by storing Homomorphic Linear Authenticators (HLA) for user's data on TPA's site. In addition, a protocol is proposed for performing efficient block-level and fine-grained dynamic-data update operations on data stored on the cloud by using Chameleon Hashing and a modified Chameleon Authentication Tree.

Demerits: Overall computation time is high.

4.2 Dynamic-Hash-Table based Public Auditing for Secure Cloud Storage.

A novel public auditing scheme is proposed for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at a third parity auditor (TPA) to record the data property information for dynamic auditing. The proposed scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, the proposed scheme can

also achieve higher updating efficiency than the state-of-the-art schemes. In addition, the proposed scheme is extended for supporting privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA, and batch auditing is achieved by employing the aggregate BLS signature technique.

Demerits: Computational cost is high during searching phase.

4.3 Dynamic Remote Data Auditing for securing big data storage in cloud computing based on an algebraic signature.

The scheme incurs minimum computational and communication costs on the auditor and server side. Also, a new data structure such as Divide and Conquer Table (DCT) is designed for efficiently supporting dynamic data operations such as insert, append, delete, and modify. With the new data structure, the proposed method can be applied for frequent update of large-scale data with minimum computational cost on the auditor and server.

Demerits: This scheme does not support for auditing the integrity of large archival files in distributed cloud storage systems.

Table.3 Comparison of Dynamic Updating

Title	Methods	Merits
Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing	Third party auditing protocol, Efficient block-level and fine-grained dynamic-data update operations, Modified Chameleon Authentication Tree	Efficient and secure.
Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage	Public auditing, Dynamic hash table, homomorphic authenticator, aggregate BLS signature technique.	Storage cost is less and secure auditing is achieved.
Dynamic remote data auditing for securing big data storage in cloud computing	Remote data auditing, Data integrity, Divide and Conquer Table	Reduced computational and communication costs.

5. CONCLUSION

This survey paper outlined the overview of security and privacy issues in fog computing. The aim of this survey is to summarize current research contribution to solve different challenges in privacy and security in fog computing. This study showed that there must be need of proposed systems to provide security to the data and the data access performance in fog enabled cloud computing**.**

6. REFERENCES

[1] Ibrahim, M. H. **(**2016). Octopus: An Edge-fog Mutual Authentication Scheme. *IJ Network Security*, *18*(6), 1089-1101.

[2] Wang, H., Wang, Z., & Domingo-Ferrer, J. (2017). Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Generation Computer Systems*.

[3] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017). An Attribute-Based Encryption Scheme to Secure Fog Communications. *IEEE Access*.

[4] Li, W. M., Li, X. L., Wen, Q. Y., Zhang, S., & Zhang, H. (2017). Flexible CP-ABE Based Access Control on Encrypted Data for Mobile Users in Hybrid Cloud System. *Journal of Computer Science and Technology*, *32*(5), 974-990.

[5] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017). An Attribute-Based Encryption Scheme to Secure Fog Communications. *IEEE Access*.

[6] Wan, Z., Liu, J. E., & Deng, R. H. (2012). HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE transactions on information forensics and security*, *7*(2), 743-754.

[7] Singh, A. P., & Pasupuleti, S. K. (2016). Optimized Public Auditing and Data

[8] Dynamics for Data Storage Security in Cloud Computing. *Procedia Computer Science*, *93*, 751-759.