EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING

[1]REGONDA SAIKUMAR, [2]SAIKRISHNA.D

[1]MCA Student, [2]Assistant Professor

DEPARTMENT OF MCA

SREE CHAITANYA COLLEGE OF ENGINEERING, KARIMNAGAR

ABSTRACT

Fog-to-cloud computing has now become a new cutting-edge technique along with the rapid popularity of Internet of Things (IoT). Unlike traditional cloud computing, fog-to-cloud computing needs more entities to participate in, including mobile sinks and fog nodes except for cloud service provider (CSP). Hence, the integrity auditing in fog-to-cloud storage will also be different from that of traditional cloud storage. In the recent work of Tian et al., they took the first step to design public auditing system for fog-to-cloud computing. However, their scheme becomes very inefficient since they uses intricate public key cryptographic techniques, including bilinear mapping, proof of knowledge etc. In this paper, we design a general and more efficient auditing system based on MAC and HMAC, both of which are popular private key cryptographic techniques. By implementing MAC and HMAC, we give a concrete instantiation of our auditing system. Finally, the theoretical analysis and experiment results show that our proposed system has more efficiency in terms of communication and computational costs.

I. INTRODUCTION

Fog computing, which is first proposed by Bonomi et al.in 2012 [6], has now been a popular technique for kinds of industrial fields based on Internet-of Things (IOT) devices [15], [16], [19], [32]. As a middleware between IOT devices and clouds, fog computing nodes have their own basic computing, storage as well as resources to achieve the requirements for data preprocessing and transmission. Therefore, the model of fog-to-cloud computing emerges as an attractive solution for data storage in some resource-constrain large-scale industrial applications.

However, fog-to-cloud computing has also to face some classical problems appeared in traditional cloud computing. One of the most famous concerns is how to ensure the integrity of stored in cloud service provider (CSP). The reason is as follows. Some CSP may try to conceal the fact that some important data of IoT devices or fog nodes has been lost or corrupted due to kinds of internal or external attacks [25]. Hence, developing efficient auditing techniques for secure data storage in fog-to-cloud computing are also very necessary and significant just like in traditional cloud computing.

Although, in past years, many auditing schemes are presented for traditional cloud storage [12], [22], [25], [26], [31], [33], including many private and public auditing schemes, all of them are not directly applicable to fog-to-cloud computing for two main reasons [23], [24]. The _rst one is that the data from IOT is generated by various devices and hence it is inadvisable for those users (or data owners) to first retrieve these data and generate corresponding authenticators before outsourcing. The second one, which is also more important, is

that the existing auditing systems do not involve fog computing nodes, which are rather crucial entities for fog-to-cloud computing because those nodes can help to efficiently process and rapidly transmit for large-scale of IOT data. Hence, it is urgent to develop new auditing techniques to ensure data's integrity for fog-to cloud computing. In recent work of [23], Tian et al. took the first step to this direction and try to _fill this gap. In fact, they designed a privacy-preserving public auditig system based on bilinear mapping and the so-called tag-transforming strategy. In addition, they also evaluated the performances of their scheme by theoretical analysis and comprehensive experiments.

It is well-known that, in public auditing scheme, the task to verify the integrity of users' data is suitable to be outsourced to another authorized third-party auditor (TPA), which may have more professional knowledge on auditing and more computational resources. However, it should also be noted that, generally speaking, public auditing systems have lower efficiencies than private ones. Just as Zhang et al. illustrated in [33], for a same data _le, the time consumptions for proving, verifying and outsourcing in public auditing scheme are hundreds (or even thousands) of times of the corresponding process in their private scheme. Hence, in some pursuing-efficiency scenarios, especially for the resource-constrained mobile sinks in fog-to-cloud computing, we believe the private auditing system may be more popular. Therefore, it is also necessary and significant to design efficient private auditing schemes for the fog-to-cloud computing.

In this paper, we try to take the step to this direction. More specifically, we propose a new auditing system base on private authentication techniques: message authentication code (MAC) [14] and homomorphic MAC (HMAC) [2], [8]_[10] schemes, both of which are important primitives in cryptography. The MAC technique is used in the transmission process between mobile sinks and fog nodes while the HMAC scheme is used to verify the integrity of data blocks stored in CSP. Since a common private key is needed for the parties in MAC or HMAC when generating or verifying the tags, this model is not suitable to introduce TPA into it.

Moreover, we give a concrete instantiation of the system by instantiating the hash-based MAC scheme in [14] and the efficient HMAC scheme designed by Agrawal and Boneh in [2].

Finally, we also analyze the performances of our proposed system and compare them with that of Tian et al. as well as two related traditional cloud auditing schemes in [20] and [18]. The experiment results show that our system outperformed Tian et al.'s system in terms of communication costs and computational efficiency. Moreover, our protocol is suitable for fog-to-cloud computing and hence prior to the two schemes in [18], [20].

II. SYSTEM ANALYSIS

EXISTING SYSTEM

Jues and Kaliski [13]. In PoR, one can combine error-correcting code with spot-checking of data blocks to ensure the data's integrity. But this technique only supports a limited number of verification operations. At the same time, Atniese et al. proposed provable data possession (PDP) based RSA-homomorphic authenticators, which can support both unlimited number of challenges and public auditing [3].
Subsequently, many works focused on the improvement of communication efficiency [4], [7], [11], [20]. Some other researches considered the dynamic update of PDP schemes [12], [22],

[26], [28]. To support data dynamics, kinds of authenticated data structures are widely introduced into the public auditing schemes. For example, in 2011, Wang et al. presented the Merkle-hash-tree-based public auditing for dynamic data [26]. Later, Zhu et al. proposed a new data structure, called index hash table, to achieve data dynamics [34]. In 2017, Tian et al. further suggested a two-dimensional data structure, named dynamic hash table, to achieve both public auditing and dynamic data updating [22]. At the same year, Shen et al. proposed another novel structure, which includes a doubly linked info table and a location array,
to achieve dynamic data [21].
However, few of them can be directly extended to achieve efficient and secure verification for data storage in the fog-to-cloud based IoT scenarios, although there are fruitful schemes suggested in the traditional cloud storage. The two main reasons are as follows. First, in fog-to-cloud case, the data are usually generated by various IoT devices, instead of the data owners themselves. Second, some new entities, like fog nodes, are introduced and also play important roles for processing and transmission in fog-to-cloud scenario. But in the traditional cloud storage, they are never considered.
Therefore, in the recent works, Tian et al., [23] and Kashif and Mohammed [18] respectively filled this gap in the public auditing setting based on different techniques. Nevertheless, the more efficient private key auditing schemes are not considered in both papers.

Disadvantages

1) The system was not implemented Attribute Based Encryption and data auditing techniques on outsourced data.
2) The system is less security due to lack of Identity-Based Encryption.

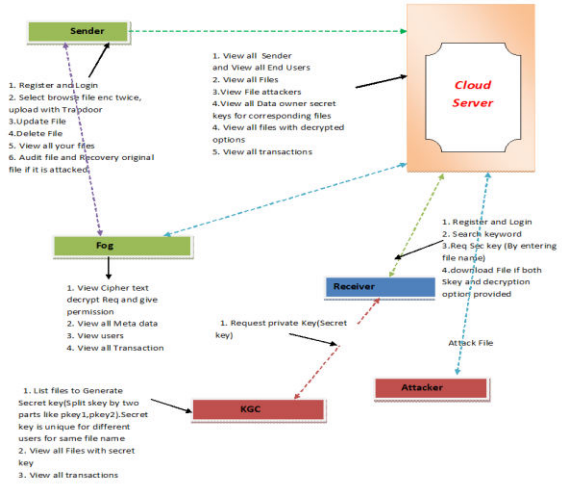
PROPOSED SYSTEM

In the proposed system, the system tries to take the step to this direction. More specifically, we propose a new auditing system based on private authentication techniques: message authentication code (MAC) [14] and homomorphic MAC (HMAC) [2], [8]_[10] schemes, both of which are important primitives in cryptography. The MAC technique is used in the transmission process between mobile sinks and fog nodes while the HMAC scheme is used to verify the integrity of data blocks stored in CSP. Since a common private key is needed for the parties in MAC or HMAC when generating or verifying the tags, this model is not suitable to introduce TPA into it. Moreover, we give a concrete instantiation of the system by instantiating the hash-based MAC scheme in [14] and the efficient HMAC scheme designed by Agrawal and Boneh in [2].

Advantages

- DATA PREVENTION. DYNAMIC UPDATE AND PREVENTING REPLAY ATTACKS.
- An Efficient Data Auditing and Recovery techniques to provide more security on the remote data sender data.

Architecture Diagram



III. IMPLEMENTATION

SENDER (OWNER)

In this module sender will have to register and get authorized before he performs any operations. After the authorization the sender can upload file with trapdoor and will have the update, delete, verify and recovery options for the file uploaded.

CSP

In this module CSP will issue permission for both owner (Sender) and user (Receiver). And view the file uploaded and the attackers related to files in cloud. View the files in decrypted format and with the corresponding secret keys and its transactions.

RECEIVER (USER)

In this module, User has to register and login, and search for the files by entering keyword and request secret key and download the particular file from the cloud if both secret key and the decryption permissions are provided.

FOG

Views all the files decrypt permission reqest form the users and provide permission and view its related metadata and the transactions related to the requests from users.

KGC

In this module the private key generator generates the secret key. It splits the key into two parts such as pkey1 and pkey2. This generated key is unique for different users for same file and view all the generated secret keys and the transactions related to it.

IV. CONCLUSION

In this project, we propose an efficient auditing system for fog-to-cloud computing. Although our system is not public auditing, it obviously outperforms the one proposed by Tian et al. in terms of communication and computational efficiencies. The simulation results illustrate the computational efficiency. We believe that our proposed system must be an interesting choice for securely storage of data in fog-to-cloud computing.

REFERENCES

[1] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, ``Charm: A framework for rapidly prototyping cryptosystems," J. Cryptogr. Eng., vol. 3, no. 2, pp. 111_128, Jun. 2013.

[2] S. Agrawal and D. Boneh, ``Homomorphic MACs: MAC-based integrity for network coding," in Applied Cryptography and Network Security, (Lecture Notes in Computer Science), vol. 5536. Berlin, Germany: Springer, 2009, pp. 292_305.

[3] G. Ateniese, R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Song, ``Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, 2007, pp. 598_609.

[4] G. Ateniese, S. Kamara, and J. Katz, ``Proofs of storage from homomorphic identi_cation protocols," in Advances in Cryptology. Berlin, Germany: Springer, 2009, pp. 319_333.

[5] A. F. Barsoum and M. A. Hasan, ``Provable multicopy dynamic data possession in cloud computing systems," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485_497, Mar. 2015.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ``Fog computing and its role in the Internet of Things," in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput., New York, NY, USA, 2012, pp. 13_16.

[7] K. Bowers, A. Juels, and A. Oprea, ``Proofs of retrievability: Theory and implementation," in Proc. ACM Workshop Cloud Comput. Secur., 2009, pp. 43_54.

[8] J. Chang, Y. Ji, M. Xu, and R. Xue, ``General transformations from single-

generation to multi-generation for homomorphic message authentication schemes in network coding," Future Gener. Comput. Syst., vol. 91, pp. 416_425, Feb. 2019.
[9] J. Chang et al., ``Secure network coding from secure proof of retrievability," Sci. China Inf. Sci., early access, Oct. 2020.
[10] J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, ``RKA security for identity-based signature scheme," IEEE Access, vol. 8, pp. 17833_17841, 2020.
[11] Y. Dodis, S. Vadhan, and D. Wichs, ``Proofs of retrievability via hardness ampli_cation," in Proc. Theory Cryptogr. Conf., 2009, pp. 109_127.
[12] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ``Dynamic provable data possession," in Proc. CCS, 2009, pp. 213_222.
[13] A. Juels and B. J. Kaliski, ``PORs: Proofs of retrievability for large _les," in Proc. 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, 2007, pp. 584_597.
[14] J. Katz and Y. Lindell, Introduction to Modern Cryptography. London, U.K.: CRC Press, 2007.
[15] A. Kaswan, V. Singh, and P. K. Jana, ``A multi-objective and PSO based energy ef_cient path design for mobile sink in wireless sensor networks," Pervasive Mobile Comput., vol. 46, pp. 122_136, Jun. 2018.
[16] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, ``Making knowledge tradable in edge-AI enabled IoT: A consortium block chain-based efficient and incentive approach," IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6367_6378, Dec. 2019.
[17] B. Lynn. The Standard Pairing Based Crypto Library. Accessed: Jul. 27, 2016. [Online]. Available: http://crypto.standford.edu/pbc