International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

An Attribute-Based Encryption Scheme to Secure Fog Communications

B .Mogileeswaraiah, Mr. S.A. Md. Noorulla Baig
Department Of Computer Science, Riims Tirupathi, Andhra Pradesh, India

ABSTRACT

Fog Computing is considered as a profoundly virtualized worldview that can empower processing at the Internet of Things gadgets, living in the edge of the system, to deliver administrations and applications all the more proficiently and viably. Since Fog processing begins from and is a non-minor expansion of distributed computing, it acquires numerous security and protection difficulties of distributed computing, causing the broad worries in the examination group. To empower true and condential interchanges among a gathering of mist hubs, in this paper, we propose a proficient key trade convention in view of cipher text policy attribute-based encryption (CP-ABE) to build up secure correspondences among the members. To accomplish condentiality, validation, inconstancy, and access control, we join CP-ABE and computerized signature procedures. We investigate the productivity of our convention as far as security and execution. We additionally actualize our convention and contrast it and the testament based plan to outline its possibility.

Keywords: Fog computing, security, ciphertext-policy attribute based encryption (CP-ABE), cloud

I. INTRODUCTION

Fog computing is a promising processing worldview that stretches out distributed computing to the edge of the system. It empowers another type of uses and administrations, for example, quality of services (QoS) improvement, and low latency. Fog Computing can give these administrations flexible assets requiring little to no effort. It likewise empowers the smooth meeting between distributed computing and IoT gadgets for content conveyance. As promising as it may be, Fog computing is confronting numerous security issues. Secure interchanges are among the issues that raise the most worries from clients when they utilize haze figuring to transmit their information to the cloud to be put away and handled. All in all, the noteworthy dangers in mist processing systems are: **Data Alteration**: An enemy can trade off information trustworthiness by endeavoring to adjust or pulverize the honest to goodness information. Consequently, it is basic to eat a security instrument to give information trustworthiness confirmation of the transmitted information between the Fog nodes and the cloud. **Unauthorized Access**: An enemy can pick up gets to unapproved information without consent or capabilities, which could bring about misfortune or robbery of information. This assault raises a security issue that could uncover a client's private data. **Eavesdropping Attacks**: Eavesdroppers can increase unapproved interference to take in a ton about the client data transmitted through remote interchanges. The essential security prerequisites for the interchanges between the fog nodes and the cloud are: privacy, get to control, validation, and undeniable nature. To adequately guard against the previously mentioned dangers, we require a proficient security component that can fulfill the essential security prerequisites. Attribute-Based Encryption (ABE) created is a promising arrangement that can give a portion of the security necessities. ABE is an open key in view of one-to-numerous encryption that utilizes the client's way of life as a characteristic. In ABE, an arrangement of properties and a private key figured from the traits are separately utilized for encryption and unscrambling. There are two principle sorts of ABE frameworks: Key-Policy ABE (KP-ABE) and Cipher text Policy ABE (CP-ABE). In KP-ABE, the parts of the credits are utilized to depict the ciphertext and an access strategy is related with the client's private key; while in CP-ABE the traits are related with the client's private key and the figure content is related with an access arrangement. In this paper, we build up a scrambled key trade convention in view of Ciphertext-Policy Attribute Based Encryption (CP-ABE) to empower validated and condential correspondences between fog nodes and the cloud. The convention sets up secure correspondences to trade the common key that can be utilized to encode and unscramble the traded data. The motivation behind this undertaking is, the paper proposes a certificateless aggregate signcryption scheme (CLASC) that is very effective. Based on the proposed plot, an information transmission convention for checking street surface conditions is composed with security perspectives, for example, data classification, common realness, honesty, protection and obscurity. In breaking down the framework, the capacity of the proposed convention to accomplish the set targets and exercise higher effectiveness concerning computational and correspondence capacities in contrast with existing frameworks is additionally considered.

II. EXISTING METHOD

The essential security prerequisites for the interchanges between the fog nodes and the cloud are: secrecy, get to control, validation, and variability. To viably shield against the previously mentioned dangers, we require a proficient security system that can fulfill the essential security necessities. Attribute Based Encryption (ABE) created by it is a promising arrangement that can give a portion of the security prerequisites. ABE is an open key in view of one-to-numerous encryption that utilizes the client's way of life as a property.

In ABE, an arrangement of qualities and a private key registered from the characteristics are individually utilized for encryption and decoding. There are two primary kinds of ABE frameworks: Key-Policy ABE (KP-ABE) and Cipher content Policy ABE (CP-ABE). In KP-ABE the parts of the credits are utilized to depict the figure content and an access arrangement is related with the client's private key; while in CP-ABE the properties are related with the client's private key and the figure content is related with an access strategy. In this paper, we build up an encoded key trade convention in light of Cipher Content Policy Attribute Based Encryption (CP-ABE) to empower validated and condential interchanges between fog nodes and the cloud. The major drawback of this existing system is the convention builds up secure correspondences to trade the mutual key that can be utilized to scramble and decode the traded data. Each fog node can get the common key just if the fog node fulfills the arrangement denned over a set of attributes which is attached to the cipher text.

III. PROPOSED METHOD

A network Model for fog and distributed computing is shown in below figure. Proposed method is made out of the accompanying substances: a cloud, a key generator server, fog nodes, and IoT gadgets. The key generator server is utilized to create and circulate the keys among the included elements. The cloud defines the access structure A what's more, plays out the encryption to get ciphertext. We accept that the access structure is given to all fog nodes. The fog node conveys an arrangement of traits that is defined by an access structure related with the ciphertext. Specifically, we accept that each fog node is related with S properties that be an important string of self-arbitrary length.

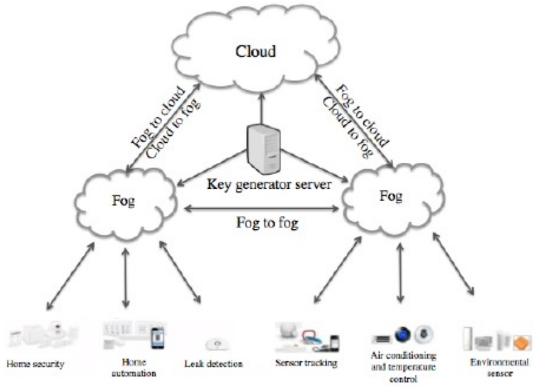

Figure 1. Proposed Model

With a specific end goal to accomplish the security prerequisites of the correspondences between fog nodes and the cloud, we propose an protocol based on the combination CP-ABE. All the more specifically, we outline a convention with the end goal that each fog node is related with an arrangement of characteristics, and allocate each ciphertext with an expressive access structure that is defined over these qualities. This element authorizes the decoding methodology in light of the fog nodes qualities. Each ciphertext conveys an access structure with the end goal that the mist can decode the ciphertext and acquire the mutual key just on the off chance that it has the specified characteristics in the access structure. In this area, we propose our convention in light of the blend of CP-ABE and advanced mark systems. In the first place, we define the get to structure of our convention. At that point, we detail our convention calculations. In our convention, we use an access tree proposed by as an access structure.

we analyze the security strength of our proposed protocol from the aspects of collusion attack resistance, message authentication, and unforgeability. Let T be a representing an access structure, where each non-leaf node is a threshold gate, and each leaf node describes an attribute. Toward the start of our convention, each haze hub is related with an access structure A. The convention can be executed with the accompanying calculations: Setup, Key Generation, Encryption, and Decryption.

A private key is issued for each fog node in light of the relating trait set S. At that point, the cloud runs the encryption calculation that yields a scrambled symmetric key. The cloud communicates the scrambled key to a gathering of mist hubs. After accepting the scrambled key, each fog node runs the decoding calculation utilizing its private key to remove the symmetric key. Our convention comprises of four calculations that are point by point as explained below:

1.Collusion Attack Resistance

In the proposed plot, we utilize CP-ABE to ensure the security of the common key (session key). CP-ABE gives a get to structure for each scrambled information, and requires just a subset of the properties for decoding. Since the mystery key includes an interesting irregular number for each quality in the get to strategy, CP-ABE can protect against agreement assaults. Therefore, illicit clients cannot get the traded shared key through intrigue exercises.

2) Message Authentication

Accept that the cloud needs to send the symmetric key K to the mist hubs, which has the normal qualities, the cloud scrambles K, at that point it communicates the scrambled message. At the point when the haze hubs acquire the scrambled message, they require their private keys SK

3) Unforgeability

A Rival who needs to make a legitimate mark of a lawful client must have the client's private key. Nonetheless, a rival can't construe the private key SK. Then again, it is inconceivable for the foe to make another, legitimate ciphertext also, signature from another client's ciphertext and mark. On the off chance that the foe modifies the ciphertext of the mutual key, the beneficiary can check that the ciphertext is illicit utilizing Calculation 4. If the rival connives with different clients to produce the ciphertext and mark, it can't succeed because CP-

ABE can protect intrigue assaults. Along these lines we guarantee that our proposed conspire is unforgeable under picked message assaults.

we propose a novel scrambled key trade convention in light of CP-ABE for secure interchanges in a fog processing system, which includes the Following accomplishments:

- ✓ We build up a convention for encoded key trade in light of CP-ABE that joins encryption and mark to accomplish a _ne-grained information get to control, condentiality, validation, and inconstancy.
- ✓ We examine the security of our convention and demonstrate its rightness. Specifically, we research the security of our convention under various assault situations.
- ✓ We break down the execution of our proposed convention and outline its effectiveness regarding message size and correspondence overhead.
- ✓ We execute and contrast our convention and an authentication based convention and demonstrates its plausibility.

Finally, extra overhead outcomes from checking the certificate's status and the certificate's legitimacy time frame utilizing either the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). Truth be told, the most widely recognized renouncement approach is the CRL which is required to download the CRL able to check the certificate's status. The size of a CRL can fluctuate between a couple of bytes to megabytes contingent upon the quantity of the repudiated certificates and accordingly it includes a capacity overhead. Interestingly, our plan does not bring about any transmission overhead since it doesn't have to trade certificates or on the other hand any character data since the client's qualities are related with the private key. Moreover, there is no need to download a file or speak with an outsider to check the certificate's status since every private key is corresponded with a lapse date. In rundown, our plan is more efficient what's more, plausible contrasted and the certificate-based plan.

IV. CONCLUSION

In this paper, we plan an encrypted key exchange protocol to build up secure interchanges among a gathering of fog nodes and the cloud. In our convention, we use the advanced mark and CP-ABE strategies to accomplish the essential security objectives: confidentiality, authentication, verifiability, and get to control. We break down the security of our convention and show its rightness and feasibility. We likewise give an execution of our plan. We additionally analyze the proposed conspire with the certificate-based scheme and delineate its efficiency. In our future research, we will center around the accompanying headings. Initially, we plan to outline a protected convention with less calculation overhead to make it appropriate for IoT interchanges. Second, we will plan an efficient get to structure for fog processing and IoT gadgets.

V. REFERENCES

[1]. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption,in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321_334.

[2]. R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 195_203.Z. Wan, J. Liu, and R. H. Deng, HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743_754, Apr. 2012.

[3]. D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, Secure data processing framework for mobile cloud computing, in Proc. IEEE Conf. Comput.Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 614_618.

[4]. J.-M. Do, Y.-J. Song, and N. Park, Attribute based proxy re-encryption for data confidentiality in cloud computing environments, in Proc. 1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng. (CNSI), 2011,pp. 248_251.

[5]. L. Xu, X. Wu, and X. Zhang, Cl-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud, in Proc. 7th ACM Symp. Inf., Comput. Commun. Secur., 2012, pp. 87_88.

[6]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute based encryption, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1,pp. 131_143, Jan. 2013.

[7]. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and grained data access control in cloud computing, in Proc. IEEE INFOCOM, Mar. 2010, pp. 1_9.

[8]. J. Hur, Improving security and efficiency in attribute-based data sharing, IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271_2282, Oct. 2013.

[9]. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, Fog computing for the Internet of Things: Security and privacy issues, IEEE Internet Comput.,vol. 21, no. 2, pp. 34_42, Mar. 2017.