International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

An Attribute Based Encryption Scheme to Secure Fog Communications

M AKHIL
M. Tech
Department of Computer Science Engineering
Bheema Institute of Technology and Science
Bellary - Adoni Rd, Dhanapuram, Andhra Pradesh

G.S Udaya Kiran Babu
Assistant Professor to Associate Professor
Department of Computer Science Engineering
Bheema Institute of Technology and Science
Bellary - Adoni Rd, Dhanapuram, Andhra Pradesh

***Abstract*—** Fog computing is deemed as a highly virtualized paradigm that can enable computing at the Internet of Things devices, residing in the edge of the network, for the purpose of delivering services and applications more efficiently and effectively. Since fog computing originates from and is a non-trivial extension of cloud computing, it inherits many security and privacy challenges of cloud computing, causing the extensive concerns in the research community. To enable authentic and confidential communications among a group of fog nodes, in this paper, we propose an efficient key exchange protocol based on ciphertext policy attribute-based encryption (CP-ABE) to establish secure communications among the participants. To achieve confidentiality, authentication, variability, and access control, we combine CP-ABE and digital signature techniques. We analyze the efficiency of our protocol in terms of security and performance. We also implement our protocol and compare it with the certificate-based scheme to illustrate its feasibility.

Keywords— CP-ABE, Fog Computing, IoT;

1. Introduction

Fog computing is a promising computing paradigm that extends cloud computing to the edge of the network. It enables a new breed of applications and services such as location awareness, quality of services (QoS) enhancement, and low latency. Fog computing can provide these services with elastic resources at low cost. It also enables the smooth convergence between cloud computing and IoT devices for content delivery. As promising as it is, fog computing is facing

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

many security issues. Secure communications are among the issues that raise the most concerns from users when they use fog computing to transmit their data to the cloud to be stored and processed. In general, the significant threats in fog computing networks are:

Data Alteration: An adversary can compromise data integrity by attempting to modify or destroy the legitimate data. Hence, it is essential to define a security mechanism to provide data integrity verification of the transmitted data between the fog nodes and the cloud.

Unauthorized Access: An adversary can gain accesses to unauthorized data without permission or qualifications, which could result in loss or theft of data. This attack raises a security issue that could expose a user's private information.

Eavesdropping Attacks: eavesdroppers can gain unauthorized interception to learn a lot about the user information transmitted via wireless communications. The risk of such attacks is that they cannot be easily detected because eavesdropping does not change anything in the network operations. The primary security requirements for the communications between the fog nodes and the cloud are: confidentiality, access control, authentication, and variability. To effectively defend against the aforementioned threats, we need an efficient security mechanism that can satisfy the primary security requirements. Attribute-Based Encryption (ABE) developed by [1] is a promising solution that can provide some of the security requirements. ABE is a public key based on one-to-many encryption that employs the user's identity as an attribute. In ABE, a set of attributes and a private key computed from the attributes are respectively used for encryption and decryption.

There are two main types of ABE systems: Key-Policy ABE (KP-ABE) and Ciphertext- Policy ABE (CP-ABE). In KP-ABE, the roles of the attributes are used to describe the ciphertext and an access policy is associated with the user's private key; while in CP-ABE the attributes are associated with the user's private key and the ciphertext is associated with an access policy. In this paper, we develop an encrypted key exchange protocol based on Ciphertext-Policy Attribute Based Encryption (CP-ABE) to enable authenticated and confidential communications between fog nodes and the cloud. The protocol establishes secure communications to exchange the shared key that can be used to encrypt and decrypt the exchanged information.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

2. Scope

The scope of this project is An Attribute-Based Encryption Scheme to Secure Fog Communications to achieve confidentiality, authentication, very ability, and access control, we combine CP-ABE and digital signature techniques. We analyze the efficiency of our protocol in terms of security and performance. We also implement our protocol and compare it with the certificate-based scheme to illustrate its feasibility. Fog computing, security, cipher text-policy attribute based encryption (CP-ABE), cloud computing, communications security.

3. Objective

Fog computing is deemed as a highly virtualized paradigm that can enable computing at the Internet of Things devices, residing in the edge of the network, for the purpose of delivering services and applications more efficiently and effectively. Since fog computing originates from and is a non-trivial extension of cloud computing, it inherits many security and privacy challenges of cloud computing, causing the extensive concerns in the research community. To enable authentic and confidential communications among a group of fog nodes, in this paper, we propose an efficient key exchange protocol based on ciphertext policy attribute-based encryption (CP-ABE) to establish secure communications among the participants. To achieve confidentiality, authentication, variability, and access control, we combine CP-ABE and digital signature techniques. We analyze the efficiency of our protocol in terms of security and performance. We also implement our protocol and compare it with the certificate-based scheme to illustrate its feasibility.

4. Existing System

The primary security requirements for the communications between the fog nodes and the cloud are: confidentiality, access control, authentication, and variability. To effectively defend

against the aforementioned threats, we need an efficient security mechanism that can satisfy the primary security requirements. Attribute-Based Encryption (ABE) developed by it is a promising solution that can provide some of the security requirements. ABE is a public key based on one-to-many encryption that employs the user's identity as an attribute. In ABE, a set of attributes and a private key computed from the attributes are respectively used for encryption and decryption. There are two main types of **ABE systems**: Key-Policy ABE (KP-ABE) and Cipher text- Policy ABE (CP-ABE). In KP-ABE the roles of the attributes are used to describe the cipher text and anaccess policy is associated with the user's private key; while in CP-ABE the attributes are associated with the user's private key and the cipher text is associated with an access policy. In this paper, we develop an encrypted key exchange protocol based on Cipher text-Policy Attribute Based Encryption (CP-ABE) to enable authenticated and confidential communications between fog nodes and the cloud.

Drawbacks

The protocol establishes secure communications to exchange the shared key that can be used to encrypt and decrypt the exchanged information. Each fog node can obtain the shared key only if the fog node satisfies the policy denned over a set of attributes which is attached to the cipher text.

5. Problem statement

For enterprise systems running on public clouds in which the servers are outside the control domain of the enterprise, access control that was traditionally executed by reference monitors deployed on the system servers can no longer be trusted. Hence, a self-contained security scheme is regarded as an effective way for protecting outsourced data. However, building such a scheme that can implement the access control policy of the enterprise has become an important challenge.

6. Proposed System

We propose a novel encrypted key exchange protocol based on CP-ABE for secure communications in a fog computing network, which features the Following achievements:

- We develop a protocol for encrypted key exchange based on CP-ABE that combines encryption and signature to achieve a fine-grained data access control, confidentiality, authentication, and variability.
- We discuss the security of our protocol and prove its correctness. In particular, we investigate the security of our protocol under different attack scenarios.
- We analyze the performance of our proposed protocol and illustrate its efficiency in terms of message size and communication overhead.
- We implement and compare our protocol with a certificate-based protocol and shows its feasibility

7. Modules Description

Data Alteration: An adversary can compromise data integrity by attempting to modify or destroy the legitimate data. Hence, it is essential to done a security mechanism to provide data integrity frication of the transmitted data between the fog nodes and the cloud.

Unauthorized Access: An adversary can gain accesses to unauthorized data without permission or qualifications, which could result in loss or theft of data. This attack raises a security issue that could expose a user's private information.

Eavesdropping Attacks: Eavesdroppers can gain unauthorized interception to learn a lot about the user information transmitted via wireless communications. The risk of such attacks is that they cannot be easily detected because eavesdropping does not change anything in the network operations.

8. Conclusion

In this paper, we design an encrypted key exchange protocol to establish secure communications among a group of fog nodes and the cloud. In our protocol, we utilize the digital signature and CP-ABE methods to achieve the primary security goals: confidentiality, authentication, variability, and access control. We analyze the security of our protocol and show its correctness and feasibility. We also provide an implementation of our scheme. We further compare the proposed scheme with the certificate-based scheme and illustrate its efficiency. In our future research, we will focus on the following directions. First, we intend to design a secure protocol

with less computation overhead to make it suitable for IoT communications. Second, we will design an efficient access structure for fog computing and IoT devices.

9. Future Enhancements

It is not possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:

As the technology emerges, it is possible to upgrade the system and can be adaptable to desired environment. Because it is based on object-oriented design, any further changes can be easily adaptable. Based on the future security issues, security can be improved using emerging technologies. Attendance module can be added. sub admin module can be added.

References

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

[2] R. Ostrovsky, A. Sahai, and B. Waters, ``Attribute-based encryption withnon-monotonic access structures," in Proc. 14th ACM Conf. Comput.Commun. Secur., 2007, pp. 195_203.

[3] A. Lewko and B. Waters, ``Unbounded HIBE and attribute-based encryption,"in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2011,pp. 547_567.

[4] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ``Fullysecure functional encryption: Attribute-based encryption and (hierarchical)inner product encryption," in Proc. Annu. Int. Conf. Theory Appl.Cryptograph. Techn., 2010, pp. 62_91.

[5] T. Okamoto and K. Takashima, ``Fully secure functional encryption with general relations from the decisional linear assumption," in Proc. Annu.Cryptol. Conf., 2010, pp. 191_208.

[6] L. Cheung and C. Newport, ``Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 456_465.

[7] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for _ne-grained access control in cloud storage services," in Proc. 17th ACMConf. Comput. Commun. Secur., 2010, pp. 735_737.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
September 2018

[8] Z. Wan, J. Liu, and R. H. Deng, ``HASBE: A hierarchical attribute-based solution for _exible and scalable access control in cloud computing," IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 743_754, Apr. 2012.

[9] 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.

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

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

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

[13] S. Yu, C. Wang, K. Ren, and W. Lou, ``Achieving secure, scalable, and _ne-grained data access control in cloud computing," in Proc. IEEEINFOCOM, Mar. 2010, pp. 1_9.

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