An Attribute-Based Encryption Scheme to Secure Fog Communications

Hisham Youssef Hassan  Malek Saad Abdelmawgood
Ahmed Abdulsattar  Bahaa Hussein  Morad Mohammed

Department of IET
GUC

19/4/2018
Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism
2. motivation
3. Network model
4. The proposed protocol
5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison
6. Conclusion
Fog computing

- 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 at low cost.
- It also enables the smooth convergence between cloud computing and IoT devices for content delivery.
- However, there are security issues when using fog computing to transmit data to the cloud.
Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
Significant Threats

Data Alteration

An adversary can compromise data integrity by attempting to modify or destroy the legitimate data.

Unauthorized Access

An adversary can gain accesses to unauthorized data without permission or qualifications, which could result in loss or theft of data.

Eavesdropping Attacks

eavesdroppers can gain unauthorized interception to learn a lot about the user information transmitted via wireless communications.
An Attribute-Based Encryption Scheme to Secure Fog Communications

Introduction

Security Requirements

Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
Security Requirements

Confidentiality
Sensitive data should be only disclosed to legitimate entities. In our system, we utilize CP-ABE to ensure confidentiality of the transmitted data.

Authentication
The system should prevent an active adversary who does not have the privilege to change or learn information of the transmitted data. Thus, a proper security mechanism should be adopted to ensure the authenticity of the data.
Security Requirements

Access Control

To reduce the risk of data exposure by an active adversary, a fine-grained access control should be enforced. The primary goal of our scheme design is to exchange the shared key securely.

Verifiability

From the entity’s signature, the fog node can be convinced that the message is generated by the same entity.
An Attribute-Based Encryption Scheme to Secure Fog Communications

Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
To effectively defend against threats, we need an efficient security mechanism that can satisfy the primary security requirements.

Attribute-Based Encryption (ABE) 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).
An Attribute-Based Encryption Scheme to Secure Fog Communications

Security mechanism

- 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 scheme 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.
- Each fog node can obtain the shared key only if the fog node satisfies the policy defined over a set of attributes which is attached to the ciphertext.
motivation

- One of the real world applications that motivates our problem formulation is smart grids.
- A smart grid system is an electrical grid that intelligently controls, measures, and balances energy.
- It can automatically change to a different energy resource depending on the availability and the energy demand, which can help consumers optimize their consumption and lower the cost of the bill.
- Smart grid system consists of suppliers, cloud, and grid sensors or devices.
An Attribute-Based Encryption Scheme to Secure Fog Communications

motivation
motivation

- Each smart grid gathers data and sends it back to the cloud via fog to analyze the behaviors of the consumers and the suppliers.
- The smart grid acts based on the results of the analysis of the collected data.
- This introduces new security challenges. In particular, attackers can easily launch many attacks when data is transmitted via a wireless channel and expose the users’ information.
- The transmitted data between fog nodes and the cloud for processing purposes allow the adversary to launch more attacks.
- Therefore we need an efficient protocol to establish secure communications between fog nodes and the cloud.
An Attribute-Based Encryption Scheme to Secure Fog Communications

Network model
Network model

- This network architecture is composed of the following entities: a cloud, a key generator server, fog nodes, and IoT devices.
- The key generator server is used to generate and distribute the keys among the involved entities.
- The cloud defines the access structure and performs the encryption to get ciphertext. We assume that the access structure is given to all fog nodes.
- The fog node carries a set of attributes that is defined by an access structure associated with the ciphertext.
- We assume that each fog node is associated with number of attributes that can be viewed as a meaningful string of arbitrary length.
In order to achieve the security requirements of the communications between fog nodes and the cloud, we propose an encrypted key exchange protocol based on CP-ABE.

We design a protocol such that each fog node is associated with a set of attributes. This feature enforces the decryption procedure based on the fog node’s attributes.

Each ciphertext carries an access structure such that the fog can decrypt the ciphertext and obtain the shared key only if it possesses the specified attributes in the access structure.

The protocol can be executed with the following algorithms: Setup, Key Generation, Encryption, and Decryption.
Algorithm 1 describes the system setup and is executed by the key generator server. It takes the security parameter $K$ as an input, publishes the public parameters $PK$ to all involved entities, and holds the master key $MK$.

Algorithm 2 is also performed by the key generator server to generate the secret key $SK$ that belongs to an entity specified by its set of attributes. It takes the public parameters $PK$, the master key $MK$, and the set of attributes to generate the secret key $SK$.

A shuffling process is introduced to mix both constellations and perform a separation between real and imaginary components.
The proposed protocol

- Algorithm 3 provides the details of the encrypted shared key $K$. It is executed by the cloud that takes as inputs the public parameters $PK$ and the access tree structure $T$. It outputs the ciphertext $C$ that contains the information.

- Algorithm 4 describes the decryption procedure to obtain a shared symmetric key. This algorithm is executed by each fog node, which takes as inputs the public parameters $PK$, the secret key $SK$, and the ciphertext $C$. Then, it outputs the information.
Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
In the proposed scheme, we employ CP-ABE and requires only a subset of the attributes for decryption. Since the secret key involves a unique random number for each attribute in the access policy, CP-ABE can defend against collusion attacks. Thus illegal users can not obtain the exchanged key.

An adversary who wants to create a valid signature of a legal user must possess the users private key. On the other hand, it is impossible for the adversary to create a new, valid ciphertext and signature from another users ciphertext and signature.
Outline

1 Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2 motivation

3 Network model

4 The proposed protocol

5 Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6 Conclusion
Communication overhead

- The cloud and fog nodes exchange the shared key, which can be transmitted between them when needed; thus the communication overhead is mainly related to the size of the ciphertext.
- The Key Generation phase does not involve any message exchange, and thus its communication cost is zero.
- In the Encryption phase, the cloud sends the ciphertext $CT$ and signature to the fog nodes. The Decryption phase involves no communication, and thus the cost is zero.
Outline

1. Introduction
   - Fog computing
   - Significant Threats
   - Security Requirements
   - Security mechanism

2. motivation

3. Network model

4. The proposed protocol

5. Analysis
   - Security analysis
   - Communication overhead
   - Comparison

6. Conclusion
Comparison

- we present a comparison study between our scheme and the traditional certificate-based scheme in terms of computational cost, and revocation issues.

- To evaluate the impact of the computational overhead in our scheme and the certificate-based scheme, we are mainly concerned about the cryptographic operations: encryption and decryption.

- In a certificate-based scheme, the computational cost takes 7201.3 ms. This cost is mainly due to the decryption operation that includes the verification phase for the certificates signature.

- The total computational cost is 638.9 ms. The major computational overhead occurred in the encryption phase due to the additional cost of the signature operation.
Comparison

- We use either the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) to check the certificates status and the certificates validity period.

- In fact, the most common revocation approach is the CRL which is required to download the CRL file to check the certificates status.

- The size of a CRL file can vary between a few bytes to megabytes depending on the number of the revoked certificates and thus it adds a storage overhead.

- In contrast, our scheme does not incur any transmission overhead because it does not need to exchange certificates or any identity information since the users attributes are associated with the private key.
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.

We analyze the security of our protocol and show its correctness.