Journal of Information Security and Applications 40 (2018) 156–165

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Multidimensional data tight aggregation and fine-grained access control in smart grid

Bo Lang[a,b], Jinmiao Wang[a,b,*], Zhenhai Cao[a,b]

[a] State Key Laboratory of Software Development Environment, Beihang University, Beijing 100083, China
[b] School of Computer Science and Engineering, Beihang University, Beijing 100083, China

ARTICLE INFO

Article history:

Keywords:
Smart grid
Multidimensional aggregation
Privacy preserving
Access control

ABSTRACT

In smart grid, for saving communication bandwidth and performing fine-grained analysis, the power data need to be collected and aggregated in multi-dimensions. As each dimension contains sensitive information of users and may be used by different analytic organizations, privacy preserving and access control for multidimensional power data are obviously important. Existing schemes either cannot support dimensional access control or require transmitting attribute sets of data together with ciphertexts, which leaks the relevant information of power data and increases the security risk. Moreover, to disseminate and implement access control of the multidimensional data, control center (CC) must firstly decrypt the data of all dimensions, which may result in the data leakage. In this paper, we propose a Multidimensional-data Tight Aggregation scheme which supports Privacy preserving and fine-grained Access control (MTA–PA). In MTA–PA, we import the extended Boneh–Goh–Nissim (EBGN) homomorphic encryption from wireless sensor networks to aggregate multidimensional power data into one ciphertext and simultaneously use key-policy attribute-based encryption (KP–ABE) to enforce fine-grained access control at the dimension level. By using MTA–PA, the gateway need not to distinguish different ciphertexts before aggregating them, and organizations only can analyze the authorized dimensions of power data. MTA–PA further achieves secure access-permission update via updating related parameters of EBGN and KP–ABE. And then, we also present the implementation methods of the algorithms. The security analysis and experimental results show that MTA–PA is a secure and efficient data protection scheme in smart grid.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

According to the investigations, both of the electrical blackouts respectively occurred in North America in 2003 and European in 2006 are due to load imbalance and lack of effective real-time diagnosis in power grid [1,2]. These incidents indicate that the traditional power grid no longer meets our growing demand for continuous stable electricity distribution. In this case, smart grid, which combines traditional power grid and information technologies, is considered as the next generation of power grid.

Unlike the traditional power grid which adopts one-way supply model, smart grid allows dual-way interaction between users and the power authority, as shown in Fig. 1. Smart meters (SMs) are responsible for collecting power data of users in an area and sending it to the control center (CC) periodicity. Then CC determines the real-time price and power-supply policies relying on the total demand, which balances the load and improves the stability of the smart grid. Since the power-supply policies are developed not based on each user's usage but on the total power demand in an area, power data should be aggregated at the gateway (GW) to reduce data redundancy and save communication bandwidth. Additionally, through comprehensive analyzing at analysis organizations (AOs), such as system engineers, auditors and researchers, etc., the power data may produce some other commercial values. Hence, based on the information collected and processed at SMs, GWs and AOs, smart grid can achieve more efficient and stable generation, transmission, distribution and utilization of power.

In order to perform fine-grained analysis, the power usage of each kind of electric appliance is needed. For example, by analyzing the power used by cooling equipment on an extremely hot day in summer, the power station can prepare enough power for the subsequent similar days. Therefore, the power data in smart grid are multidimensional in nature [3]. Before being transmitted to GW, the privacy of each dimension should be preserved because it may contain sensitive information about the users. For instance,

* Corresponding author at: State Key Laboratory of Software Development Environment, Beihang University, Beijing 100083, China.
E-mail addresses: langbo@buaa.edu.cn (B. Lang), wangjinmaio@buaa.edu.cn (J. Wang), caozhenhai@buaa.edu.cn (Z. Cao).

https://doi.org/10.1016/j.jisa.2018.03.008
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

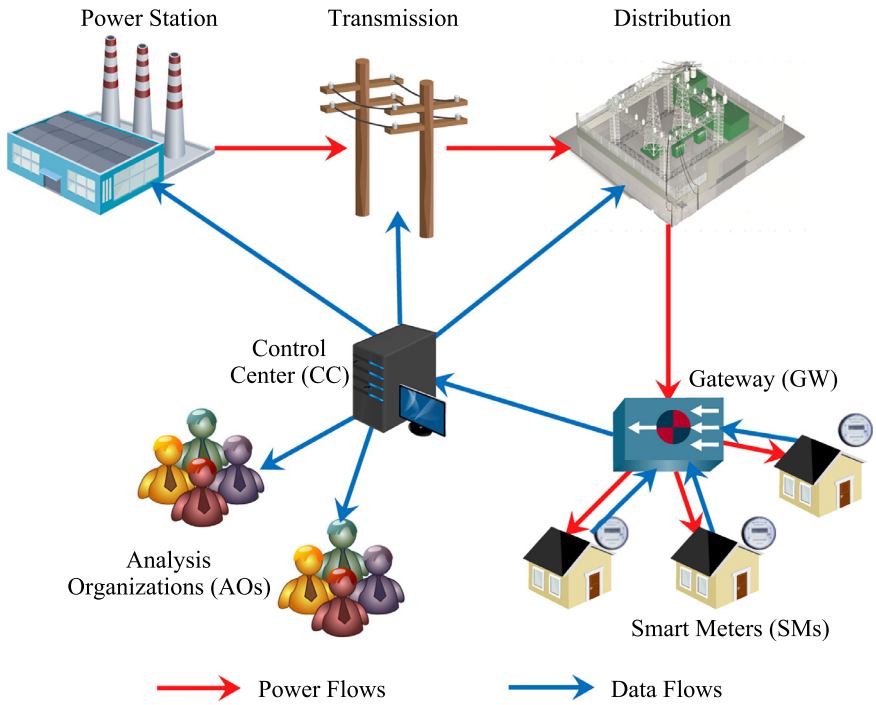

Fig. 1. Architecture of smart grid.

lack of power consumption from cookers indicates that the home owners are probably away from their house. Access control is another security challenge in smart grid. According to each AO's function, it only can be authorized to access some specific dimensions of power data. In practice, the access permissions of AOs maybe modified for some reasons. Hence, the update of access permission also should be considered for enforcing flexible access control.

Homomorphic encryption is an encryption technique such that some algebraic operations, such as addition and multiplication, toward the plaintext are equivalent to the counterparts conducted on the ciphertext. This feature allows GW to aggregate the power data without decrypting, which prevents GW from accessing users' data. Hence, homomorphic encryption is widely used in smart grid [3–9]. At present, although there are some schemes [3–7] focusing on multidimensional data aggregation, none of them can enforce access control on each individual dimension. Besides, to get the total power demand of an area, they require CC to decrypt all dimensions of power data, which increases both of the computation burden of CC and the risk of data leakage. The RN scheme [8] claimed that it achieved fine-grained access control as well as privacy preserving. However, it requires the remote terminal unit (RTU), which is like CC in Fig. 1, to decrypt all dimensions of power data and re-encrypt them with ciphertext-policy attribute-based encryption (CP–ABE), which means the access permission cannot be controlled immediately after the power data being collected in smart meters. And also, it introduces heavy computation burden to RTU and increases the risk of data leakage. Moreover, when processing multidimensional data, RN does not treat the dimensions as a whole; i.e., it has to separately encrypt every dimension that is identified by a set of attributes, pack the ciphertexts and send to GW, which is called *loose* aggregation. In order to allow GW to aggregate the dimensions with the same set of attributes, the attributes should be sent together with the ciphertext, which not only introduces some extra overhead to GW but also leaks sensitive information from the attributes. Therefore, there are still limitations in the existing data aggregation schemes regarding effective multidimensional data aggregation and fine-grained access control.

In this paper, we propose a Multidimensional-data Tight Aggregation scheme supporting Privacy-preserving and fine-grained Access control (MTA–PA). As a homomorphic cryptosystem, extended Boneh–Goh–Nissim (EBGN) is used in wireless sensor networks (WSN) [10]. We import EBGN to smart grid to encrypt the power data. By using EBGN, each dimension can be encrypted with a different public key and the multidimensional ciphertexts are fused to one ciphertext, which achieves *tight* aggregation. To further enforce access control, we use key-policy ABE (KP–ABE) to encrypt the private keys of EBGN. In KP–ABE, the user's private key is generated over an access policy and the ciphertext is encrypted with a set of attributes. If and only if the set of attributes satisfies the access policy, can the user decrypt the ciphertext. In our scheme, the relationship between an EBGN private key and an attribute set is fixed. Hence, the attribute set need not to send along with the ciphertext, which prevents the privacy leakage from the attributes. The KP–ABE scheme can revoke a single user's privilege at attribute level without affecting other users, which can be used to update the AOs' access permission in our scheme. To implement MTA–PA, we also present the implementation methods of the algorithms in our scheme. The main contributions of our work are summarized as follows.

- We import EBGN from WSN to achieve multidimensional data tight aggregation. Compared with RN, the attributes need not to be sent with the ciphertext and the encrypted data will not be decrypted at CC, which prevent the leakage of data and the attribute information and also lessen the burdens of CC. Besides, we optimize the encryption algorithm of EBGN, which significantly improve the encryption efficiency.
- By encrypting the EBGN private key of each dimension with KP–ABE, we realize fine-grained access control at dimension-level since the power data are collected by the smart meters. Additionally, we add one special dimension to record the total demand of an area and authorize its access privilege to CC; hence CC never needs to decrypt each dimension for getting this value, which not only restricts the privilege of CC, but also simplifies the operations.

Download English Version:

https://daneshyari.com/en/article/6884578

Download Persian Version:

https://daneshyari.com/article/6884578

Daneshyari.com