Smart Grid Data Security Aggregation Method Based on Fog Computing Architecture for Integrated Energy Services

Su Chang¹, Song Ge², Gang Yining³, Yao Zhenxian*¹

¹ Liaoning Electric Power Energy Development Group Co., Ltd., Shenyang Liaoning 110000, China
*Corresponding author’s e-mail: sg_eiconf@126.com

Abstract. Integrated energy systems incorporate new types of clean and distributed energy into the power grid. In the future, smart grid will emerge in the form of integrated energy services. However, the application of new technology inevitably brings the threat of privacy disclosure. To deal with this kind of information security, a smart grid data security aggregation technology based on fog computing architecture for integrated energy services is proposed in this paper. Real-time data is encrypted in the energy acquisition equipment to obtain the first layer of privacy protection, and fine-grained aggregation at the fog end to obtain the second layer of privacy protection, so as to achieve the confidentiality and privacy of the entire network data transmission and processing. Finally, the safety and performance evaluation shows that this technology has a great advantage over other schemes in terms of safety, practicability and efficiency.

1. Introduction
Integrated energy service technology is a new service model that can meet the diversified energy needs of users. On the basis of the traditional energy use model, integrated energy services can effectively integrate electricity, heat, natural gas and other energy types. At the same time, the technology combined with big data, fog computing, Internet of things and other new communication technologies. The coordinated supply of multi-energy comprehensive energy cascade utilization is realized, so as to improve the efficiency of energy system and reduce energy cost.

Integrated energy systems incorporate new types of clean and distributed energy into the power grid. In the future, smart grid will emerge in the form of integrated energy services. However, the application of new technology inevitably brings the threat of privacy disclosure. To deal with this kind of information security, a smart grid data security aggregation technology based on fog computing architecture for integrated energy services is proposed in this paper. Real-time data is encrypted in the energy acquisition equipment to obtain the first layer of privacy protection, and fine-grained aggregation at the fog end to obtain the second layer of privacy protection, so as to achieve the confidentiality and privacy of the entire network data transmission and processing. Finally, the safety and performance evaluation shows that this technology has a great advantage over other schemes in terms of safety, practicability and efficiency.

2. Fog computing framework for integrated energy services system
At present, cloud computing, with its powerful computing power and storage capacity, has become a supporting platform for many energy-consuming enterprises to analyze and process big data. At the same time, it is expected to become the future development trend of the Internet of things. However,
with the geometric growth of power network terminals, the realization capacity of cloud computing brings great challenges.

The concept of fog computing was proposed and defined in detail in 2011. Fog computing is an extension of cloud computing, and none of the weaknesses described above are available. In addition, IT equipment is mainly used in the edge network, data transmission has a very low delay. Fog computing is a large scale sensors network with a large number of network nodes. Fog computing has excellent mobility, mobile phones and other mobile terminals can be directly localized operations. Fog computing is not for high performance servers, but rather for distributed local computers. Compared with cloud computing, the architecture adopted by fog computing is more distributed and closer to the edge of the network. Fog computing concentrates data, data processing, and applications on devices at the edge of the network, rather than stores them almost entirely in the cloud, as cloud computing does, and the storage and processing of data is more dependent on local devices than servers. Fog computing is a new generation of distributed computing, in line with the decentralized characteristics of the Internet.

![Image](Figure.1. Integrated energy service system architecture based on fog computing architecture.)

3. Information security analysis of fog computing system

The fog computing framework for integrated energy services system was given above. This section analyzes the security threats to the above systems. There are three main threats to consider, as shown in figure 2.

1) **Threats on fog and cloud nodes:** Fog and cloud nodes are generally considered honest and trustworthy. They follow protocol and are trusted most of the time. But should not be neglected, and cloud fog node also has the possibility of captive, so the system must ensure that the fog and cloud nodes cannot obtain a single user privacy data plaintext, namely data nodes in mist and cloud cannot take the form of plaintext, and cloud and fog node cannot have the decryption key, so as to ensure the security of the system.

2) **Threat of eavesdropping on communication links:** Eavesdropping may acquire users' private data by eavesdropping on communication links, so the system must ensure that no private data plaintext of a single user appears in each communication link, that is, the data exists in the form of ciphertext in the transmission process of each communication link. The key generation center sends the decryption key to various terminals through a trusted channel. At the same time, the decryption key is not transmitted in the communication link from the terminal to the fog node. Therefore, eavesdroppers...
cannot eavesdrop on the decryption key. Through the above mechanism, even if the eavesdropping from the communication link eavesdropping information, also can not crack the user's private data.

(3) **Threat of active attack by the attacker:** In addition to passive attack by eavesdropping, the attacker can also carry out malicious injection by means of camouflage, thus damaging the authenticity and integrity of private data. Therefore, before the fog node or cloud node receives the data and performs the protocol operation, it must ensure that the data comes from the legitimate entity through the key negotiation authentication, as well as that the data is sent to the legitimate entity.

![Information security analysis of fog computing system.](image)

**Figure 2.** Information security analysis of fog computing system.

### 4. Data security aggregation technology

As integrated energy services rely on energy data from energy-consuming devices in the physical world, data are read at regular intervals from regional smart terminals. However, in the process of data reading and transmission, there is a certain risk of privacy disclosure. Therefore, a data security aggregation technology is adopted in this paper to ensure the privacy and confidentiality of data in the transmission process. The multi-granularity aggregation of fog layer and cloud layer can effectively reduce the amount of transmitted data and thus reduce the transmission consumption. The result of multi-granularity aggregation can also improve the flexibility of power dispatching.

**1. Key generation and distribution**

KGC first randomly selects two large prime numbers \( p \) and \( q \) to satisfy \( \gcd(pq, (p-1)(q-1)) = 1 \). The public key of homomorphic encryption \( N = pq \). Definition of \( L(u) = (u-1)/n \), and pick a random integer \( g \approx (g < N^2) \). We get the public key as \( (N, g) \) and the private key as \( (\lambda, \mu) \). The key generation center sends the same set of public key and private key to each smart electricity meter in the coverage area of the same fog node, and sends the corresponding public key to the fog node, and provides the public key and private key to the comprehensive energy service provider.

**2. Terminal data report**

In order to avoid exposing users’ private data to eavesdroppers in the “acquisition terminal-fog” communication link, this paper chooses to encrypt private data at the acquisition terminal. The data generated by the acquisition terminal is generally uploaded to the fog node periodically, assuming that the time interval is 15min. Then the acquisition terminal encrypts the real-time energy data every 15min, generates a signature on the encrypted data after the two parties of transmission complete the key negotiation, and sends the data report to the corresponding fog node, waiting for the fog node to
aggregate it. Suppose there are \( n \) acquisition terminals in a subregion. The information stored by the \( i \)th acquisition terminal \( SM_{ij} \) in this subregion is \( x_{ij} (0 < i < n, 0 < j < f) \). The \( SM_{ij} \) identity for a given user can be defined as follows:

\[
T_{SM_{ij}} = a_i P
\]  
(1)

\[
h_i = H_2 \left( T_{SM_{ij}} + ID_{SM_{ij}} + \text{nonce} \right)
\]  
(2)

\[
s = \left[ a_i \left( x_{SM_{ij}} + d_{SM_{ij}} + h_i \right) \right]^{-1} \mod m_p
\]  
(3)

And send a message to the fog node \( \text{fog}_j \), where \( \text{nonce} \) is the current timestamp. Then wait for the reply report of fog node \( \text{fog}_j \). If the reply report is a resend command, the key negotiation will be conducted again. And if reply report is \((ID_{\text{fog}}, h_3, s, \text{nonce})\), then it is determined whether the \( \text{nonce} \) in it is the timestamp issued by the previous acquisition terminal. At this point, the data coefficient satisfies

\[
\begin{align*}
K_{h_j} &= (X_{SM_0} + d_{SM_0} + a_j) X_{\text{fog}_j}, \\
K_{2_j} &= (X_{SM_0} + d_{SM_0} + a_j) P_{\text{fog}_j}, \\
K_{h_j} &= (X_{SM_0} + d_{SM_0} + a_j) T_{\text{fog}_j}.
\end{align*}
\]  
(4)

According to formula (4), \( K_1, K_2 \) and \( K_3 \) are calculated. If the fog node negotiation fails, the fog node \( \text{fog}_j \) is required to resend the validation message.

(3) Fog node fine-grained aggregation report

Directly uploading data from the explosive growth of acquisition terminals to the cloud will generate a large amount of transmission energy and increase the bandwidth burden, making it difficult to meet the needs of low delay transmission. Therefore, this section reduces the data flow at the core network by introducing the fog node, and further reduces the data volume by performing relevant calculations at the fog node, so as to reduce the energy consumption of data transmission.

Therefore, in the fog node, the data \( A \) encrypted in the user report sent by the coverage acquisition terminal is aggregated after multiplying the data in \( B \). Therefore, in the fog node, the data \( C_j = \{C_{b_{ij}}, C_{t_{ij}}, \cdots, C_{n_{ij}}\} \) encrypted in the user report sent by the coverage acquisition terminal is aggregated after multiplying the data in \( C_j \).

\[
\text{Sum}_j = C_{b_{ij}} \cdot C_{t_{ij}} \cdots C_{n_{ij}}
\]  
(5)

The cloud receives the encrypted and aggregated data from the cloud node within the coverage area of the cloud node. In order to achieve multi-granularity aggregation of the data in this region, the data obtained after the final comprehensive energy service provider decryption can be accurate to the fog node layer. In figure 3, the communication overhead from the acquisition terminal to the cloud node of the method presented in this paper is compared with the traditional PPUAC, SIG-ADD and PDAF. Similarly, the comparison of communication overhead between cloud node and integrated energy service provider is shown in figure 4. The results show that the proposed method is a lightweight multilevel aggregation scheme for private data and can effectively reduce the data transmission overhead.
Figure 3. Communication overhead from the acquisition terminal to the cloud node.

Figure 4. Communication overhead from the cloud node and integrated energy service provider.

5. Conclusion
To deal with information security of integrated energy services, a smart grid data security aggregation technology based on fog computing architecture for integrated energy services is proposed in this paper. Real-time data is encrypted in the energy acquisition equipment to obtain the first layer of privacy protection, and fine-grained aggregation at the fog end to obtain the second layer of privacy protection, so as to achieve the confidentiality and privacy of the entire network data transmission and processing. Finally, the safety and performance evaluation shows that this technology has a great advantage over other schemes in terms of safety, practicability and efficiency.

References
[1] Zijian Cao, Jin Lin, Can Wan, et al. Optimal Cloud Computing Resource Allocation for Demand Side Management in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(4):1943-1955.
[2] Mamadou Bilo Doumbouya, Bernard Kamsu-Foguem, Hugues Kenfack. Argumentation and graph properties[J]. Information Processing & Management, 2015, 52(2): 1561-1573.
[3] Ali Hadi Abdulwahid. A Novel Method of Protection to Prevent Reverse Power Flow Based on Neuro-Fuzzy Networks for Smart Grid[J]. Sustainability, 2018, 10(4) 1876-1885.
[4] Papaioannou T G, Hatzí V, Koutsopoulos I. Optimal Design of Serious Games for Consumer Engagement in the Smart Grid[J]. IEEE Transactions on Smart Grid, 2018, 9(2):1241-1249.
[5] Izudin Džafić, Rabih A. Jabr, Sylwia Henselmeyer, et al. Fault Location in Distribution Networks Through Graph Marking[J]. IEEE Transactions on Smart Grid, 2018, 9(2):1345-1353.