Research on smart grid access control based on CP-ABE

Wang Jun[1,*], Li Zhipeng[1], Dong Rui[1], Jia Yangfan[2], Yu Jun[2]

[1]State Grid Gansu Electric Power Company, Digital Division, Lanzhou, 730000, China
[2]Sichuan Zhongdian Qimingxing Information Technology Co., Ltd. Information Enterprise Platform Business Unit, Chengdu, Sichuan, 610000, China

Corresponding author email:wangjun17@lzu.ed

Abstract. Smart grid is a new power system based on information technology, which combines traditional power grid with communication, computing and other technologies. The rapid development of smart grid poses new challenges to the security and privacy protection of power grid. Access control is one of the key technologies to protect smart grid systems from unauthorized access and data breaches. Traditional access control models often fail to meet the needs of smart grids, so converged attribute based encryption (CP-ABE) technology becomes a promising solution. This paper proposes a smart grid access control scheme based on CP-ABE. Firstly, the smart grid entities are divided into three roles: user, data owner and data user, and the corresponding policies and permissions are defined. Then, CP-ABE technology is introduced into the access control system to precisely control the user's access rights to data by defining attribute sets and access policies. At the same time, in order to improve the efficiency and scalability of the system, a storage method based on hierarchical structure and index is used. The experimental results show that the CP-ABE integrated smart grid access control scheme can effectively protect the data security and privacy in the smart grid system, and has high efficiency and scalability. This scheme can provide reliable access control guarantee for the practical application of smart grid system.

keywords: CP-ABE; Smart grid; access control

1 Introduction

With the progress of information technology and the rapid development of smart grid, smart grid system has become an important part of modern power system. However, the smart grid system is faced with increasingly serious security and privacy protection issues. As a key technology to protect systems from unauthorized access and data breaches, access control is critical to the security of smart grid systems [1]. In order to solve the above problems, the researchers began to explore the possibility of incorporating attribute based encryption (CP-ABE) technology into smart grid access control. CP-ABE technology is an attribute based encryption scheme, which can control the user's access to encrypted data according to the set of attributes [2]. Compared with the traditional role-based access control model, CP-ABE technology is more flexible and

B. K. Kandel et al. (eds.), *Proceedings of the 2023 8th International Conference on Engineering Management (ICEM 2023)*, Atlantis Highlights in Engineering 23,
https://doi.org/10.2991/978-94-6463-308-5_45

refined, and can achieve fine-grained access control over data. The purpose of this study is to explore the smart grid access control scheme with CP-ABE and evaluate its applicability and effect in smart grid systems.

2 Access control mechanism based on CP-ABE

2.1 Access control model

Typically, the RTU collects data and sends it to the SCADA/EMS, which consists of a control center and a data center [3]. The distributed access control architecture of this paper, as shown in Figure 1, consists of four subjects, namely control center (CC), RTU, data center and user, as follows :(1) CC. Based on the practical application of smart grid, the control center is trusted and responsible for the distribution of attributes and users' private keys. (2) RTU. The RTU of the sub-station sends the collected data to the data center. Only the RTU can create, update, and delete data files, and other users only have the read permission. (3) DataCentre. DataCentre is distributed in different areas and consists of data service managers and databases. The DSManager is semi-trusted and runs programs and related access protocols faithfully, but it may be curious about data content. The database is only responsible for storing the corresponding data file. (4) User. The User can access the corresponding data file only when the access conditions are met. It is assumed that the communication channels between all participants are secure.

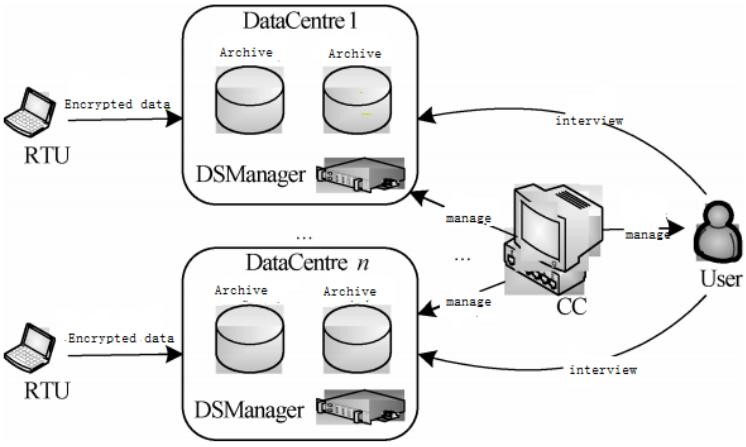

Fig. 1. Distributed access control model of smart grid

2.2 The construction of the scheme in this paper

(1) Establishment of the system.

The control center CC selects a doublet group G of order p, the generator G, and then selects a, b ∈ RZ*p. Public parameters and the master key is respectively: PK = {beta G, G, h = G, f = g1 beta, e (G, G)} and MK = {alpha beta, G}.

(2) Key generation.

The key generation phase consists of the property key (user private key) generated by CC and the path key generated by DSManager. The two algorithms are as follows :(1) The user private key generation algorithm inputs user set U and attribute set λ, and the algorithm outputs the private key SKt corresponding to attribute set Λ⊆λ of each user ut∈ U. CC randomly selected ∈ r Z ∗ p (different) each user, for each attribute lambda I ∈ Λ randomly select ri ∈ Z ∗ p, then generate ut per user private key, finally will SKt sent to the user through the security channel ut: SKt = (D = g (alpha + r)/beta, ∀ lambda j ∈ Λ : Dj = gr h. (lambda j) rj, Dj '= GRJ) CC The attribute group λi for each attribute λi is sent to the DSManager. Such as user u4, u5 and u6 attribute sets are respectively 2} {1, lambda lambda, {1, lambda lambda. 2, lambda 3} and {lambda 1, 3} lambda, the corresponding attribute group for U lambda. 1 = {u4, u5, u6}, U lambda = {u4, u5} and U 2 lambda 3 = {u5, u6}. (2) Path key generation algorithm First, DSManager constructs a binary tree -- KEK tree (as shown, where the arrow represents the access path; Dashed lines represent users linked to leaf nodes.), leaf nodes represent each user in U; Secondly, a random number KEKj ∈ Z*p is assigned to each node vj. The set of random numbers corresponding to all nodes between the root node of the tree and user ut is defined as the path key PKt, for example, the path key of user u4 is PK4= {KEK1, KEK3, KEK6, KEK10}. The DSManager sends the PKt to the user ut over a secure channel

(3) Data encryption.

Data encryption consists of two parts: RTU encryption of data and DSManager re-encryption of received ciphertext. The details are as follows :(1) Before ciphers generate RTU to transmit data M, an access tree T is defined according to attribute set λ, and each leaf node of the tree represents an attribute. Let kx=1 be the threshold for each node in T, and choose a polynomial q of degree KX-1 for node x. Randomly select s∈Z*p, for the root node R, let qR(0)=s; For non-root node x, let qx(0) = qparent(x)(index(x)), and index(x) return the sequence number of node x in its sibling node. Suppose Y is the set of all leaves, then the ciphertext of M is: CT= (T, C~=Me(g,g)αs, C=hs, ∀y∈Y: Cy=gqy(0), C 'y =H(λy)qy(0)) After constructing ciphertext CT, it is sent to DSManager through secure channel. (2) Re-encryption After receiving ciphertext CT, the DSManager uses the member information of the attribute group to carry out the following re-encryption: For the attribute group Uλy corresponding to each attribute y∈y, Kλy∈Z*p is randomly selected as the group secret key of Uλy, and the calculation is :CT '=(T,C~=Me(g, g)αs,C=hs, ∀y∈Y:Cy=gqy (0), C 'y =(H(λy)qy(0) Kλy) In the KEK tree, find the smallest subtree that can cover all users in the Uλy, and define the random number corresponding to the root node of these subtrees as the path key of the attribute group Uλy, denoted as KEK(Uλy). The attribute group Uλy={u4, u6, u7}, the root node of the smallest subtree that can cover users u4,u6 and u7 in the KEK tree is {v10,v7}, so the path key of Uλy is KEK(Uλy)={KEK10,KEK7}, that is, only users in Uλy have permission to know KEK(Uλy). Encrypting the group key with the symmetric encryption algorithm E and the path key of the attribute group generates

the header message as follows: Hdr=(∀y∈Y: {EK(kλ y)}K∈KEK(Uλy))DSManager saves (Hdr, CT ') in the database.

(4) Data decryption.

To access data M, the User first decrypts the header message Hdr to get the group key, and then decrypts the ciphertext CT 'to get M. The specific process is as follows :(1) Decrypt the group key When a User initiates an access to data M to the DSManager, the DSManager returns to ut (Hdr, CT '). Set the valid attribute λj of ut, then ut uses KEK∈KEK(Uλj)∩PKt to decrypt Hdr to obtain the attribute group Uλj key Kλj. If attribute group Uλ1={u4,u6,u7} and path key is KEK (Uλ1) = {KEK10, KEK7}, path key PK4 of user u4 ={KEK1,KEK3,KEK6,KEK10}, therefore,u4 can decrypt Hdr using KEK10∈KEK(Uλ1)∩PK4 To lambda 1 K, then update the private key: SKt = (D = g (alpha + r)/beta, ∀ lambda j∈Λ : Dj = gr h. (lambda j) rj, D 'j = (GRJ) K1 lambda j) (2) data decryption user DecryptNode ut first define a recursive algorithm (CT', SK, x), computed tomography (CT) 'is a cipher, SK is Λ shut with attribute set The associated private key, x is the node of tree T. When x is a leaf node, perform the following: DecryptNode CT ', SK, (x) = e (Cx) Dx, e (D 'x, C' x) = e (g, g) RQX (0) lambda x ∈ Λ, ut ∈ Gx otherwise {coming when x is a leaf node set x child node sets {what zj had}, j p kx; Calculate the corresponding Fzj= DecryptNode (CT ',SK, zj)=e(g, g)rqzj(0) for each child node zj, and then choose the Fzj of the kx child node as the interpolation node of the Lagrange interpolation polynomial for calculation :Fx=∏z∈SxFΔi, S 'x(0)z=∏z ∈Sx(e(0) G, g) RQZ Δ I (0)), (0) = ∏ S 'x z ∈ x (e, g, g) rqparent (z) (index (z))) Δ I, S' (0) = ∏ z∈x Sxe RQX (g, g) (I) Δ I, S 'x (0) = e (g, g) RQX (0), I = inedx (z), S' X = {index (z) : z∈x}, for the root node R, set A = DecryptNode CT ', SK, (R) = e (g, g) rs, ut unlock: C ~ (A) (C, D) e = C ~ (e (hs, g (alpha + R)/beta) e (g, g) rs) = M

2.3 User authorization

If some users do not have access to DataCentre, they can authorize other users to access the datacentre. Assume that Ud has authorized user attributes Λ ~ ⊆ Λ, Ua authorized user private key for SKt = (D, ∀ lambda j∈Λ : Dj, Dj '), random selection of r $_k$ and r, ∀ k∈Λ , generate a new key:

$$SK_d = (\widetilde{D} = Df^{\tilde{r}}, \forall \lambda_k \in \tilde{\Lambda}: \widetilde{D}_k = D_k g^{\tilde{r}} \cdot H(k)^{\tilde{r}_k}, \widetilde{D}'_k = D'_k g^{\tilde{r}_k})$$

Since the algorithm re-randomizes the key, the key is equivalent to the private key received directly from the CC.

3 Scheme analysis

3.1 Security analysis

Theorem 1 This scheme provides resistance to collusive aggression. Proof: Suppose that only some attributes of each unauthorized user meet the access structure, and when multiple unauthorized users conspire, their attributes meet the access structure tree T, but when the private key is generated, each user's r is different, then each user's D 'i =grH(λi)ri is different, so each unauthorized user can only calculate the value e(g, g)r at the corresponding node x qx(0), but cannot calculate e(g, g)rs, so the attacker cannot decrypt CT 'to get M. Therefore, the scheme in this paper has anti-collusion aggression[4].

Theorem 2 This scheme guarantees data confidentiality. It is proved that :(1) the attacker does not have the corresponding attribute set that satisfies the access structure tree T, and cannot calculate e(g, g)rs and C~=Me(g, g)αs to obtain data M, so the data ciphertext is secret; (2) If the attacker does not have the attribute λi, then the group key Kλi of the attribute group Uλi is a random number, so the key is also secret; (3) It is also impossible for an attacker to obtain the group key from the header message by deciphering the AES symmetric encryption scheme. In summary, the scheme guarantees the confidentiality of the data.

Theorem 3 The scheme in this paper has both backward and forward confidentiality. It is proved that when a new user joins the attribute group Uλi, the updated group keys K 'λi and e(g, g)α(s+s') are obtained, but the previous group keys K 'λi are not known, and s' is random, so e(g, g)αs cannot be calculated, so the scheme has backward security. When a user's permission changes, DSManager changes the ciphertext group corresponding to s to the ciphertext group corresponding to s'. Therefore, when the user leaves the attribute group, he does not know the new group key K 'λi and only knows e(g, g)αs, but not e(g, g)α(s+s'). Therefore, this scheme has forward security.

3.2 Comparison and analysis

The proposed scheme is compared with the traditional scheme in terms of functionality and calculation times, as shown in Table 1 and Table 2 respectively.

Table 1. Functional comparison

option	store	Single bottleneck problem	accredit
Traditional scheme	concentrate	Work out	No
This scheme	distributed	Work out	There are

Table 2. Comparison of RTU calculation times

option	multiplication	Power reference	Pair operation
Traditional scheme	4n+1	5n+1	1
This scheme	1	2n+2	0

This scheme uses the idea of cloud computing for regional decentralized storage to solve the storage problem of massive data, improve the access efficiency, and ensure the availability of the system in time and space, while the traditional centralized storage pool will reduce the access efficiency. This solution uses a CC and multiple DSmanagers to coordinate work, solving a single bottleneck problem, while referring to the idea of authorization, solving the problem that users are inconvenient to access data directly, and facilitating flexible access to data, while the traditional solution does not provide this function. In the case of data encryption and user authority revocation, all the traditional work is completed by RTU, which increases its calculation and communication burden. In this scheme, the re-encryption work and user permission revocation are transferred to DSManager to complete, so the computation, communication and permission management cost of RTU are reduced. Because the smart grid uses many smart terminals and wireless transmission, it is necessary to save computing and communication. The addition operation is relatively inexpensive, so only multiplication, exponentiation, and comparison of operations are performed, assuming a total of n properties. The experimental environment of RedHatEnterpriseLinux6.2 built on the virtual machine of VMwareWorkstation was allocated 1GB memory, and the experimental code was written based on cpabe-0.10 library [5]. The encryption time increases linearly as the number of attributes increases. The communication for this scenario includes from RTU to DataCentre and from DataCentre to User. The ciphertext transmission from RTU to DataCentre requires (2+n)|G|+n(|H|+|si|)bit, where n indicates the number of attributes. |H| indicates the length of the hash result; |si| represents the secret value for each leaf of the access policy tree T. From the DataCentre to the User in addition to the ciphertext CT 'Hdr, and header to (2 + n) | | G + n (| H | si | | + + | | Ek) bit, the size of the | | Ek for symmetric encryption. So, the total traffic is 2(2+n)|G|+2n(|H|+|si|)+n|Ek|. Smart grid data files are generally relatively small, and this scheme is effective. When the data file is relatively large, the CP-ABE algorithm is not suitable for encrypting large data files due to its complexity. Therefore, the symmetric encryption key can be used to encrypt the data file to obtain the ciphertext, and then the symmetric key can be encrypted using the CP-ABE algorithm with a fixed ciphertext length to obtain the key ciphertext. Then the user can decrypt the key ciphertext and data ciphertext to obtain the data file.

4 Conclusion

This research is based on CP-ABE integrated smart grid access control scheme, aiming to solve the security and privacy protection problems in smart grid system. By introducing CP-ABE technology, the research realizes the authority management and data access control of different entities in smart grid system. The scheme can achieve fine-grained data access control and protect the data security of the system and the privacy of users by precisely defining the attribute set and access policy. The experimental results show that the smart grid access control scheme with CP-ABE is efficient and scalable. This scheme can quickly and effectively deal with the complex access control requirements in smart grid systems, and keep the computing and communica-

tion overhead low. At the same time, the scheme can also adapt to smart grid systems of different sizes and complexity, and still maintain good performance in large-scale data storage and access scenarios. In addition, CP-ABE integrated smart grid access control scheme is of great significance for the practical application of smart grid system. It can provide reliable access control guarantees for smart grid systems, prevent unauthorized data access and disclosure, and enhance system security and privacy protection. The scheme also provides a feasible technical support and solution for the further development of smart grid system.

Reference

1. Chen T, Ren Z, Yu Y, et al. Lattices-Inspired CP-ABE from LWE Scheme for Data Access and Sharing Based on Blockchain[J]. Applied Sciences,2023,13(13).
2. Yao Y, Chen H, Shen L, et al. A CP-ABE Scheme Based on Lattice LWE and Its Security Analysis[J]. Applied Sciences,2023,13(14).
3. Yilong L, Shengwei X, Ziyan Y. A Lightweight CP-ABE Scheme with Direct Attribute Revocation for Vehicular Ad Hoc Network. [J]. Entropy (Basel, Switzerland),2023,25(7).
4. Hun K C, Hyun G K. Strategies for sensing innovation opportunities in smart grids: In the perspective of interactive relationships between science, technology, and business[J]. Technological Forecasting & Social Change,2023,187.
5. Mojtaba M, Turaj A, Farrokh A, et al. Coordinated expansion planning of transmission and distribution systems integrated with smart grid technologies[J]. International Journal of Electrical Power and Energy Systems,2023,147.