Wuhan University
Journal of Natural Sciences

2022, Vol.27 No.3, 231-239

Article ID 1007-1202(2022)03-0231-09

DOI https://doi.org/10.1051/wujns/2022273231

Fine-Grained Access Control Mechanism of Energy Internet

☐ **MIAO Siwei[1], ZHANG Xiaojuan[1], LIU Zhe[2†]**

1. China Electric Power Research Institute, Beijing 100192, China;

2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, Hubei, China

© Wuhan University 2022

Abstract: The Energy Internet has generated huge amounts of information on the production devices, transmission devices, and energy consumption devices. The leakage of data in the collection, transmission, and storage process will cause serious security problems. The existing Energy Internet security methods rely on traditional access control mechanisms and specific network boundary defense mechanisms, which has the limitations of static strategies and coarse design. We combine the advantages of role-based access control (RBAC) and attribute-based access control (ABAC), and propose a trusted Energy Internet fine-grained access control model based on devices' attribute and users' roles. We have not only achieved fine-grained Energy Internet resource allocation, but also ensured that the access control process is related to the security status of the environment in real time. Experimental results show that the access control model can safely and accurately execute access decisions in the Energy Internet scenario, and the processing performance is more stable.

Key words: Energy Internet; attribute-based access control (ABAC); access control; trusted computing

CLC number: TP 391

Received date: 2021-11-28

Foundation item: Supported by the State Grid Corporation of China Science and Technology Project Funding

Biography: MIAO Siwei, female, research direction: electric power network and information security. E-mail: miaosiwei@epri.sgcc.com.cn

† To whom correspondence should be addressed. E-mail: 2016102110052@whu.edu.cn

0 Introduction

Human economic and social activities are inseparable from the production and consumption of energy. Therefore, ensuring energy security and high-quality development is the long-term strategy of the country. By closely combining the progress of energy technology and Internet technology, a new model of Internet + Smart energy [1] was born, which undoubtedly led the profound revolution in the field of energy production and consumption, and had a broad market prospects.

Energy Internet uses advanced sensors and software and hardware applications, connecting the manufacturing equipment, transmitting entity equipment and consumer equipment system [2,3], generating huge information data during the operation of the equipment. These data contain a large amount of sensitive information (e. g., voltage data somewhere in the smart grid) and very important privacy information (including user identity information and location information, etc.) [4]. Energy Internet decentralized infrastructure and diversified application requirements significantly increase the risk of data leakage [5,6] in Energy Internet systems, so it is very necessary to protect data collection, transmission and storage on the Energy Internet.

In April 2015, the Swedish Transport Authority granted management and service authority to outsourcing companies when it sent the database to the cloud, leading to disclosure of top military secrets [7]. In November 2016, the light rail system in San Francisco was hit by ransomware. In that same year, an online database of a digital electronics company was hacked, causing much leak private information [8]. In July 2017, senior power

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

company employees were suffered to spear phishing attacks [9] via fake email. These cases show that network attack or failure of Energy Internet networks will lead to failure of monitoring, control and disclosure of privacy information, affecting the safe and stable operation of Energy Internet networks. Identity authentication and access control are the main way to protect Energy Internet security and privacy[10]. Aiming at the problems of resource data leakage, unreliable operation, low validity of authority management mode and serious harm of internal attack in Energy Network control security mechanism, a trusted Energy Network control method based on user terminal attributes and roles is proposed. The main contributions of this article are as follows:

1) Use USB Key as the external trusted root to obtain device use permissions through dual-factor authentication. While using the password, the user needs to complete the master authentication of the USB Key equipment through the PIN code, and add the security status of the user and the terminal into the formulation and execution of the permission allocation policy. The dual factor authentication mechanism ensures that even if the terminal is physically damaged, there is no risk of being used or data compromised.

2) The traditional access control models have some problems such as low static policy correlation flexibility and coarse granularity of role management. Combined with the two advantages of role-based access control (RBAC) and attribute-based access control (ABAC), user attributes and terminal attributes are taken as key elements of dynamic permission allocation, and an improved trusted Energy Internet access control model is put forward to achieve dynamic access authorization.

3) Realize the prototype system of reliable Energy Internet access control method based on devices' attribute and users' roles, and experiment the access control function and performance of the system to verify the feasibility of this model.

1 Related Work

The Internet of Things (IoT) , the foundation of the Int Identity authentication technologies and access control technologies, can avoid network violence such as illegal intrusion, while secure communication between devices can avoid sensitive data leakage[11,12]. Due to the particularity of the Energy Internet, in addition to the need for security and privacy, the access control should take into account scalability, flexibility and lightweight to fit the Energy Internet environment. Traditional access control strategies include autonomous access control policies such as discretionary access control (DAC), forced access control policies such as mandatory access control (MAC), and role-based access policies such as RBAC.

In the autonomous access control model, the subject will restrict access to the object resources based on the permissions set by the administrator. However, due to the waste of storage space and the increase of the complexity index of access control table caused by the excessive user resources, the DAC cannot guarantee the effectiveness of the authorization process, which increases the operation difficulty of the model permission management.

In the forced access control model, the subject and object resources each maintain a security attribute, and the model determines whether to make access authorization based on matching both security attributes. However, with the increase of the complexity of resources and access subjects, the unified calculation standard and the increased allocation range of security attributes cannot be effectively solved in real-world scenarios.

In the role-based access control model, the system will implement access operations to the resource based on the set of permissions corresponding to the roles assigned by the user[13-15]. However, in the face of untrusted access agents, RBAC only considers the true legitimacy of its identity, so the model cannot guarantee the security of resource data with the allocation of static role permission sets and cannot dynamically and efficiently control when security requirements change during the access operation.

Due to the complex users, network environment, data flow and application flow within the Energy Internet system, it is very vulnerable to malicious attacks from different network locations, resulting in adverse consequences such as key privacy data leakage and abnormal termination of services. Traditional access control mechanism has been unable to deal with a large number of users, complex resource types and flexible Energy Internet environment. At the same time, the current Energy Internet information system access control mechanism lacks security assessment of the network environment, and cannot guarantee the credibility of the access terminal and the whole Energy Internet environment for accurate judgment and continuous monitoring.

The attribute- based access control concept can solve the access authorization problem of massive access subject and resource data in large-scale distributed complex systems [16-18]. Based on the principle of minimum permissions, combining the user role, resources, operation, environment context and other elements, this paper flexibly combines the attributes of the access requester to form a collection of access permission attributes and realize the dynamic authorization function.

2 System Design

In the Energy Internet system, when the user can access the resources through the terminal network, the user, the terminal and the access context environment will all pose security risks to the security of the access resource process. The design principles of the Energy Internet access control model based on user terminal attributes and roles are as follows:

1) Separate the user from the terminal. In the Energy Internet system environment, the user makes a resource access request to the server by using the terminal, so the terminal should also act as a logical object and have the relevant attribute characteristics.

2) Use the properties of the entity object as the key element to assign permissions. Role permissions and user roles are assigned comprehensively by their own attributes, environmental attributes and trust level, and security attributes of the role, then a security access model with fine-grained, high flexibility and strong security is formed.

The trusted Energy Internet access control model is shown in Fig. 1.

The trusted Energy Internet access control model based on user terminal attributes and role consists of three main parts:

1) Entities: A collection of all objects involved in the Energy Internet access control model, including accessing the user U, terminal device D, role collection R, session collection S, permission collection P, administrator collection A, and the system resource collection SR;

2) Entity Properties: Access to a collection of attributes associated with the access control model, where user entities, terminal entities, role entities, administrator entities, and system resource entities also have different subsets of basic attribute characteristics: (i) Basic Properties attribute trust rating (ATT). User entities, terminal entities, and role entities all have their own collection of basic attributes, which are expressed as (attribute name, operator, attribute values). (ii) Level of Trust (TL). User entities and terminal entities have trust rating attributes, including historical level of trust (HTL) rating and current trust assessment rating TL, and TL will be affected by HTL. (iii) Access Security Level (ASL). Role and resource entities have access security levels that ensure confidentiality of resources during user access under the

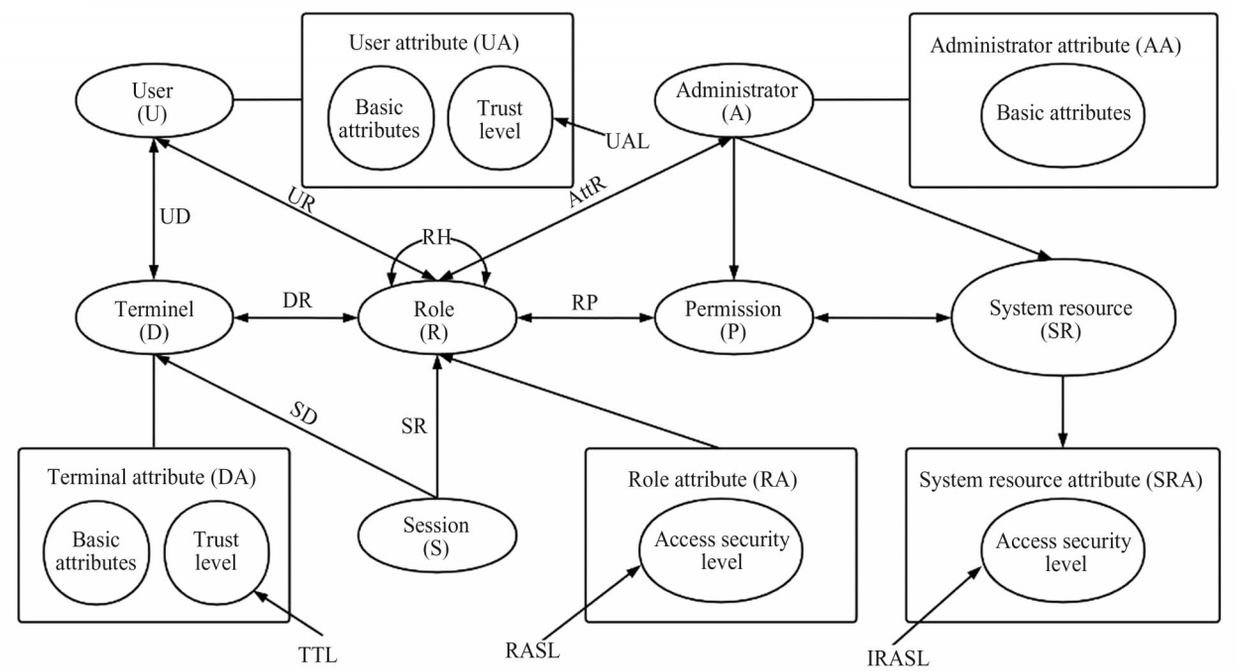

Fig. 1 Trusted access control model for Energy Internet

role mapping.

3) Inter-entity relationship: Access control policies between entities are implemented through joins and mappings between collections. The operations include user terminal device binding, user role assignment, role permission assignment, role inheritance, user trust level assignment, terminal trust level assignment, role security level assignment, system resource security level assignment, attribute role mapping management, terminal session mapping management, and role session mapping management.

3 System Implementation

3.1 User Identity Authentication

Existing Energy Internet access control mechanisms do not ensure the data confidentiality of Energy Internet sensitive resources during the execution of access operations during the complex network terminal access. In this part, from the perspective of identity authentication, we design the authentication mechanism to realize the most basic authentication control operation in the authority management model.

By using USB Key in authentication, users can bind terminal access permissions to external trusted roots in combination with two-factor authentication. Based on the PIN code verification function, the access to the USB Key device is obtained only if the PIN′ input meets Hash (PIN′) =Hash (PIN); otherwise the verification fails, and the user access is denied. Subsequently, the user inputs authentication information including the user name UN′ and password UP′, and signs the device serial number UK′ and the user authentication information after packaging to sign (UK′, UN′, Hash (UP′)) sent by the trusted terminal to the security authentication center to complete the remote user authentication process in the authentication center. By using the PIN code to generate a user-controllable encryption key and sign sensitive information, the integrity and non-tamperability of the information during the communication with the certification center are guaranteed.

3.2 Access Policy Management

Figure 2 shows the access control policy of the Energy Internet in details. The access implementation process of the trusted Energy Internet mainly includes three main processes, which are described as follows.

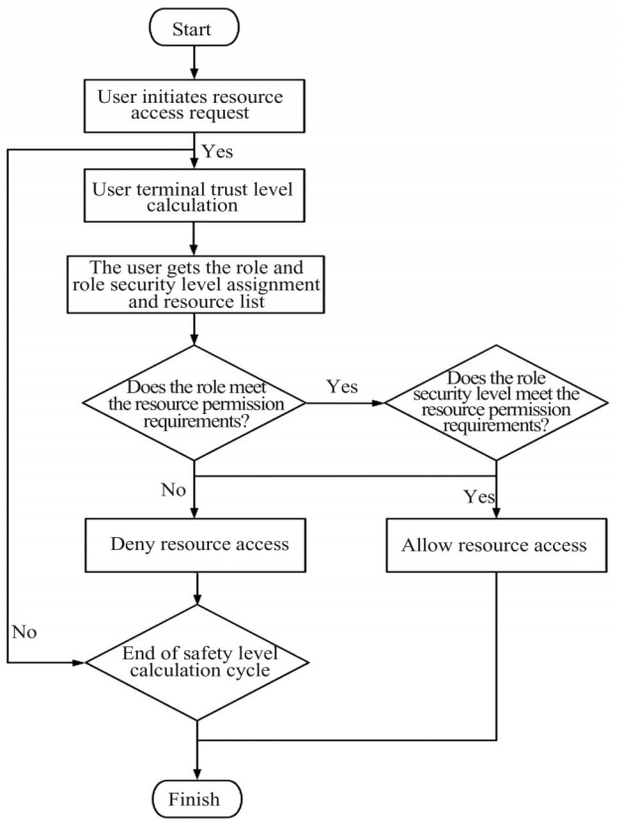

Fig. 2 The access control policy of the Energy Internet

1) Resource access policy management

In the Energy Internet, the access system presets the model policy table items stored in the database in the trusted authorization center, and the attribute structure of the model entities is recorded in the form. User access rights with different access security levels will also change accordingly. The Trusted Authorization Center assigns user role and access security level according to user terminal attributes to perform fine-grained dynamic access control, and the access control policy table is encrypted to the trusted server and policy when the user requests access.

2) User access request resolution

After the user completes the USB Key device authentication, the trusted terminal will collect the terminal hardware equipment information using the OSHI tool. In order to realize the flexible allocation of user rights and the real-time evaluation of the trusted terminal status at the same time, the trusted terminal will also continue to collect and analyze their own attributes.

3) Access control policy execution

After receiving the authorization request, the authorization request of the Security Certification Center conducts role permission assignment and user access per-

mission management according to the basic attributes and trust level collection of the user terminal. When the user initiates the access request, it performs the trusted Energy Internet access control policy based on user terminal attributes and role, and realizes the association between Energy Internet resource rights and user terminal trust level through the access control policy table.

4 Model Feasibility Analysis

In order to analyze the realization effect of the access control method, we design two access scenarios that are described as follows. The access control effect under the original problem scenario is compared with that under this method, so as to complete the feasibility analysis of improving the access model under the trusted network.

1) When the user initiates the access request using the terminal, user password is at the risk of being stolen and the terminal may be at security risk.

In the system, assuming the user U accesses the network using the trusted terminal T and completes identity authentication through the user name UN and password UP, and the access system simply assigns the corresponding role R directly according to the user identity UID. At this time, if the user password up is stolen or the terminal T itself has a security risk, after the system completes authentication and allows the terminal access, the user will obtain access to all energy Internet resources corresponding to the policy assignment role R. Only depending on the role granularity to allocate permissions, there is a great risk of illegal access, which will bring security risks to the confidentiality of energy Internet resources.

In a trusted Energy Internet based on the user terminal attributes and role, the user U must first access the trusted terminal T, with the Energy Internet using the user name UN, password UP and the PIN code of the USB Key device. At this time, due to no access to the USB key device, the authentication fails even if the user password UP was stolen. Thus, the access system will deny illegal user access and role permissions.

When a legitimate user U initiates an access request in the Energy Internet using a terminal T with certain security risks, the attribute information is collected to the user terminal by the trusted terminal building process, and signed by the trusted root to the trusted level Users Level of Trust (UTL) and Terminal Level of Trust (TTL) of the user terminal. The trusted authorization center will calculate the credibility level based on the basic and security attributes of the user terminal. The trusted authorization center can get the access security level assignment of the corresponding role. In this case, the higher the user terminal's trust level is, the higher the role access security level is.

In the user-terminal-role access allocation policy, the higher the permission of energy Internet resources, the lower the confidence of high-risk terminals and the lower the access permission. The user role assignment is related to the current access security level. When this security level exceeds a threshold, the Energy Internet access system will revoke the user's role assignment and reject access requests made by the user U using the terminal T'.

Therefore, the improved role-based access system refines the role-based access control, and adds the security status of users and terminals to the formulation and execution of permission allocation policies. The more secure user access environment, the more advanced access he can obtain in the role, which can enhance the security of resource access allocation in the Energy Internet.

2) During the user's access to system resources, the security status of the user and the terminal may change.

In the original Energy Internet, suppose the legitimate user U uses the terminal T to access the Energy Internet and perform intranet resource access operations. During the access process, the user, the terminal and the security status have changed. For example, users carrying trusted terminals leave the Energy Internet or terminals suffer cyber-attacks and vulnerability threats. In this case, due to the static association of user roles and permissions in a role-based access control policy, the Energy Internet access system still allows users to perform access operations using the access rights policies corresponding to the assigned role. In the process of system response to user access request, the risk of Energy Internet data leakage cannot be avoided.

In the trusted Energy Internet based on the user terminal attributes and role, it is assumed that the legitimate user U uses the terminal T to access the Energy Internet and conducts the intranet resource access operation, while the terminal T suffers malicious attack, and the basic attributes and security attributes of the user and terminal change. The trusted Energy Internet access control system continuously monitors the user terminal attributes, and the authenticity and credibility of the attribute

information is guaranteed by the external trusted root device. At the same time, in the next security level calculation cycle, the trusted authorization center recalculates the user terminal credibility level UTL and TTL and the role access security level ASL, develops a new Energy Internet access policy table based on the role security allocation security threshold, and dynamically adjusts the user access rights.

Therefore, the Internet access system of trusted energy in this paper improves the process of authority allocation between user role attributes and roles. This process ensures that the resource access control process is linked to the security status of the Energy Internet environment in real time. Simultaneously, the Energy Internet resource authority allocation is flexibly adjusted according to the access environment, and ensures the confidentiality of sensitive resource data of the Energy Internet.

5 Experiment and Discussion

5.1 Implementation

The system is developed in Java language, development tool is Eclipse IDE for Java EE Developers (64-bit) 4.5.1, development environment uses Java Development Kit 8, running environment is Java SE Runtime Environment 64 bit.

The experimental environment contains four hosts, three of which are Energy Internet Access trusted terminals, and one is a resource access server. This server provides multiple trusted services, including the security certification, the trusted authorization, the trusted storage, etc. The LAN is formed through the network cable and switch connections.

5.2 Access Policy Testing

According to the implementation described in Section 3, we build a trusted network control system with access control model deployed. According to the actual scenario requirements of the power grid, the model has two main functions: dynamic access control and security access control to implement the access control policy. In the process of dynamic access control, the user access authentication mechanism is preliminarily realized by designing the actual authentication control scenario. In the security access control function, the focus is changed from the implementation of one scenario to the analogy analysis of multiple security scenarios. Based on the different scenarios above, we analyze the initial implementation of access control function and the subsequent dynamic security respectively. Details are as follows:

1) Dynamic access control

The legal user using the dual factor identity authentication and platform integrity measurement results meet the requirements of the security authentication center, allowing the terminal to access to the trusted internal net. The experimental results are shown in Fig. 3 and Fig. 4.

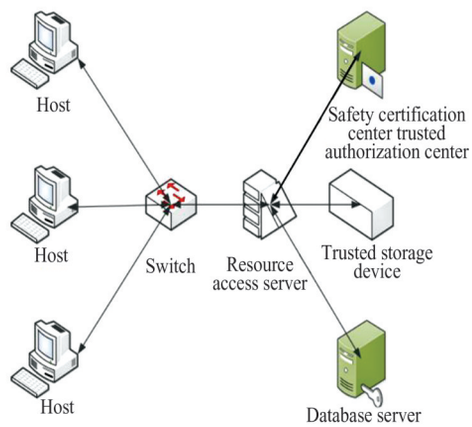

Fig. 3 Test network topology

Condition monitoring

Attributes	Value
Host category	PC
Credible assessment level	10
Department	SAO
IP address	192.168.11.32
Identity	Staff
Ukey serial number	66666465

Check for updates

Fig. 4 Status detection

2) Security access control

In view of the problems existing in the original Energy Internet access scenario, the three secure access control scenarios were designed for the trusted Energy Internet access prototype system, including user connection timeout, the abnormal terminal environment, and the terminal with a lack of integrity. The test results are listed in Table 1.

It can be seen from Table 1 that the system can have a relatively sensitive detection of the changes of user and terminal attributes, and adjust the permissions

according to different attribute changes, with a good performance on the safe access control of the trusted Energy Internet.

5.3 Performance Analysis

In order to verify the functional implementation effect of the trusted Energy Internet access control model, we test the main functions of the proposed system 50 times, and list the experimental results in Table 2.

The experimental results show that the trusted Energy Internet access control model has a stable operation

Table 1 Security access control function test

Test content	Test method	Times	Results
Integrity verification for terminal failed	Modify or delete key system files such as authorized driver files and kernel files	40	Platform integrity authentication failed, user access failed
The connection is not safe because the user is not in the time domain	Abnormal users attempt to access the Energy Internet system many times outside the specified time	40	The trust degree, access security level and authority range of the system to users are reduced, and the system enters the alert state
Abnormal terminal execution environment such as characteristic attributes	Load the malicious code file, and the terminal protection software will check and record	40	The system has been successfully detected, the access security level has been reduced, and the scope of authority has been reduced
User attempted dictionary attack	Users use known user names to constantly try passwords and brute force cracking	40	When a malicious user brutally cracks the same account, the account and its connected terminal will be frozen

Table 2 Performance of the Energy Internet access control

Experimental content	Method of the experiment	Results
Verification of equipment attributes and integrity information	The system will verify the attributes and integrity of the collected devices when they are accessed again	There were no exception, runtime between 2.24-4.31 s with an average runtime of 3.58 s
Collection of device properties and integrity information	Terminal attributes and integrity information are collected during user login verification	There were no exception, runtime between 4.98-7.09 s with an average runtime of 6.64 s
External security equipment access verification	The external security device is the USB key. User inserts USB Key device to verify PIN code (ignore user input time)	There were no exception, response time between 0.09-0.18 s and the average response time was 0.14 s
Verify user personal identity security	First, the user enters the user name and password, and then the security authentication center completes the Energy Internet identity authentication (the user input time is not calculated)	There were no exception, with a response time between 0.17-0.32 s, and the average response time was 0.22 s
Energy Internet resource access request	The user refreshes the resource request list for a trusted server response	There were no exception, response time between 0.44-0.70 s and the average response time was 0.55 s
Energy and Internet resource operation	Test users use the terminal for Energy Internet data upload and download function	There is no exception

effect and the dynamic and flexible access control policy. The test response time can meet the basic user access requirements. In terms of the time-consuming in collecting user terminal attributes and integrity information, the traversal range of system key files and the calculation rate of system hash values are related. The server returns the corresponding resource based on the user allocation role and the access security level, extending the access response time. At the same time, when users request access to Energy Internet resources, the server will return the corresponding resources according to the access control policy corresponding to the user's assigned role and access security level, thus prolonging the access response time, but the response speed is within the acceptable range, and hardly hindrance the normal use of users.

We compare our system with other related approaches, and the details are shown in Table 3. The results show our system can provide more trusted services than other approaches.

Table 3 Comparison of our system with others

Method	Lightweight	Scalability	Fine granularity	Identity certification	Simulation or implementation
Ref.[19]	Yes	Yes	Yes	No	Yes
Ref.[20]	No	Yes	Yes	No	Yes
Our method	Yes	Yes	Yes	Yes	Yes

6 Conclusion

The existing Energy Internet access systems have insufficient resource access allocation, and traditional access policies have low security and flexibility in permission management. Access allocation cannot be adjusted in real time according to network environment changes. In the traditional trusted Energy Internet access policy, users, roles and permissions are statically related, and permissions cannot be adjusted in real time according to the changes of network environment. The two factors above pose a security threat to the confidentiality of energy Internet resource data.

The method proposed in this paper adopts the combination of trusted computing technology and access control security mechanism to improve the current trusted Energy Internet access control mechanism. A strong association scheme of role and terminal based on USB Key identity authentication technology is proposed to establish a one-to-one correspondence while protecting the authenticity of user role; By optimizing the traditional access control policy and combining the advantages of RBAC and ABAC, a dynamic access control policy based on user roles and terminal attributes is proposed to meet the security requirements of dynamic role changes. By ensuring strong correlation between roles and terminals, roles and permissions can be dynamically adjusted to ensure secure allocation of terminal resources and protect system privacy.

References

[1] Cao J W, Yang M B, Zhang D H, *et al*. Energy Internet: An infrastructure for cyber-energy integration[J]. *Southern Power System Technology*, 2014, **8**(4): 1-10(Ch).

[2] Dong Z Y, Zhao J H, Wen F S, *et al*. From smart grid to Energy Internet: Basic concept and research framework[J]. *Automation of Electric Power Systems*, 2014, **38**(15): 1-11(Ch).

[3] Tian S M, Luan W P, Zhang D X, *et al*. Technical forms and key technologies on Energy Internet[J]. *Proceedings of the CSEE*, 2015, **35**(14): 3482-3494(Ch).

[4] Chin W L, Li W, Chen H H. Energy big data security threats in IoT-based smart grid communications[J]. *IEEE Communications Magazine*, 2017, **55**(10): 70-75.

[5] Yan T S, Cheng H Z, Zeng P L, *et al*. System architecture and key technologies of Energy Internet[J]. *Power System Technology*, 2016, **40**(1): 105-113(Ch).

[6] Liao H M, Xuan J X, Zhen P, *et al*. Energy Internet Technology form and Key Technology [J]. *Power Informatization*, 2019, **17** (8): 18-23.

[7] The European Times. The Swedish government is now the largest leakage of military and civilian information is afraid to be exposed [EB/OL]. [2017-04-16]. *http://www.oushinet.com/europe/other/* 20170726/267856.*html*.

[8] Ma D. San Francisco Transit Transportation system attacked by ransomware [EB/OL]. [2016-11-12]. *http://world.people*.

com.cn/*n*1/2016/1129/*c*1002-28910915.*html* .

[9] Saheli Roy Choudhury. Cybercriminals are exploiting fears of the pandemic to steal personal information[EB/OL]. [2020-04-15].*https*://*www.cnbc.com*/2020/04/15/*coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html.*

[10] Li F H, Su M, Shi G Z, *et al*. Research status and development trends of access control model[J]. *Acta Electronica Sinica*, 2012, **40**(4): 805-813(Ch).

[11] Hussein D, Bertin E, Frey V. A community-driven access control approach in distributed IoT environments[J]. *IEEE Communications Magazine*, 2017, **55**(3): 146-153.

[12] Yang Y, Zheng X H, Guo W Z, *et al*. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system[J]. *Information Sciences*, 2019, **479**: 567-592.

[13] Chen H C. Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application [J]. *Mobile Networks and Applications*, 2019, **24**(3): 839-852.

[14] Figueroa-Lorenzo S, Añorga J, Arrizabalaga S. A role-based access control model in modbus SCADA systems. A centralized model approach[J]. *Sensors* , 2019, **19**(20): 4455.1-24.

[15] Thakare A, Lee E, Kumar A, *et al*. PARBAC: Priority-attribute-based RBAC model for azure IoT cloud[J]. *IEEE Internet of Things Journal*, 2020, **7**(4): 2890-2900.

[16] Yu Y, Sun L F, Ma Y H. Attribute-based access control model for attribute-based cloud manufacturing collaboration platform [J]. *Computer Integrated Manufacturing System*, 2017, **23** (1): 196-202.

[17] Shan F F, Li F H, Xie R N, *et al*. Multi-dimensional digital media-oriented access control scheme[J]. *Journal on Communications*, 2015, **36** (11): 52-60.

[18] Wang R. *Attribute-Based Entrusted Access Control Model and Its Application in Smart Home* [D]. Xi'an : Xi 'an University of Electronic Science and Technology, 2020*(Ch)*.

[19] Shi J S, Li R, Pine T T. Blockchain based access control framework for the Internet of Things [J]. *Computer Application*, 2020, **40** (4): 931-941.

[20] Du R Z, Liu Y, Tian J F. An access control method using smart contract for Internet of Things[J]. *Journal of Computer Research and Development*, 2019, **56**(10): 2287-2298 (Ch).

□