Research on Cyber Security Defense and Protection in Power Industry

Zhiyu Chen*, Yonghe Guo, Dongxia Bai, Jiaxin Wang, Yaozhong Dong, Shengqi Qian, Teng Lu, Hairui Xing
State Grid Information & Telecommunication Branch, Beijing, China
*Corresponding author’s email: sevsevf@163.com

Abstract. The power information network is a significant part of national key information infrastructure, as well as the core promoting force to guarantee the strategic development of energy internet. Due to its correlative characteristics in industrial control network, the internet and IoT, superadd a large of nodes and data sensitivity, the evolving network attack technology has put forward new requirements and challenges to its security protection system, which also hinders the overall interconnecting and interworking of energy internet to a certain extent. In order to improve the network security capability of full-service power network under the energy internet environment, a power information security framework based on cloud service was proposed to improve the safety and reliability, build an end-to-end electronic authentication mechanism and security management mode of strong data interworking, finally realize the life cycle data protection, trusted identity management and reliable electronic voucher application, meet the rapid development of the energy internet and escort the new digital economic of the power industry.

Keywords. Information security, identity authentication, block chain, domestic cipher

1. Introduction
With gradual implementation of the energy internet strategy, all nodes will generate massive data at any time and place. A huge social value can be generated via data integration, data mining and business application. The energy internet big data becomes the important asset. The energy internet big data applications are becoming rich and provide energy suppliers/traders, facility operators and users with efficient enterprise operation service in the digital economy age with data as key elements. As the key state information infrastructure, the power grid system platform features diversified business, data, users and interactions, so some severe security conditions are faced in the steps such as data collection, transmission, storage and use [1]. With promotion of digital office of power enterprise, massive electronic business data and trading data are generated in trading of businesses such as enterprise marketing, electronic commerce and financial technology, which involve plentiful sensitive enterprise information and individual privacy data. The sensitive data storage and frequency transfer among application systems in the business chain involve user privacy or system security. Once these data are disclosed or attacked, it will lead to irrevocable aftermaths.

Development of the digital economy promotes digital industrialization and industry digitalization, drives construction of the new-generation infrastructure, forms independently, controllable, secure and trustable new industries, new businesses and new modes, promotes deep fusion of internet, big data,
AI and entity economy, and releases doubling role of digits to economy. However, with deterioration of the network environment, security threats are increasing and it frequently fails to prohibit cases such as information disclosing, network cheat and data eavesdropping, so the digital economy security faces to severe challenges [2,3]. Because of security weakness at any point will endanger the whole information system, data security protection shall transform from passive prevention to proactive protection. With popularization of mobile internet, smart terminals have become the important means for business data interaction. Considering particularity of mobile terminal nodes, the traditional security protection means cannot cover security management steps from data generation, transmission, storage and analysis, so the data security and privacy protection will face to severe conditions. Therefore, complicated and diversified power network has higher requirements for identity authentication and data protection. No security measures can effectively cover the whole-cycle data security. It is urgent to design and perfect the data security protection system based on cryptogram technology and realize secure interaction in the whole chain of the business data.

2. Analysis of power information security
To ensure secure and stable operation of the power business, a higher security is required in network identity authentication, trustable information interaction and data eavesdropping. The power grid fuses the industrial control network, internet and IoT. The industrial control network features network interconnection, interaction operability, connection openness, information truth and instantaneity. The internet features instant message, massive data, global coverage and diversified interaction. IoT is the ubiquitous network based on the internet by using different perception technologies, features smart processing capabilities, and can intelligent control devices. The energy internet is based on the ubiquitous interconnection of the power network by referring to openness, ubiquity and interaction features, brings some reforms in energy development, configuration, consumption, production and living steps, and features strong network architecture, extensive interconnection, high intelligence, openness and interaction. Securities include confidentiality, integrity, availability, authentication, authorization, non-repudiation and auditability. The energy internet integrates multiple physical systems and information network and faces severe requirements and challenges unlike the traditional power informatization features.

2.1 Power network security
The network boundary is becoming fuzzier. Now the power information system is insufficient in management regulations, business systems, operation level and security protection, so some potential troubles exist in business flow. Illegal behaviors such as false trading, counterfeiting behaviors, contract cheat and infringement of consumer’s lawful right and interests during enterprise operation frequently occur. Some security risks in trustable operation and identity illegality of the business end exist. These risks include identity confirmation of both parties, confidentiality of online information transmission, information tampering prevention, effective evidence collection and default repudiation prevention. Figure 1 shows potential troubles in the network environment.

![Figure 1. The structure diagram of blockchain](image-url)
2.2 Information protection based on cryptography

The cryptographic algorithm and models with complete technical system has formed in China. The cryptography is the kernel immune system of the information system, can be extensively applied in the network entity identity mark, identity validation and identification, identity authentication and authorization management, and can effectively ensure truth, integrity, confidentiality and non-repudiation of the information transfer in the network [4,5]. The cryptography can effectively solve the following security issues:

1. The cryptography is combined with data marks, digital signatures and network identity to ensure secure and orderly flowing, effectively support data tracing, behavior tracking and privacy protection, and provide technical means of perfect supervision and guarantee system.

2. The identity identification, trust management, access control, data encryption, trustable computing, cryptograph computing and data decryption based on the cryptography can be used for whole-cycle security management in data generation, transmission, storage, processing, analysis and use.

3. The cryptography is used to solve trust bottleneck in data fusion, realize opening and sharing of information resources, construct true and non-repudiation "digital contract", establish trust foundation for data resource right confirmation, openness, circulation and trading, and further solve the trust obstacles in data fusion.

3. Power cloud security construction

With transfer of businesses from independent servers to power cloud, potential data security problems of online business are highlighted. The physical network security boundary is gradually disappearing and replaced by the logic network security boundary in a cloud computing environment. The traditional security protection gateway deployment mode is not applicable. This paper analyzes security of the data interaction chain in the cloud environment and proposes the security protection architecture from system access authentication, precise data protection to data non-repudiation.

3.1 Identity authentication of power cloud environment

This paper recommends to construct CA center in the cloud environment, construct the security system with the identity authentication, uniform user management and digital signature as kernel applications, provide identity authentication, and secure data transmission and access control management to form an electronic authentication cloud platform and further solve security issues in a cloud environment [6]. Figure 2 shows the power cloud architecture diagram. The cloud security technology is divided into identity security, data security and device security, including certificate production, certificate validation, device resource and data encryption component and is the foundation for cloud electronic authentication service. CA center authenticates user identities by using the multi-factor strong authentication mechanism, determines resource use right and range of access users and strengthens confirmation of legality of business operations. The identity authentication is combined with the cloud computing to realize integrated identity authentication and resource authorization of users with different cloud services and business systems [7,8]. Express, convenient and open cloud services can promote security of mobile applications. The data of mobile terminal can be legally transmitted by using the online cloud CA service, so it can effectively improve work efficiency of the mobile operations.

The identity authentication can determine legality of access users by using the public and private key encryption and decryption mechanism of the asymmetric keys generated by the CA center. The public key signed by CA is public in a traditional PKI environment. Generally the private key is transmitted to the specified users and system via the offline physical mediums to secure distribution. The offline distribution mode cannot ensure update frequency of the private key and severely affect the security level of the business trading. With great promotion of the domestic cryptographic algorithms, if the domestic cryptographic algorithm is used to encrypt the private key, in theory, it can ensure absolute security of the online private key transmission. The domestic cryptographic algorithms
are gradually applied in the power information system, so the authentication mechanism of the power grid need not be reconstructed much in the plan. This plan is well adaptable and can effectively improve operation efficiency of electronic authentication. The new cloud security protection system includes the following features:

1) The system establishes the authentication service middleware architecture and realizes centrally integrated, secure and trustable electronic authentication environment of heterogeneous systems at multiple user centers.

2) The system strengthens secure storage technology of sensitive data and private data, solves data integrity validation and truth issues, and realizes secure data storage cloud service.

3) The system constructs a third-party evident tracing system, connects multiple CA and provides the secure and integrated operation integration environment in the industry.

4) The system forms the operation mode of integrated resource scheduling and integrated infrastructure management and can effectively improve operation efficiency of the electronic authentication system.

![Figure 2. Power cloud computing security protection architecture.](image-url)
3.2 Cryptographic cloud service

The digital economy coexists with the network space and features the data resources as the kernel elements, information technology as reform power and data fusion as main mode. The cryptogram is the kernel technology and foundation support of the network space security and plays an irreplaceable role. Development of digital economy will depend on collaborative innovation mechanism of the cryptography and information technology. It is necessary to strengthen cryptogram application in network trust, network governance, internet application, cloud service, mobile terminal, citizen privacy and digital asset protection and construct a cryptogram support system for the state key foundational information.

![Diagram of Cryptographic Cloud Service](image)

**Figure 3.** SaaS mode password service cloud based on domestic cipher algorithm.

With issuing of the requirements for the domestic network security technologies are urgent, it marks higher and higher requirements for network security. To further improve security level of data protection, by combining domestic cryptogram technology and cloud computing technology, the cryptogram encryption/decryption service cloud platform is constructed. This cryptogram service cloud platform is established based on the state cryptogram algorithms, can provide trustable keys to protect business data, form the encryption/decryption application architecture based on SaaS mode, and extremely improve data security level [9]. Figure 3 shows the encryption/decryption service cloud platform based on SaaS mode, which provides security key for whole-chain data security in the cloud environment. The flow was described as follows:

1) The provincial cloud application system will call the security service of the cryptogram service platform via middleware.

2) The cryptogram service platform applies the password generation device for a key.

3) The headquarters cloud device will generate the algorithm key and encrypt data by using the key generated by the cryptogram gateway.

4) After the provincial cloud service platform gets the encrypted algorithm key information, it will get the algorithm key via decryption.

5) The decrypted information is used for cryptogram service such as encryption and decryption, signature and validation.
3.3 Data security interaction based on block chain

Quick development of “Internet+” transformation, electronic commerce, finance technology, electric car and comprehensive energy business is promoted hard in the power industry based on the energy internet strategy. The power enterprise supply chain quickly changes and extends and covers nodes such as manufacturer, service provider, channel provider, finance agencies, supervision agencies and customers [10]. The supply chain management becomes more difficult and collaboration efficiency is restricted by plentiful factors such as isolated data islands, data trust issue and performance guarantee issue.

With development of the supply chain finance, some scenarios such as multi-body participation, asymmetric information, imperfect trust mechanism and no trust data are formed. The supply chain includes multi-tier supply and sale relation, but generally trust of kernel enterprises can only cover the directly trading L1 suppliers and L1 franchisers and cannot be transferred to upstream and downstream medium-size and small-size enterprises requiring financial services [11,12]. Such mode is inherently matched with the blockchain technology. As on distributed account book, the blockchain provides a fair collaboration platform for participants, reduces trust collaboration risks and cost among organizations, and features decentration, openness, tamper-proofing and autonomy. The blockchain can remove the trading relation among layers to transfer trust to remote enterprises not directly trading with the kernel enterprises and contain them into the service scope of the supply chain [13,15].

The enterprise supply chain based on the blockchain technologies collaborates upstream and downstream enterprises to complete trading. Multi-party collaboration promotes the industry ecological chain to evolve to more true, more transparent and more intelligent direction and solve data interconnection and intercommunication, trustable sharing and orderly collaboration of private data such as digital identities and data assets. Collaboration of the blockchain technology can ensure that enterprise contracts can automatically execute fairly without disturbance. The asset digitalization makes the asset value feature right confirmation, transfer and disassembly and effectively improves liquidity of digital assets. All trades are completed by all parties in the ecological chain together. All parties have complete trading information, so it can further ensure truth of contract and order information. The mechanism based on cryptography can ensure non repudiation and damage of the trades. The block chain technology can strictly authenticate identity of nodes in trading flows and solve identity truth issue of participants. Figure 4 shows data trust transfer based on the blockchain.

Figure 4. Data trust transfer based on block chain.

4. Conclusions

With improvement of information security consciousness of the public, the requirements for data security and privacy protection are higher and higher. It is difficult to solve security threats in enterprise internet by only using single network security technology in new network security environment and supervision requirement. By combining CA authentication, cryptogram service cloud and blockchain collaboration technologies, a new architecture of power industry identity
authentication and data protection is established in this paper to authenticate access from the business terminal to the cloud service end secure data transfer and trust of the whole business chain, and securely protect data circulation at different steps in a power cloud environment..

Acknowledgment
This research was supported by the Science and Technology Project of State Grid Information & Telecommunication Branch (Key Technologies for Omni-scenario Cyber Security Defense and Protection).

References
[1] Chen M, 2018 Application of commercial cryptography in power industry no 5 (Information Security and Communications Privacy) pp 50-56.
[2] Tian M, 2018 Review on chinese cryptography standard hierarchical system no 5 (Information Security and Communications Privacy) pp 94-101.
[3] Miao X, Zhang L, Ma P, et al, 2017 Optical fiber transmission solution of measurement and control signal between substations based on quantum key distribution and one-time pad vol 41 no 12 (Automation of Electric Power Systems) pp 212-217.
[4] Bai J, Lin F, Xu Y, et al, 2017 Digital metering system of new generation smart substation in China vol 54 no 17 (Electrical Measurement &Instrumentation) pp 40-45.
[5] Jing J, and Liu L, 2017 The “2.0-Era” of Certification and authentication techniques vol 3 no 6 (Journal of Information Security Research) pp 573-576.
[6] Shen L, Wang D, and Xuan J, 2018 Security risk analysis and evaluation techniques in power information system cloud no 2 (Telecommunications Science) pp 153-160.
[7] Tian J, and Sun K, 2015 Trust-distributed-based authentication mechanism using hierarchical identity-based cryptography vol 52 no 7 (Journal of Computer Research and Development) pp 1660-1671.
[8] Wen Q, Yang W, Zhang Y, 2017 Application of SM9 and PKI in e-government e-mail system vol 31 no 4 (Computer Applications and Software) pp 105-109.
[9] Li C, and Bovik A. C, 2017 Research on the fusion architecture and application mode of quantum cryptography and classic cryptography (International Conference on E-Society, E-Education and E-Technology. ACM) pp 28-32.
[10] Zhang X, 2018 Research on model optimization of supply chain management based on blockchain vol 32 no 8 (China Business and Market) pp 42-50.
[11] Wang J, Goa L, Guo A, et al, 2017 Block chain based data security sharing network architecture research vol 54 no 4 (Journal of Computer Research and Development) pp 742-749.
[12] Wu J, Gao Y, Zhang Z, et al, 2018 A multi-party privacy preserving fair contract signing protocol based on blockchains vol 3 no 3 (Journal of Cyber Security) pp 8-16.
[13] Wang B, Li Y, Zhao S, et al, 2019 Key Technologies on blockchain based distributed energy transaction vol 43 no 14 (Automation of Electric Power Systems) pp 53-64.
[14] Zhao Y, Peng K, Xu B, et al, 2019 Status and prospect of pilot project of energy blockchain vol 43 no 7 (Automation of Electric Power Systems) pp 14-22, 58.
[15] Zeng S, Huo R, Huang T. et al, 2020 Survey of blockchain: principle, progress and application vol 41 no 1 (Journal on Communications) pp 134-151.