Design and Implementation of Cloud Crypto Secure Server System for Power System Based on Sharing Encryption Resource

Tie-jun JIA* and Yang LI

College of Information Technology, Shanghai Jianqiao University, Shanghai, China
*Corresponding author

Keywords: CCSSS (Cloud Crypto Secure Server System), Cryptograph service, Shared encryption resources, System platform establishment, Cloud Encryption.

Abstract. It is very important to use the new technology of cloud security and encryption to improve the security of the power information system and business data. Based on the requirement analysis of cloud security cryptograph service in power information system, design and implement CCSSS (Cloud Crypto Secure Server System), it's helpful to improve the uniform formulation of various application system encryption specifications and the overall security effectiveness of cryptographic products. Practice has proved that providing services such as shared cloud encryption resources and development, management and maintenance in platform approach can provide more effective and comprehensive security sharing services for the power industry.

Introduction

The security of the power information system directly affects the national economy and the people's livelihood, social stability and economic development. The centralized processing of various power information systems and business data makes the risk of continuous security of business services increased, there is an urgent need to build CCSSS.

New technology of cloud security encryption helps to provide more effective overall network security protection. Through the analysis of the requirements of cloud security cryptograph service in power information system, CCSSS is designed and constructed so as to improve the effectiveness of unified formulation of system encryption specification and overall encryption security, integrate existing encryption technologies and methods, and providing more comprehensive and effective resource sharing and management of cloud encryption services based on the system cloud service platform [1].

Requirement Analysis of Cloud Encryption Service in Power

Requirement Analysis of Cloud Security in Power Information System

The power information system mainly includes power control system, power dispatching system, business data processing system and related management information system. Risk analysis is needed for its network cloud security needs. It mainly includes seven cloud security key risk areas and security threats summarized by the cloud security alliance CSA (Canadian Standards Association).

Abuse and Nefarious Use of Cloud Computing, Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking, Unknown Risk Profile. The confidentiality, integrity and availability of network information security are three basic attributes. It is also the most basic demand for power enterprises to use cloud encryption service. First, after uploading to the cloud information and processing, the cloud service can only be accessed or used by the authorized users. Second, the cloud service related data should be complete, true and effective, and can not be illegally manipulated, tampered, forged or destroyed and can be reviewed.. Third, the network, data and service have continuity and timeliness, ensuring that the cloud service is used in time for the authorized users [2,3].
The needs on relevant hierarchy of power information cloud encryption services: the bottom is the infrastructure security, including basic platform security, virtualization security and safety management; the middle is data security, the top is cloud encryption service, peripheral include network security access related detection and defense technology [4], the demands mainly include:

1. The cloud encryption service platform is built to provide unified, standardized and efficient encryption underlying services for the new key business and management information system of the power industry, and provide diverse cryptograph service components and program call interfaces.

2. A perfect key management system is gradually established to provide a standard key management underlying service for the information system.

3. Unified customization and encapsulation of commercial cipher algorithm and key management interface, meeting the application requirements of security mechanisms such as information encryption, identity authentication, integrity verification, digital signature and key management in the development of information project, providing multi-platform, multi-level standard cryptograph interface software package (CryptoAPI).

4. According to the construction of power information system security strategy and related laws and regulations, formulating relevant cryptograph and encryption technology and product application technical specifications and guidelines, and further standardize the application of cryptograph technology in power information system.

The Distribution of Cloud Encryption Services
Using Unified Threat Management (UTM), which is equivalent to the integration of anti-virus software, firewall and intrusion detection system, the CCSSS constructed needs to form a unified management distribution, as shown in Figure 1.

System Design and Implementation

Structure Design of CCSSS
CCSSS is used for general safety function development and running platform of power industry management information system and enterprise network system construction, is a complete and the underlying cryptograph hardware combination, provide a variety of cryptograph cloud services in the application layer and the transport layer system and cipher suite. Cloud security components mainly composed of: ①PKCS11 - C language PKI function call interface component compatible with PKCS11 standard; ②JCE - Java language security interface extension component compatible with SUN JCE; ③CSP - Encrypted IC card and USB key cryptographic device abstract interface
component; ④CryptoAPI - The cipher service application programming interface component after the second encapsulation for the power industry. Write a programmer's manual for the application of cryptograph technology in the power industry to provide accurate and detailed description of function calls and typical routines.

Through the organic combination of the above security components, the power industry CCSSS can provide a full range of multi-level security for the cloud terminal users. The CCSSS structure of the power industry is shown in Figure 2.

![Figure 2. The CCSSS structure of the power industry](image)

Among them, the CSP abstract device layer is between the standard interface layer and the hardware device layer. It hides the call and implementation details of the underlying device for the upper interface program, and provides all functions supported by the cryptograph device for the upper program, providing flexible programming interface environment.

The CryptoAPI interface is a programming interface that provides cryptograph operations and key management directly for the cloud user application system, use the hardware cryptograph device to complete the popular cryptograph algorithm, public key cryptographic algorithm and HASH and MAC cipher algorithm which are in line with Chinese commercial cryptograph specification.

PKCS11 conforms to the cryptograph functional programming interface of RSA's PKCS#11 cryptograph function call interface standard. The power industry CCSSS PKCS11 provides the main function provided by PKCS#11 interface.

Other layers are mainly enterprise customized CryptoAPI and SSL secure sockets layer system services, Cert certificate management services, etc., which can be directly invoked by the upper application system.

The Composition and Function of CCSSS

For the power industry CCSSS, the safety function of every component is different and complement from the view of computer operation system, and form a CCSSS of power industry application system. It mainly includes:

(1) Core cryptograph function module. Preserving the confidentiality of stored and transmitted information through a trusted and high-performance cryptograph algorithm, which consists of oriented C++ environment Crypto-C and Java oriented environment Crypto-J.

(2) Security protocol SSL module. According to the industrial standard security protocol, the encryption service of application system transport layer is provided. The specific functions of SSL-C include SSL and TLS, CA authentication supporting multiple configurations and certificate service.

(3) Key management module. The power industry CCSSS uses the three level key management system, the main key, the exchange key and the session key. The main key (asymmetric key) is used
to sign and authenticated the data, and to distribute and authenticate the exchange key, so that the two level key is not exposed outside the encryption card in the form of plaintext in the process of generation, distribution and setup.

Implementation and Deployment of CCSSS

Implementation of CCSSS

(1) Access new encryption card, encryption IC card and USB key through the CSP layer; Access SJY series cipher machine through PKCS#11 and vendor proprietary interface in an abstract device layer; Project oriented application development, provide C language and JAVA environment cryptograph service interface components PKCS11, JCE and CryptoAPI; Key support application development based on Windows 2K, SCO UNIX, Linux AIX and HP-UX server system and minicomputer, and provides application development manual [3,5].

(2) For PKI (Public Key Infrastructure) series of server-based password machine, encryption IC card and USB Key, shielding the details of the implementation of cryptograph to achieve a common password service interface to ensure that the various information systems in the development, production, operation and maintenance various stages, can flexibly choose and replace the cryptograph hardware equipment from different vendors, to improve the independence and interchangeability of cryptograph technology application equipment.

(3) The encryption platform combined with the improved Homomorphic Encryption (HE) technology, High intensively encrypts the private key used for decryption, and encrypts the user privacy data [6,8].

(4) Realize encrypted information sharing. The standard algorithm is used to lay a good foundation for the sharing of encrypted data between the systems; Provide a unified cryptograph support services based on the unified application platform, to ensure the unity of key management, encryption algorithm, and key length between two or more systems that require information exchange; The data exchange with third party should be completed by encryption machine.

(5) According to the practical requirements of development project using security encoding, Based on the standard cryptograph interfaces PKCS # 11, CSP (Commerce Server Provider) and JCE, the power industry specific Crypto Application Programming Interface (CryptoAPI) is identified and encapsulated to shield the complexity of the application of the standard crypto interface.

(6) For the power industry outlets and management system cloud client, provides CSP and PKCS#11 two kinds of interface software cryptograph computing module, and according to the actual needs supporting the use of encryption IC card and USB key two hardware interfaces, focusing on cloud client key storage and digital signature verification issues.

Deployment and Application of CCSSS

CCSSS provides encryption services for all kinds of UNIX and Windows cryptograph secure API (Application Programming Interface), static libraries, dynamic libraries, service components and Java class libraries or cryptograph security middleware. It usually provides cryptograph support services based on PKI and KMI (Key Management Infrastructure), while internal encryption services provide encryption protection for data transmission and data storage. The application deployment of the application systems to encrypted cloud encryption services is shown in Figure 3.

Among them, the deployment of encryption service in the power business application is as follows:

(1) The "Cloud Encryption Service Module" is invoked by "Business Logic" and invokes the "Cloud Encryption Service Component" deployed on the "Integrated Platform" to directly perform the encryption service.

(2) Using application adapter, security control can be carried out for different applications access to "integrated platform", and encryption processing can be forced invoked according to the requirements.
(3) The encryption service can be invoked directly through the cloud encryption service API in the application. It is convenient to realize the encryption protection of data transmission between applications by using the integrated platform (mode ① and ②). For applications that are not integrated on the integrated platform (mode ③), the same encryption and decryption basic component (API) is used to implement the encryption problem of data transmission [7].

![Encrypted cloud encryption service deployment of application system](image)

Figure 3. Encrypted cloud encryption service deployment of application system

Usually, encrypted basic component is applied when data is transmitted, and CCSSS is applied to the application system after combining with communication basic component. It enables cloud security processing to invoke application logic and reduce the complexity of application system construction. The actual application effect mainly embodies 5 aspects:

1. In the two levels of the head office and the branch office, the sharing of various resources of the cloud security cryptograph can be realized, and the repeated investment of the cryptograph devices can be avoided.
2. In the follow-up development of information projects, there is no need to repeat the development of cryptograph operation processing modules, which can speed up the progress of the project and save a lot of manpower and material resources.
3. There is no need to worry about the problems of after-sale service and equipment shutdown by realizing the upgrading and expansion of the power cloud security cryptograph products.
4. Overall improvement of the security level and effectiveness of the power information system.
5. Strengthen the key management service through the cloud and the server side. It includes generation, storage, distribution, input and output, update and discarding of the key. The symmetric key adopts three level key system (main key, work key and session key), and the public key / private key manages the public key and private key by using the key management infrastructure (KMI).

**Conclusion**

The security service with cloud encryption technology can combine basic cryptograph algorithm operation, resource management and key management mechanism to provide efficient cryptograph services including encryption, signature, signature verification, digital envelope, etc., and the CCSSS platform itself has high integrity, reliability and security. From function and structure analysis and design, all cloud computing virtual machines of the cloud cryptograph service have encryption functions, the cryptograph function execution unit performs the basic cryptograph operation, the cloud security API encapsulates the cryptograph operation and the internal key management mechanism, and provides cloud security application a unified and secure cryptograph function call interface, and the cryptograph resource management module implements the management and
scheduling of the cryptograph execution unit and the management functions of the overall system security mechanism.

The encryption platform combines the improved homomorphic encryption technology to encrypt the private key used for the decryption, and encrypts the cloud data with the new homomorphic encryption technology [8]. For the cryptograph computing speed of the resource encryption platform, the test shows that the key to meet the requirement can be generated in a short time.

Acknowledgement
This research was financially supported by the National Science Foundation (61402280). Computer Technology discipline of Shanghai Jianqiao University (AASH1609).

References


