Research on mobile application support system based on internal and external network

He Wu*, *Lin* Qiao, *Shuo* Chen, *Wei* Liu, and *Feng* Li

State Grid Liaoning Electric Power Supply Co., Ltd. Information and Communication Branch,Heping District, Shenyang City, Liaoning, China

Abstract. Since 13th Five-Year, great changes have taken place in the situation at home and abroad. Internal and external factors such as "Internet +" innovation and development, new technology driven and information security situation have had a wide and profound impact on the production and operation of enterprises. At the same time, new requirements for information and communication work have been put forward. Based on the existing internal and external network structure of the enterprise, we study a fast response, collaborative innovation, security and controllable mobile application support system, so as to speed up the construction of enterprise mobile applications, and help "Internet +" management innovation and business innovation.

1 Intoductions

In recent years, according to the national innovation-driven development strategy, information and communication technology innovation and development action plan and other work requirements, the number of mobile applications has increased significantly, and the scope of application has expanded year by year [1]. So that the security, stability, scalability, maintainability and other aspects of the requirements of mobile applications are constantly improving.

Therefore, this project carries out the research of mobile application support system based on internal and external network, analyzes business model and process on the basis of enterprise business scenario modeling, integrates application and data flow model according to different business objects in-depth, so as to provide a unified development, deployment, operation and maintenance framework for different mobile applications. It also provides standard logic design and security access standard for new applications. Through the design of data access control and exchange mode, the flow of data usage is standardized, which improves the ease and consistency of data and enhances the security of data by endogenous mechanism. And a multi-factor authentication method which combines biometrics technology with traditional identity recognition method is used to realize the security authentication of mobile terminal and its users, and ultimately to support the rapid development of enterprise mobile application security.

* Corresponding author: wh07cp3@qq.com

2 Main methods

This research is based on the mobile application support system of internal and external network. Through modeling the business scenario, analyzing the business model and process, abstracting and integrating the application and data flow model according to different business types, it provides a unified framework for the development, deployment and operation of different mobile applications, and provides a standard for new applications. Quasi logic design and security access specification. Through the design of data access control and exchange mode, the flow of data usage is standardized. The data usability and consistency are improved, and the data security is enhanced by endogenous mechanism. A multi-factor authentication method combining biometrics technology with traditional identification methods is used to achieve security authentication for mobile terminals and their users.

2.1 Business scenario modelling

By analyzing the different needs of various mobile application user groups in enterprises, and considering the mobile terminal access mode, network architecture design and security protection measures, many application scenarios are merged reasonably, and the differentiated services are constructed from three application scenarios: intranet mobile operation, extranet mobile cooperation and Internet mobile service. The flow model and the corresponding data flow model can realize the collaborative optimization of service flow and data flow, thus providing a unified framework for the development, deployment and operation of different mobile applications, and meeting the different network access modes and security requirements.

2.2 Differentiated network access of security

According to the results of business scenario modeling, network access is provided in the following ways:

Intranet mobile operation class refers to the real-time interaction between mobile terminals and business information systems deployed in the enterprise information intranet. All business processes are completed in the intranet, mainly serving the mobile applications of enterprise internal operators. Client in the intranet employee mobile portal on the shelf, using the dedicated mobile terminal as the carrier, with the dedicated encryption network as the channel, through the intranet security access platform access to the enterprise information intranet.

External mobile collaboration refers to the real-time interaction between mobile terminals and business information systems deployed in the enterprise information extranet. Business processes are completed in the extranet. There are only specific data interaction behaviors between mobile terminals and intranet information systems. It mainly serves the internal employees of the enterprise and the temporary external personnel who participate in the production and operation activities of the enterprise. The client is hosted on the mobile application portal of the employees in the external network, using the personal smart phone as the carrier, using the Internet as the channel, accessing the enterprise information extranet through the external network security interactive platform, and exchanging specific data with the intranet through the isolation device.

Internet mobile services refer to the real-time interaction between mobile terminals and business information systems deployed in the enterprise information extranet. Business processes are completed in the extranet. There are only specific data interaction behaviors

between mobile terminals and intranet information systems, mainly serving the mobile applications of the public. Clients are hosted on the Internet client mobile application portal, using personal smart phones as carriers, using the Internet as a channel, accessing the enterprise information extranet through the external network security interaction platform, and exchanging specific data with the intranet through isolation devices.

2.3 Using a network isolation device based on black-and-white list

Through the design of data access control and exchange mode, the flow of data usage is standardized. The data usability and consistency are improved, and the data security is enhanced by endogenous mechanism. The data security exchange method of the network isolation device includes reading the data to be exchanged and matching the isolation rule strategy, stripping the pure data content to match the successful protocol, matching the keywords in the black-and-white list, sending the white-list matching successfully, blocking and remembering the successful blacklist matching. Logging, if the black-and-white list does not match successfully, the pure data content will be pushed to the administrator for manual selection configuration. Intelligent black-and-white list technology is adopted to solve the technical problems that traditional isolation devices cannot meet the special transmission requirements. The intelligent extraction and expansion of keywords in black-and-white list is realized, which not only ensures the security of data interaction, but also enhances the flexibility of data transmission.

2.4 Mobile access to dual factor security authentication

Factor 1 refers to a secure access authentication method for mobile terminals based on fingerprint identification technology, which includes four steps: establishing an encryption channel, user registration, user information audit and user service access. Theoretically, biometric authentication has uniqueness, permanence, universality, portability, higher security and better user experience [2]. Factor 2 refers to collecting terminal characteristic information through the client, including USBKEY serial number, digital certificate serial number, and mobile. Terminal serial number and other terminal equipment characteristic information. The security access gateway verifies the integrity and validity of the terminal information and determines whether the terminal can access the protected server according to the verification results. By combining biometrics technology with traditional device identification methods, two-factor authentication ensures the identity legitimacy of access terminals and their users.

3 Advantages

3.1 Mobile application scenario support

Common mobile application platforms at home and abroad are only for ordinary Internet users, and only need to support general Internet mobile applications. There is only one Internet service scenario model, which does not support mobile applications with specific needs such as user groups, terminal types, network bearers, and secure access modes in proprietary business scenarios.

Through the analysis of the overall requirements of enterprise mobile applications, combined with enterprise security requirements, according to the actual needs of different business scenarios to develop different deployment methods and security requirements, thus providing comprehensive support.

3.2 Network security protection

Most of the common mobile applications at home and abroad do not belong to a single external network environment, mobile terminal access mode is single, network security uses traditional single security measures such as firewall, IPS, IDS, etc., which cannot achieve the differential security protection for mobile terminal access inside and outside the network [3]. Furthermore, traditional IDS will act on each intrusion alarm, so if the sensitivity is too high, it will produce too many false intrusion alarms, which will not only destroy some of the necessary functions of the normal system, but also cause a lot of additional burden on the system; and low sensitivity will make IDS unable to detect some intrusion behavior. So that intruders successfully enter the system and cause unexpected losses [4].

This project uses the security interactive platform, security access platform, isolation devices and other types of special security equipment, using black-and-white list access control, fingerprint identification technology to achieve the internal and external network mobile terminal differential access mode and security requirements. Intranet terminals use dedicated mobile terminals as carriers and private encryption networks as channels to access the enterprise information intranet through the Intranet security access platform. External terminals use personal smart phones as carriers and the Internet as a channel to access the enterprise information extranet through the External Network Security Interactive Platform. Through isolation devices and The information intranet carries out specific data interaction.

3.3 Data synchronization and data security interaction

Common isolation devices at home and abroad often use buffer technology, authentication technology to achieve data security exchange, and black-and-white list access control technology is often used in firewall ACL; common client authentication methods often use hardware fingerprints (including hard disk physical serial number, CPU serial number, MAC address, BIOS serial number, master). One or more of the board serial numbers and International Mobile Device Identity Codes (IMEI), but for the terminal device hardware solidification information needs higher privileges, there is a risk of user privacy leakage. Information security has become an important factor to restrict the development of mobile applications. Universal authentication technology has the following shortcomings: the password is difficult to remember and easy to be cracked; SMS authentication code has the possibility of being intercepted and stolen, and its response speed is slow; external key has poor flexibility and inconvenience to carry [5].

This project will be widely used in the firewall black-and-white list access control technology for data security exchange isolation devices, enhance the traditional isolation device security protection flexibility and maintainability. In the aspect of user authentication, the terminal characteristic information collected by the client includes USBKEY serial number, digital certificate and so on. Combined with biometric information such as user fingerprint, multi-factor authentication ensures the identity legitimacy of the access terminal and its users.

4 Effects

4.1 Social benefits

By building a mobile application support system based on internal and external network, it promotes the safe and efficient development of all kinds of mobile applications in enterprises, effectively improves the service level of enterprises, reduces the service

response time, improves the communication mode with users, and is very important for improving the satisfaction of users and maintaining a good social image of enterprises. The meaning of it. At the same time, vigorously promoting the construction of mobile information also responds to the strategic call of integration of the two countries and Internet +, which helps to promote the rapid development of mobile information related industry chain, and promotes the transformation of IT infrastructure to green, energy saving, environmental protection and high efficiency, and enhances the value creativity and core competitiveness of enterprises.

4.2 Management efficiency

By building a mobile application support system based on internal and external network, transaction response speed and processing capacity can be effectively improved. At the same time, the platform promotes the development of enterprise mobile applications and the real-time interaction of information, develops the potential value of data, helps optimize the allocation of core resources of human and financial resources, improves the efficiency of enterprise management and the ability of scientific decision-making, continuously improves the level of enterprise information management, and promotes the enterprise to intelligent. The direction of industrialization and lean development is constantly developing.

5 Conclusion

Based on the principle of "big platform, micro-application", the mobile application support system of this project meets the requirements of enterprise mobile application design by modeling of business scenarios, differentiating network layer security access, using black-and-white list-based network isolation device, mobile terminal access multi-factor security authentication and so on. Common requirements, such as development, security access, application publishing and operation guarantee, can effectively support the construction of enterprise mobile applications.

Acknowledgement

Note: This paper is supported by the project of "Research on Improving Technological Innovation Ability and Mass Innovation - Information Communication Branch of State Grid Liaoning Electric Power Supply Company Limited (5222XT180033)"

References

1. Jiang Wei. (2013). On Security Control Technology of Mobile Applications. *Enterprise Science And Technology & Development.* (2013.12):78-80
2. Tang Ya Fei, Zhang Yunyong, Zhang Ni. (2015). Cloud Security Certification Technology Based on Fingerprint Recognition. *Telecommunications Science*. (2015211):1-7
3. Liu Qiang, Yang Wei Yong, Liu Jin Suo. (2015). Research on the Security of Power Mobile Informatization. *Electric Power ICT*. (2018.08):83-87
4. Li Jing Chun. (2014). Security problems and protective measures of APP application in mobile terminals. *Information security and communication secrecy*. (2014.12):47-48
5. Huang Zelong, Zhang Wenan. (2015). Scheme and application of mobile security authentication based on UIM card. *Operation and Application*. (2015.12.005):16-19