Research on the Construction and Application of Smart Hospital Based on Mobile Terminal Security Aggregation Business Management Platform

Yixin Wang(✉), Weiqing Fang, Liang Chen, and Wei Zhu

Changshu No. 2 People's Hospital, Changshu 215500, Jiangsu, China
715246936@qq.com

Abstract. Accelerate the construction of smart hospitals and the standardization of hospital information by accelerating the "trinity" of electronic medical records, smart services, and smart management. Mainly use the self-developed mobile terminal platform to study the transformation of mobile applications such as hospital medical management, reporting and review, and epidemic reporting. Taking the Second People's Hospital of Changshu City as an example, in combination with the actual clinical business environment, combined with the security boundary of data exchange, the important clinical application and medical management of the hospital are completed within the theoretically divided area using data transmission technology that meets safety standards The effective data is centralized, so as to establish a customized standard software application system. Through the management method of safe aggregation, the research on the integration and integration of all mobile systems in the hospital will provide the basis for the development and application of intelligent hospitals. The self-developed mobile platform has added security management and monitoring functions to create a scalable, high-efficiency and high-security network service platform.

Keywords: Information Security · Smart Hospital · Management Platform

1 Introduction

2022 is an important year for the medical and health industry to vigorously develop new technologies such as the Internet of Things, big data, cloud computing, mobile Internet, artificial intelligence, and blockchain [1]. In the further improvement of the medical service action plan (2018–2020) [2] and a series of major policies to innovate the medical service model, optimize the medical service process, improve the quality and safety of medical care, and improve the public's medical experience, start with a high starting point, start with a high standard, and start with a high standard. Quality promotes the construction of medical information technology is particularly important. Strengthening the construction and development of medical care by means of information technology is an important part of deepening the reform of the medical and health system, maintaining

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 532, pp. 354–361, 2024.
https://doi.org/10.1007/978-3-031-50571-3_25

and promoting people's physical and mental health, comprehensively promoting the rule of law, innovating social governance, and promoting social harmony and stability. China, the rule of law in China, and a safe China are of great significance [3].

Our hospital belongs to a tertiary hospital. Accelerating the construction of a smart hospital and hospital information standardization of electronic medical records, smart services, and smart management is an important part of hospital construction and hospital development, because information technology can improve Overall work efficiency, standardization of technical processes, reduction of management costs, improvement of hospital image and other benefits [4, 5]. Combining some of our hospital's current diagnosis and treatment service processes, post-diagnosis service processes, internal management processes, and related medical information systems (HIS), structured electronic medical record systems (EMR), inspection systems (LIS), and nursing management systems (NIS), electrocardiogram system (ECG), medical image system (PACS), and office (OA) system have conducted a comprehensive analysis, and feel that some process optimization can be carried out in the direction of mobile Internet [6, 7]. The specific analysis is as follows:

For patients, the current medical service field is facing an unreasonable allocation of medical resources. In my country, problems such as difficult and expensive medical treatment have existed for a long time [8–10]. "Waiting for three hours and three minutes to see a doctor" has become the norm. Registration, fees, inspections, and inspections have long waiting times in line [11]. Access to medical care for patients presents difficulties.

For the office application of medical staff and managers, the current hospital intranet management office cannot keep up with the current development trend of the mobile Internet, resulting in protracted procedures, long approval time, untimely communication, and low office efficiency. As medical staff, the speed of response to critical values also brings hidden dangers to patient safety. As a manager, it is impossible to understand the operating status of the hospital anytime and anywhere, which brings inconvenience to management decision-making. These low-efficiency operation problems provide an opportunity for the development of mobile "online" technology [12, 13].

For the above analysis, the mobile Internet provides medical services and mobile office functions [14–16], improving the hospital's work efficiency and information service level. The main research direction of this topic is based on the construction and application research of mobile security aggregation business management platform[17]. Provide high-quality medical conditions through information-based online technology combined with high-quality offline medical environment, and use mobile office to optimize internal management and medical service processes, which is convenient for medical care and hospital managers, improves office efficiency, simplifies processes, and more Good service to sick patients. At present, on the basis of adapting to the general environment of medical reform, our hospital optimizes its own medical treatment process, improves the quality of medical service [18], and constantly adds innovative information means to make "information" run more, so that patients with diseases and their families can walk less. Effectively facilitate patients, improve patients' medical experience, and build a harmonious doctor-patient relationship [19, 20].

2 Research Significance

At the end of 2017, the total number of 4G users in China reached 860 million. Under the wave of "Internet+", smart healthcare has become the ultimate goal of medical informatization. In the era of mobile Internet, the provision of medical information and medical services through mobile communication technology has become the key content of medical information construction. The trend of medical mobility has basically taken shape, and the transformation of medical management mobility is also imperative.

In the general environment of the trend of hospital intelligence, the number of hospital information systems is increasing, and there are more and more supporting manufacturers for each system. There is an increasing demand for mobile use of hospital systems for maintenance and management. Clinical users and The person in charge of the function cannot stay in front of the hospital computer all the time to deal with emergency medical treatment, emergencies, epidemic reporting, clinical data query, etc. at the same time, due to the professionalism of medical management, authorized personnel must be able to deal with the responsibility through the computer Obviously, the timeliness and convenience of medical management and the urgency of clinical application have become prominent contradictions in medical project management.

At the same time, there are more and more mobile applications in hospitals. If the mobile application system needs to be accessed outside the hospital, it must complete the VPN security authorization access by itself. The hospital cannot manage the operation and maintenance in a unified manner. Inconvenient, while increasing the exposed surface of external security.

3 Research Content

The main innovation of this study is to use the self-developed mobile terminal platform to study the transformation of mobile applications such as hospital medical management, reporting and review, and epidemic reporting.

Taking the Changshu No. 2 People's Hospital as an example, in combination with the actual clinical business environment and the security boundary of data exchange, the important clinical application and medical management of the hospital are completed within the theoretically divided area by using the data transmission technology that meets the safety standards The effective data is centralized, so as to establish a customized standard software application system.

At the same time, security reinforcement is carried out for the VPN system, and the VPN deployment architecture is optimized. In actual deployment, the VPN device must be deployed outside the data center, and IPS and other devices must be deployed on the incoming and outgoing directions of the VPN device. On the one hand, IPS and other devices can defend against VPN attacks, making it more difficult for attackers to attack; on the other hand, when an attacker obtains VPN permissions and scans network segments, the relevant devices will immediately alarm, thereby greatly improving the time when encountering an attack. Defense response speed. Moreover, since the VPN is deployed outside the data center, the data center's firewall, IPS, WAF and other equipment can protect against attacks on important servers initiated from the VPN, preventing the situation of "one-click breach, and the entire network is lost".

Further strengthen the security management of VPN devices Separate the management interface and user interface of VPN devices, adopt ACL control, the management interface of VPN devices can only be accessed through the bastion machine; restrict unnecessary ports such as Redis of the device from being accessed by unauthorized IP; Strengthen threat intelligence, monitor the vulnerabilities of VPN equipment, keep in touch with manufacturers and upgrade and strengthen equipment in a timely manner.

Strengthen the access control strategy of VPN users Strengthen the management and control of VPN users and set up necessary groups, different groups have different permissions, and refine the management and control strategies, such as setting up medical and student groups, and controlling their access scope. Strengthen the management of privileged personnel, set policies to strictly manage the operation and maintenance personnel of equipment and information systems, and restrict such personnel from the policy to only access the IP of the bastion machine after logging in to the VPN. Finally, restrict the access of VPN to prevent users in the hospital from accessing the Internet and campus resources through VPN agents.

For lateral penetration attacks after the VPN obtains permissions, VPN vendors are required to build a complete log system and strengthen log auditing. The VPN system log should at least include information such as account number, login IP, acquisition IP, access IP, access protocol, access URL, and concurrency. In addition, the VPN system and security products should adopt a unified NTP server to ensure the consistency of log time of various devices. In addition, the VPN system must use Syslog, Rsync, Kafaka, etc. to connect with third-party logs or situation platforms. After comprehensive log analysis, it can analyze and judge in the first time and effectively trace the source. See Fig. 1.

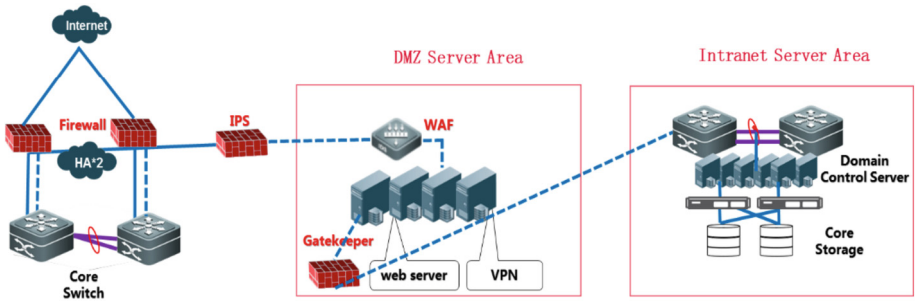

Fig. 1. Network Topology Diagram of Security Devices

4 Key Technologies

Use mobile means to transform the original working method, and unify the management method to make it more efficient, timely and convenient, reduce the workload of medical staff and management personnel, and can also warn hospital staff at any time about the patient's condition (critical value), and track the approval in the hospital through mobile

Changes in the matter process, etc., can better solve the urgent needs of hospital feeling, public health department personnel's mobile quick information inquiry and reporting process when they leave the hospital under the current epidemic situation. Through the management method of safe aggregation, the research on the integration and integration of all mobile systems in the hospital will provide the basis for the development and application of intelligent hospitals. The self-developed mobile platform has added security management and monitoring functions to create a scalable, high-efficiency and high-security network service platform. On the security aggregation platform, the identity requirements of mobile office workers can be strictly authenticated and monitored, and at the same time ensure sufficient security when data is transmitted on the Internet, which can meet medical confidentiality and privacy and prepare for the expansion of many users in the future.

5 Architecture Design

According to the mobile terminal SDK integrated development kit provided by the VPN manufacturer, develop and realize the external network mobile terminal login VPN, realize the function of accessing hospital business resources (including APP and other applications) on the mobile terminal, and manage the authorization of each account to access the corresponding authorization according to the system authority The functionality of the application.

5.1 Business Management Platform

Business architecture: users log in to the security aggregation service platform through VPN to obtain a list of authorized applications, users start the authorized applications on the mobile phone, and the mobile applications access resources in the hospital through VPN.

Application management: Configure the application entrance of each software manufacturer. The application is divided into web pages and mobile APPs. Relevant information needs to be filled in, including: the web page provides the URL address of the web page, application name, icon, and manufacturer-related information provides the path for external calls allowed by the APP, and related calls Parameters, icons, manufacturer-related information.

Authorization management: User management, the list of users allowed to log in to the mobile security aggregation platform, needs to be configured in conjunction with the VPN account. Authorize the corresponding application access rights with each user, so that authorized users can only see the list of authorized applications.

Log management: View usage, error reporting, and exception log records.

5.2 Mobile Functions

VPN access: Direct access to various applications or addresses in the hospital intranet through the VPN gateway function in the case of an external network. Users log in to

the application through their own accounts. The user turns on the VPN through the VPN account. Launch the desired app or access the desired network.

Obtain application list: After successful VPN login, the list of accepted applications is automatically obtained from the mobile security aggregation platform according to the interface definition, and displayed on the interface.

Start the application: the user clicks the application icon to enter the application, and the web application directly opens the embedded browser. The APP application starts the application through the authorization path. Automatically report the enabled applications, which is convenient for statistics on the system platform.

5.3 Function Realization

The system functions are mainly divided into three parts, the mobile phone end, the server end, and the interface end. After the mobile phone end and the server end are dialed through VPN, data exchange is realized through interface interaction. See Fig. 2.

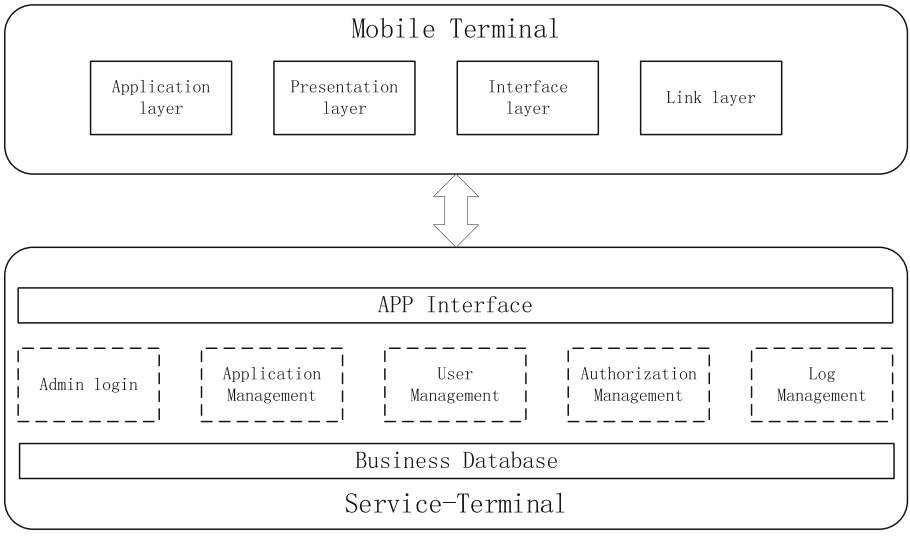

Fig. 2. Schematic Diagram of System Function Realization

6 Summary

On the basis of using the mobile terminal security aggregation business management platform, the hospital's mobile business systems are managed in a unified manner and a secure data exchange channel is established to solve the cumbersome management and application problems of different service platforms within the hospital. Provide a unified and stable platform support for clinical management on the mobile terminal, provide a new perspective for the development of mobile clinical medical business in medical

management research, and optimize and expand in combination with the development needs of hospital smart services and smart management to achieve independent and reliable platform development Finally, we will cooperate with mature mobile technology and information big data companies to promote it to other regional medical communities.

References

1. Marchenko, R., Borremans, A.: Smart hospital medical equipment: integration into the enterprise architecture. In: Digitalization of Society, Economics and Management: A Digital Strategy Based on Post-pandemic Developments. Lecture Notes in Information Systems and Organisation, vol. 53, pp. 69–84 (2022)
2. Levina, A., Iliashenko, V.M., Kalyazina, S., Overes, E.: Smart hospital architecture: IT and digital aspects. In: ASBC 2021. LNNS, vol. 387, pp. 235–247. Springer, Cham (2022)
3. Gourisaria, M.K., Agrawal, R., Singh, V., Rautaray, S.S., Pandey, M.: AI and IoT enabled smart hospital management systems. Stud. Big Data **114**, 77–106 (2022)
4. Wijethilaka, S., Porambage, P., De Alwis, C., Liyanage, M.: A comprehensive analysis on network slicing for smart hospital applications. In: IEEE Consumer Communications and Networking Conference, CCNC, pp. 276–279 (2022)
5. Alsbou, N., Price, D., Ali, I.: IoT-based smart hospital using cisco packet tracer analysis. In: IEMTRONICS 2022, 2022 IEEE International IOT, Electronics and Mechatronics Conference
6. Wijethilaka, S., Porambage, P., De alwis, C., Liyanage, M.: A comprehensive analysis on network slicing for smart hospital applications. In: 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 276–279 (2021)
7. Kumar, A., Dhanagopal, R., Albreem, M.A., Le, D.-N.: A comprehensive study on the role of advanced technologies in 5G based smart hospital. Alexandria Eng. J. **60**(6), 5527–5536 (2021)
8. Omarov, B., et al.: Smart hospital: automation of business processes in medical centers. In: ICCIKE 2021, pp. 106–111 (2021)
9. Chuma, K.G., Ngoepe, M.: Security of electronic personal health information in a public hospital in South Africa. Inf. Secur. J. Glob. Perspect. **31**(2), 179–195 (2022)
10. Kardaras, K., Lambrou, G.I., Koutsouris, D.: Security methods and approaches for internal and external network hospital information systems with single sign-on. Int. J. Electron. Secur. Digit. Forens. **11**(4), 434–446 (2019)
11. Avianto, H., Ogi, D.: Design of electronic medical record security policy in hospital management information system (SIMRS) in XYZ Hospital. In: ICAITI 2019, pp. 163–167 (2019)
12. Pereira, B., Pavão, J., Carreira, D., Costa, V., Rocha, N.P.: A security review of a portuguese hospital using the cyber security framework: a case study. In: Antipova, T. (ed.) DSIC 2021. LNNS, vol. 381, pp. 367–378. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-93677-8_32
13. Brodin, M., Rose, J.: Mobile information security management for small organisation technology upgrades: the policy-driven approach and the evolving implementation approach. Int. J. Mob. Commun. **18**(5), 598–618 (2020)
14. Zhang, X., He, Y.: Information security management based on risk assessment and analysis. In: 2020 7th International Conference on Information Science and Control Engineering (ICISCE), pp. 749–752 (2020)
15. Tariq, M.I., et al.: Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. Sensors **20**(5), 1310 (2020). (36 pp.)

16. Awang, N., et al.: Identification of information security threats using data mining approach in campus network. In: Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future (PACIS 2020) (2020)
17. Hina, S., Dominic, P., Durai, D.: Information security policies' compliance: a perspective for higher education institutions. J. Comput. Inf. Syst. **60**(3), 201–211 (2020)
18. Wang, Y.: Network information security risk assessment based on artificial intelligence. J. Phys. Conf. Ser. **1648**, 042109 (2020). (8 pp.)
19. Wang, C., Jin, X.: The researches on public service information security in the context of big data. In: ISBDAI 2020, pp. 86–92 (2020)
20. Kang, M., Hovav, A.: Benchmarking methodology for information security policy (BMISP): artifact development and evaluation. Inf. Syst. Front. **22**(1), 221–242 (2020)