ATLANTIS PRESS
Advances in Engineering Research (AER), volume 61
International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2017)

The Research on Key Techniques of Cross-Domain Data Services

Xinming Yin [a], Haiping Jiang, Haiye Huang, Junhao Bi, Zhiwei Cao

Information Security Technology Division, The Third Research Institute of Ministry of Public Security, Shanghai 201204, China

[a]yinxm6@163.com

Keywords: Cross-domain security, Data sharing, Unidirectional transmission, Physical isolation.

Abstract. With the deepening development of Internet plus and cloud computing, big data technology constantly breakthrough in the field of application, cyber security becomes an important research field which can't be ignored in the information environment nowadays. Besides, with the development of the business, there are more and more demands on safe and effective data sharing among the different networks and heterogeneous systems. This paper researches the key technologies for cross-domain data services and proposes a cross-domain security data sharing technology. The technology combines physical isolation with proxy service dynamic configuration on data security sharing. Through analysis and verification, the proposed approach is able to carry out data fields and services mapping transformation in heterogeneous system, which can achieve safe and effective data sharing.

1. Introduction

At present, with the rapid development of information technology, informatization has deep into the government organs and institutions. The information systems for different businesses also arise at the historic moment. However, most of these business information systems construct independently. There are many differences in the system architecture, application model, database selection. It can't directly conduct information sharing. These systems become the "information island", which hampers the rapid development of the "e-government" and the informatization in industry. Information sharing platform is an important part of the public foundation platform for the informatization in industry. It is a hub to realize the information sharing between various systems and services. At the same time, security issues are also increasing. Under the premise of data cannot be directly shared between the networks at different levels of security, it has become the current urgent security issue, and may lead the leaks of sensitive information from the networks at high level of security to the networks at the low level of security [1-4]. At present, in order to ensure the security of data sharing between networks in different domains, the significant networks in most government agencies separate from each other with physical isolation. But the technology terminates the extension of the handshake protocol, and one can't directly use the WebService, XML-RPC, ESB to implement the request and response of service. It is unable to effectively control the leakage of sensitive information if the shared data are completely exposed to the requester. Only in the form of human review, artificial authorization and screening on shared data, the data is ferried to the requester through the unidirectional transmission system [5-9]. This paper proposes a kind of security data sharing technology among different domains with the physical isolation transmission technology, which can carry out data field mapping and transformation among heterogeneous systems in networks with different levels of security, configures the data and services shared by various systems, realizes the efficient transmission shared data automatically [10-12].

2. The key technical analysis

2.1 System architecture

The system architecture of this cross-domain security sharing platform is shown in figure 1:

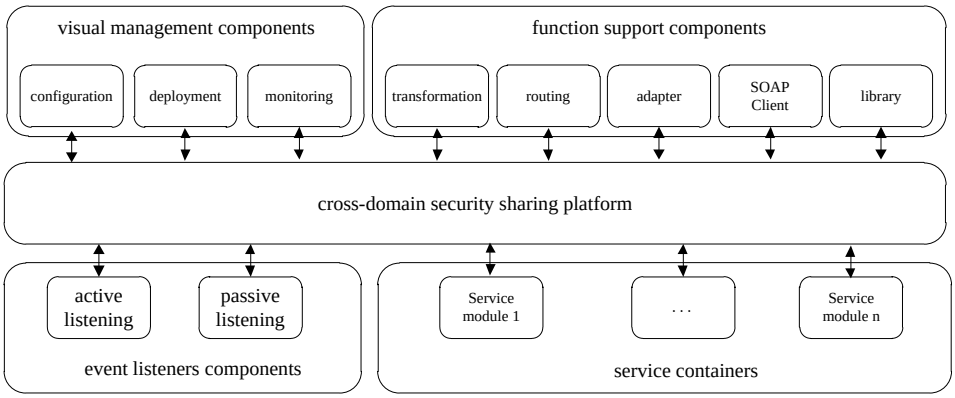

Fig. 1 The system architecture diagram

This system is mainly composed of four components: visual management components, function support components, event listeners components and service containers. Visual management components provide dynamic configuration and deployment of sharing platform by the Web interface, and real-time monitor the running status and system load conditions. Function support components provide core functionality of sharing platform, including the message format transformation, content-based routing, Web services calling, as well as safety control, to support the specific service configuration of the platform; Event listeners components detect real-time events, combined with active and passive way of listening, the event data unified into the message as the platform standard and perception itself format; Service containers may deploy, encapsulate, apply the service modules of the specific integrated operation logic and be responsible for resolving the configuration of the platform, registering the service component unified as a service to the registry library. That division of labor and collaboration between service components, and the clear overall structure ensure the reliability of the data integration.

2.2 Service definition based on WSDL

Web Services Description Language (WSDL) is a standard method which describes the service interface definition language. It provides service providers with the method which describes the remote method invocation (RMI) request and response message format. WSDL does not depend on the underlying protocol and code requirements. It is a kind of abstract language, and one can use its parameters and data types to define the release operation. Developers use WSDL documents to describe a set of operations supported by services, including operating object types, the formats of the specific network and data coding schemes desired by input and output, which constitute the core of the service interface definition.

Based on the medium of the WSDL document, it connects service requesters and service providers in different networks, provides smooth and effective service and data transmission. Its schematic diagram is shown in figure 2.

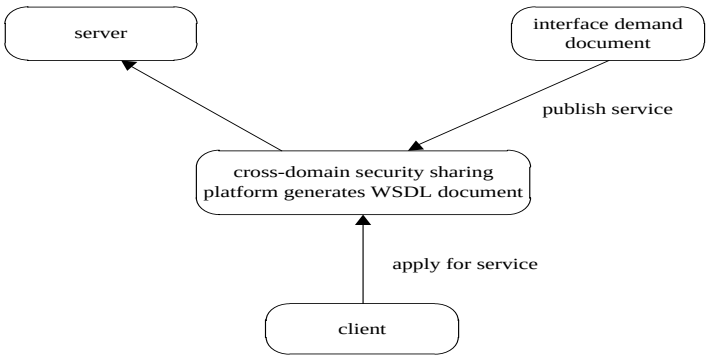

Fig. 2 The client and server docking

2.3 The service data type mapping

Service providers and requesters are in the networks of different security domains. The original service description need keep confidential. To prevent the leakage of the original service description, it provides the basic description of services requested by requesters. So it need to generate a new

information service description documents from the original service description by a mapping transformation and make it meet the basic requirements of the requester. Assume that the service description of a service as S, request demand as Q, mapping transformation as f, the requester hope to get the basic service description as S ' ,so so f: S(Q)→ S ' (Q).

That f as an algorithm provided by the service with the method of visual drag-and-drop. It may regularization deduce to generate a new information service description using service names, service types, message types, service request parameters, the service returns in the original service information. Assume that an original service information described by WSDL document. When it receives the cross-domain request which needs to consider the service information hiding, and use the service mapping method to map the original service description. Then, it generates a new _WSDL document. Then the _WSDL document will be transmitted to the requester. The service description obtained by the requester only meet cross-domain request expected by the actual amount of information. The requester can't know the actual service description. It can effectively protect the service information privacy.

2.4 Services mobilization and control

Cross-domain data sharing among heterogeneous systems can be converted into resources and services sharing. Service providers provide services to the requesters. Service calls and control mainly map, control and forward by the agent of the client and server. The client agent forwards service requests and returns the responses from the server. The server agent receives service requests and transfers to the server, and receives the responses from the server and transfers to the client.

Assuming that system A as the server, it publishes a service: according to user's keyword query user information, the system A provides data template (data template contains the user requests and responses data) to configure on the sharing platform (data mapping, IP, port, etc.), and generates the WSDL configuration file through cross-domain security sharing platform. When the client system B needs to use the services of A, system B needs only apply for this service from cross-domain security sharing platform. After applying successfully, cross-domain security sharing platform will initiatively send the WSDL configuration file from the service to the client. The client writes the client logic implementation according to the WSDL configuration file. A and B are need to register on the cross-domain security sharing platform. And publishing services and application services need the relevant platform personnel to review. Business processing sequence diagram is showed in figure 3.

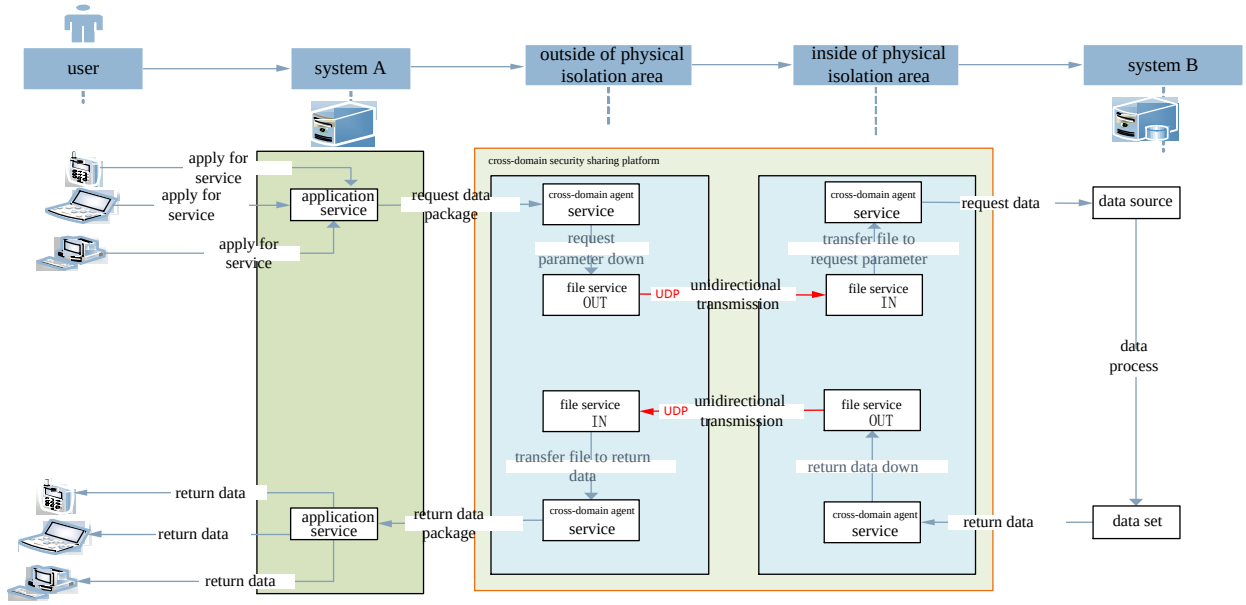

Fig. 3 Business processing sequence diagram

2.5 The safety transmission of the WSDL configuration file

The service description is based on WSDL. To prevent the WSDL data from been tampered or fake, this paper adopts the bidirectional authentication and key negotiation generation technique based on the asymmetric certificate. On the basis of that, we encrypt transmission with the digital signature.

2.5.1 The bidirectional authentication based on the asymmetric certificate

Before starting transmission of the service description, bidirectional authentication based on public key private key mechanism, ensure that the request for the service and the identity of the authenticity, this method need to be in before the start of the service public key exchange. As shown in figure 4.

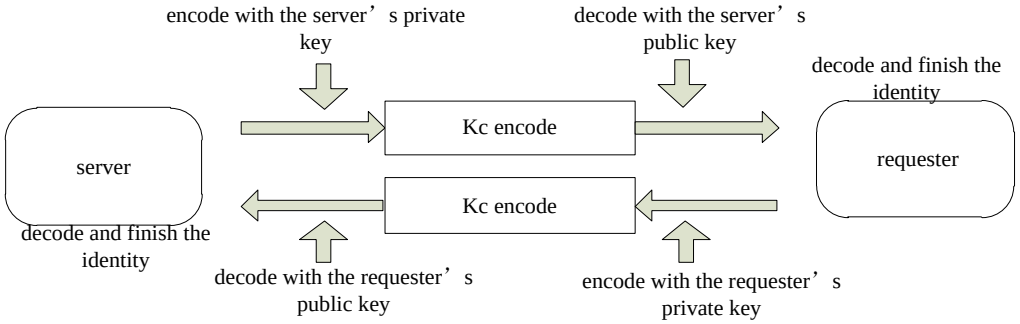

Fig.4 The bidirectional authentication based on the public key

2.5.2 The key generation based on the asymmetric keys

In order to ensure that the data can’t be cracked and tampered with, before the service information transmission, it encrypts data with the public key and private key. This method need to carry out the public key exchange before starting service, as shown in figure 5.

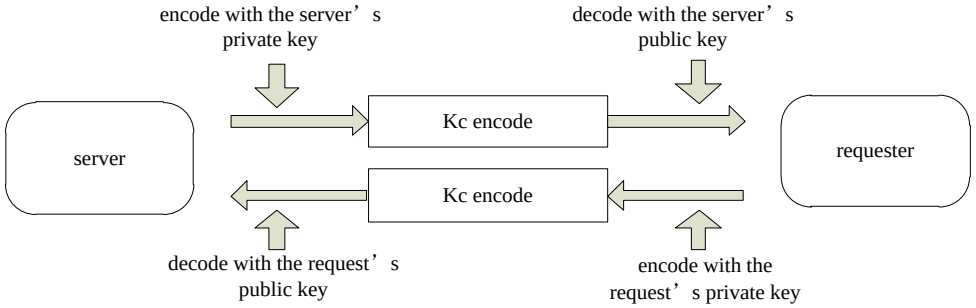

Fig. 5 Custom encryption key by own

2.5.3 The watermark technology against forgery and tamper-proof

With the visual drag-and-drop, the system may generate the new service description. Thus, it may generate the configuration file of the service description with the watermark technology against forgery and tamper with. Last, the system transmits the file to the requester. As shown in figure 6.

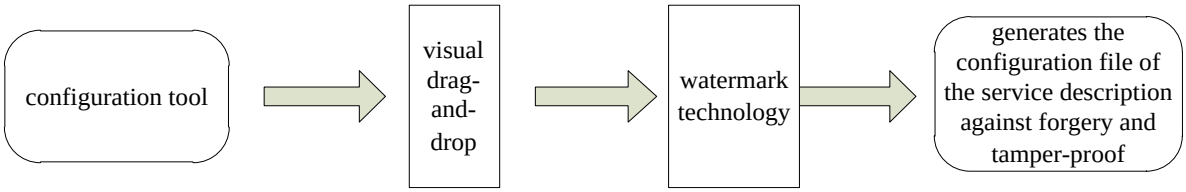

Fig.6 The watermark against forgery and tamper-proof

3. Conclusion

This paper proposes a data security sharing method using the physical security isolation technology, which ensures the safety of the data unidirectional transmission and effectively keeps sensitive information from leaking among application systems in different networks. Packaging the service description based on WSDL on the application layer can prevent that the service description fully exposed to the requesters across domains. It uses the flexible configuration method, such as visual drag-and-drop to process, control, transfer the original service description, then the method generates the new service description document with the way of services mapping. In order to meet the demands of the requester, the method provides a new service description. WSDL hides the detailed description of the service, which effectively guarantees the information security of the server. To ensure the security of the service description transmission, the bidirectional authentication and key negotiation generation based on asymmetric certificate, the watermark technology against tamper-proof and forgery,

effectively guarantee the safety and reliability of the data and the transmission. Considering that when updating and changing the business, stopping and restarting Web services will impact business, the service dynamic invocation and Web service hot deployment mentioned in this paper play a role in the practical application?

References

[1]. HE Liang,FENG Dengguo,WANG Rui.MapReduce-Based Large-Scale Online Social Network Worm Simulation.Journal of Software,2013,24(7):1666-1682.
[2]. YAN Xixi,MA Zhaofeng,YANG Yixian.A Distribution Protocol Based on Proxy Re-Encryption in Domain Environment of E-Document Management.Journal of Beijing University of Posts and Telecommunications, 2012, 35(5): 81-84.
[3]. ZHANG Mingde,ZHEN Xuefeng,LV Shuwang,ZHANG Qingguo.Research on Trust Degree of Authentication.Computer Science,2011,21(11):43-47.
[4]. LIAO Ziyuan,WANG Wei,CHEN Mingzhi.Research on Trust Model for Security Strength Evaluation of Cloud Computing.Netinfo Security,2016(7):15-19.
[5]. ZHANG Yongqiang,LU Weilong,TANG Chunming.Research on An Efficient and Practical Cloud-based Digital Signature Scheme.Netinfo Security,2016(7):1-6.
[6]. LIN Wen,SUN Wenbo,MENG Kun.Cloud Computing Security:Architecture,Mechanism and Modeling.Chinese Journal of Computers,2013,36(9): 1765-1784.
[7]. ZHENG W, XU P, HUANG X. Design a cloud storage platform for pervasive computing environments. Cluster Computing, 2010, 13(2): 141-151.
[8]. HUANG Q L, MA Z F. Secure data sharing and retrieval using attribute-based encryption in cloud-based OSNs. Chinese Journal of Electronics, 2014.
[9]. Ruj S, Nayak A. A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids. IEEE Transactions on Smart Grid, 2013, 4(1):196-205.
[10]. Hu H, Ahn G, Jorgensen J. Multiparty Access Control for Online Social Networks: Model and Mechanisms.IEEE Transactions on Knowledge and Data Engineering,2013,25(7): 1614-1627.
[11]. HONG Cheng,ZHANG Min,FENG Dengguo.Achieving efficient dynamic cryptographic access control in cloud storage.Journal on Communications,2011,32(7):125-132.
[12]. AO L, SHU JW, LI MQ. Data deduplication techniques.Journal of Software, 2010, 21 (5):916-929.
[13]. WU Hao.Research on Data Redundancy Technologies of Distributed File System Based on HDFS.Xidian University, 2011.
[14]. MA Zhuo,MA Jian-Feng, LI Xing-Hua,JIANG Qi.Provable Security Model for Trusted Network Connect Protocol.Chinese Journal of Computers,2011(9):1669-1678.
[15]. ZHAO Boting,LI Fei,MU Pengzhi.Study and Design of Safe One-way Information Transmission Equipment .Computer Application and Software,2010,23(6):98-99.