Analysis and Countermeasures of Data Sharing in the Network Environment

Lei CEN
Department of Information Science & Technology
Guangxi College of Education
Nanning, 530023, China

***Abstract*—This paper puts forward the framework of sharing data model based on the secure multiparty computation, carries on the design according to the hierarchical structure to progressive realize. The model consists of three layers, the lower is the data access, which manage the data from the node in each domain. The middle layer is a function main body layer, providing various atomic operation based on multi-party secure computation. The top layer is the user interface layer, provides a unified interface for the application, which is convenient extension for cross domain communication.**

Keywords: Network security; Cross- domain authentication; Data sharing; Symmetric encryption

I. INTRODUCTION

With the development of Internet and popularity of smart mobile devices, people contact and use Web application system in daily life is more abundant. In the mobile Internet and Web application trend of rapid development, many traditional distributed tight coupling application is also gradually to be loosely coupled Web application development direction. The security field in the Internet, cross domain authentication and related technology in recent years is the popular research [1-3].

The so-called cross domain authentication, is actually a way to verify the identity of the user in a computer network, through this certification, the user can access to the other domain resources in a domain, instead of going by several identity authentication in multiple domain radius. Similarly, in the research field of cross domain recognition card technology, Web certification loosely coupled tightly coupled scheme also has the traditional authentication scheme and more and more popular in these two categories. The former generally requires dedicated infrastructure, security requirements to high [4]; the latter stream communication based on the Web data, more emphasis on flexibility and the cost of deployment and other factors [5]. In addition, various other certification related technology is also in rapid development. In terms of security, the current network crime is very frequent in harm way, many harm have to globalization, cooperation attack the direction of evolution, if the operator network domain only rely on local information to deal with, obviously against the crime of the network is negative. So in the improvement of network security and network monitoring level, cooperation cannot be ignored.

II. THE ARCHITECTURE DESIGN OF SHARING MODEL

The whole network data sharing model based on secure multi-party computation is adopted to design the hierarchical structure, which is as shown in figure 1. The whole model is divided into three layers, the bottom layer is the data provided layer, the middle layer is the core calculation layer, and the upper is application layer. The data provide the receiving participant data input, data for network measurement data, participants were declared at this level, some necessary environmental statement itself, such as its IP and its ports are essential, this statement process similar to a registration process, let themself become a process of application participants. The computation layer complete the work that is a variety of protocols and algorithms of secure multi-party computation for atomic, then a unified control those atomic operations provide the interface to the upper application. The upper layer is the application layer, network application calls for secure multi-party computation of atomic operations to complete network data sharing.

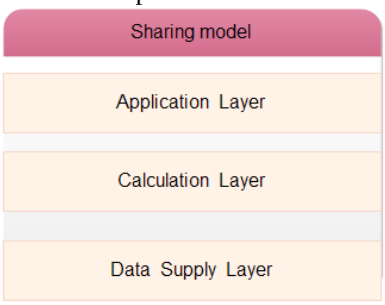

Fig.1 Model hierarchical structure diagram

A. The relationship between the node structures

From the point of view, each participating node are equal, this means that the capacity of each node exactly is the same permissions, won't appear individual different abnormal, change to the function level or code level, structure of each node is basically the same, the local environment configuration will vary slightly. But this does not affect the secure multi-party computation process. Because the environment is in the absence of a trusted third party, the semi honest environment, so the calculation process is a collaboration between nodes to achieve. Therefore, a simple example to secure three party calculation, structure of system node and inter node should be as below 2 shows.

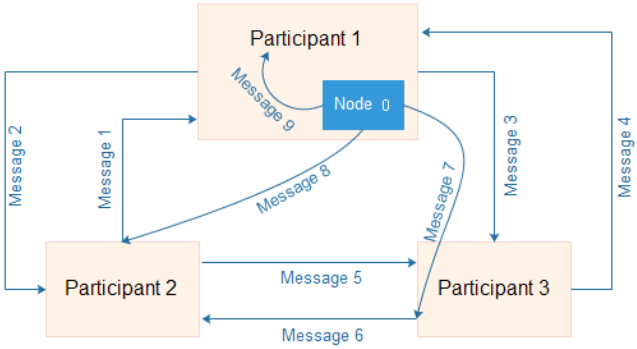

Fig.2 The relationship between the node structures

B. *The internal structure of nodes*

The internal structure of each node are basically same, they need to complete the function of the same steps to get the final result in secure multi-party computation process. Network data sharing model use the hierarchical structural in the internal nodes in this paper. According to the concept of network protocol, the lower layer provides the interface to the upper layer, the upper call interface to complete the relevant application. The internal nodes is divided into three layers, the bottom layer is the supply data, the supply data layer receive node that input data, nodes are declared in this level, and some essential environmental statement, the node complete registration process with a statement in this layer, make oneself become one of application nodes. The middle layer is the core layer calculation, calculation layer to complete the work is a variety of protocols and algorithms of secure multi-party computation for atomic, then a unified control those atomic operations provide the interface to the upper application. The upper layer is the application layer, network application is in this layer to achieve. Network application calls for secure multi-party computation atomic operations to complete network data sharing. The basic hierarchical structure of single node is as shown in figure 3.

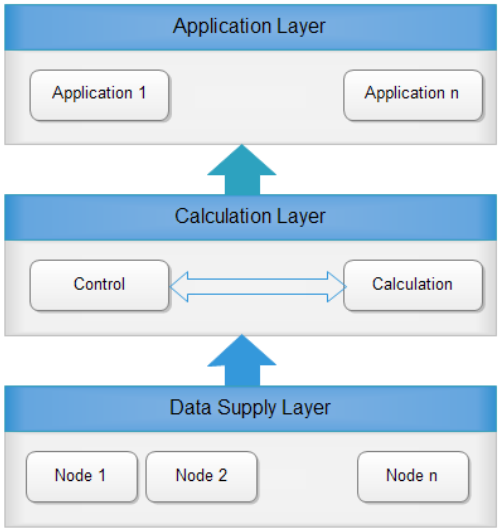

Fig.3 The internal structure of node

III. THE DESIGN AND IMPLEMENTATION OF SHARING MODEL

A. *The master control module*

The master control module is the core part in the whole data sharing model. This module interacts with other multiple function modules, integrated control of each safety calculation process, it is responsible for the control of interactive, connection management, data sharing, to run the calculation and other functions. The module is defined as the platfomi module, the module and the other modules will be scheduling, the relative relation is as showed in figure 4.

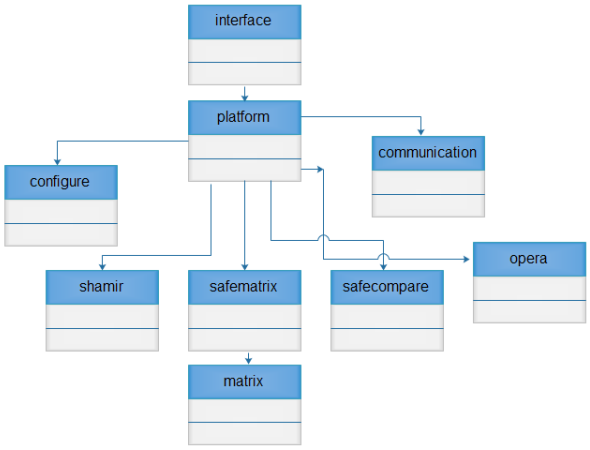

Fig.4 Chart of platform class module

The platform module defines the platform class, this class will return object of a node, and the platform object will save node's private information and the other nodes identification information.

```
class Platform:
def_init_(self，plaver.A_matrix):
self.port=None
Player[self.id = "playerid"]# own ID
Self.matrix=A_matrix
Self.players={}# node list of friends
Self.players[player["playerid" "= player# himself into a list
self.num_players=1# The number of nodes
Save self.protocols={}# link
Self.matrixDict={}
self.num matrixDict = 0# The number of above Dictionaries
Self.matrix_PPY=None
Self.squareSumList ={}# deposit square and list, self.matrix.row
Self.squareSumList_last = None# is 1 *t matrix type
Self.matrix_square_parts={}# deposit square and divide
Save self.listOne_ip=[]# Shamir first list
Self.listOne_visit=[]# memory Shamir first list
Self.list_ save shamir=[]# list the results after Shamir
```

B. *Design and implementation of asynchronous communication module*

The interactive function of secure multi-party computation sharing model between node and node is

provided by the communication module in the paper. Shared communication module model adopts asynchronous non-blocking implementation, so it do not wait after sending data, but directly following operations can be performed at run time, wait until the other side return data in time, will call the procedure returns processing function. This way you can save a lot of waiting time program, improve program of time utilization rate. This module uses the twist Library in Python language to write, this is very widely used asynchronous non-blocking network programming library. Data sharing asynchronous communication module in the model mainly consists of three parts, one part is a protocol module, a part is the factory module, and the third part is a return to the processing function part.

The protocol module defines the connection class, the class that contains the relevant operation involves a connection, the code is as follows:

```
class Exchanger(lnt32StringReceiver):
MAX_LENGTH = 9999999
Def_ink_(self):
self.peer_id = None # Link your ID
….
def connectionMade(self):
def connectionLost(self，reason):
def stringReceived(self，stri):
```

The factory module unified management all link, the factory module will specify connection type protocol factory management, this kind of code:

```
class ExchangerFactory(Reconnect!ngClientFactory ，ServerFactory);
protocol = Exchanger
def_ink_(self’ platform，players，protocols-ready):
self.platform = platfomi
self.players = players
self.needed_protocols = len(p!ayers)-l
sdf.protocols_ready = protocols_ready #create_runtime return deferred
def identify_peer(self，protocol):
self.platform.add_player(seIf.players[protocoLpeer_id]，protocol)
self.needed_protocols -=1
if self.neededjrotocols =0:
self.protocols_ready.calIback(self)
```

IV. THE EXPERIMENTAL RESULTS

We conducted a performance test for the model application, it respectively were tested in three groups of data sets X01, X06, XII, table 1 gives the running schedule with three groups of test, we can see that the application of the data sharing model frame is stable.

Table.1Application performance test

True Data 400*144Matrix	DATASET	Multiparty safety computation results		
		Start Time	End Time	Run Time
	X01	1326540746.42	1326540879.23	132.81
	X06	1326541682.92	1326541813.94	131.02
	X11	1326542516.98	1326542629.68	112.7

V. CONCLUSIONS

This paper introduces the frame structure of the network data sharing model based on secure multi-party computation, first introduced the overall structure and the relationship between node and node, that every participant is equal, its ability is exactly the same permissions. And the paper introduce the internal nodes of the structure, adopts a layered architecture thought, the internal nodes of the structure is divided into 3 layers, including application layer and data providing layer, computing layer. This paper completed the hierarchical model framework, focusing on the intermediate calculation layer, and finally complete the core control module, asynchronous communication module and other auxiliary modules.

REFERENCE

[1] Liu Guangwei, Zhou Enguang, Yan Hong, et al. An improved cross- realm client- to- client password- authenticated key exchange protocol [J]. Journal of Northeastern University, 2009, 30 (1): 42 - 45

[2] Zhang Hongqi, Zhang Wenbo, Zhang Bin, et al. Study on identity- based cross- domain authentication in grid environment [J]. Computer Engineering, 2009, 35 (17): 160 - 162

[3] Ping Ye. Design and realize the trans- domain authentication platform base on PKI /CA [D]. Beijing: Beijing University of Posts and Telecommunications, 2009

[4] Hu Jianbin, Wang Yonggang, Xin Wei, et al.A novel secret data cross- domain transfer mechanism [J]. Computer Applications andSoftware, 2011, 28 (8): 80 - 82

[5] Ren Zhiyu , Chen Xingyuan , Shan Dibin.Cross- domain authentication management model based on two tier role mapping [J]. Journal of Computer Applications, 2013, 33 (9): 2511 -2515.