Research on Security Portocol of Scheduled Services on Cloud Computing

Li Yang , Chen Xiang
Hangzhou Institute of Service Engineering, Center for Service Engineering Hangzhou Normal University, Hangzhou, China
E-mail:liyangtom@163.com, flyingchen77@163.com

Lu Xiao-ying, Xing Ya-lin
Zhejiang Province communications industry services company, Network technology branch, Market management department, Email:luxy@zjccsnt.com, xingyl@zjccsnt.com

Li Cheng-bin
Educational Technical College, Shenyang Normal University, Shenyang, China, Email:dalicaz@163.com

***Abstract*—With the large growth of wireless sensor network, the current security architecture couldn't solve the problems. This paper provides a security protocol of scheduled service based on cloud computing. The system is consisted of three groups that are domain server domain register server domain and functional server domain. The system encrypts the server address by disconnected message. Then two algorithms are proposed for dynamic key change when system should re-calculate the login key. At last, the performance loss is measured for above algorithms. Meanwhile, the improvement of system is discussed by experiment results.**

Keywords- cloudy; encryption; authentication; security;

I. INTRODUCTION

The security research of cloud computing has two areas: the topology architecture of wireless network and encryption. Some researchers aimed at physical details of wireless communication. Such as Sastry et al. proposed the Echo protocol [1], a modification of the distance bounding protocol that uses ultrasound. Echo algorithm uses RF link for verifier-to-prover challenges and uses ultrasonic link for prover-to-verifier responses. But because of the cloud service, recently people pay close attention to system structure and protocol. Morten[2] present an asynchronous group key distribution scheme with no time synchronization requirements. The scheme decreases the number of key updates by providing them on an as needed basis according to the amount of network traffic. Florian Kerschbaum[3] provides a RFID-Based Supply Chain Partner Authentication and Key Agreement. In this model, users exchange tags over the cycle of a supply chain and, if two entities have possessed the same tag, they agree on a secret common key they can use to protect their exchange of business sensitive information.

Besides above research, some security protocols are designed for the special service application, such as evolutionary design of secrecy amplification protocols[4], self-healing control flow protection[5], practical characterization of 802.11 access points inparis[6] and so on.

The paper provide a security protocol of scheduled service based on cloud computing(SPSS). The server is always in a state of being disconnected. When client send service request, the system sends the error message with register server's IP address. The client logs on to the register server and processes the authentication. After identity authentication, client could invoke service. Once the client invokes service for several times, it has to choose a new function server to re-authentication for security.

II. DISCONNECTION LOGIN MODEL

In the original cloudy service, the customer should take the authentication, in order to invoke the system services. In order to improve the security of the system, we provide a complex authentication system within several stages.

The formal description of SPSS framework is as following:

Definition1. SPSS system is 3-topology 〈S, R, T〉 defined below.

(1) S is the domain server in cloud system. Its task is to send the error message to all the connecting clients, and to record the history information of each node. Once the same user get failure message in the cycle time M, it will get the encrypted address of register server. The history information recorded in domain server is mainly included: the IP address

0076

of connecting node, the time of connect request, the failure times of connect request and encrypted address information sending to client.

$$S = \{sip, DB\}$$
$$\forall t_i \in DB, t_i.\inf \in \{tip, time, fail, sip\}$$

(2) R is the register server domain. When client decryption error message and get the register sever adderss, it will calculate the key and login into a register server. After the server make the identity authentication, it would send the login information and login period to client.

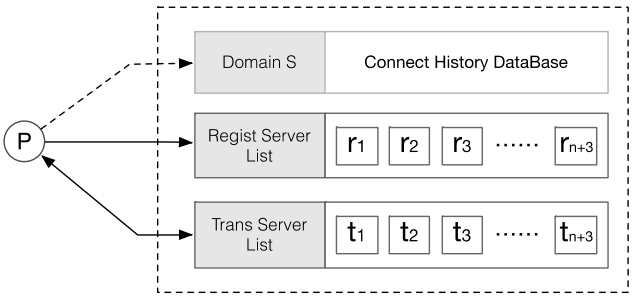

Figure 1. The Architecture of SPSS

(3) T is the function server domain. When the client pass the identity authentication, it should login into a function server before time of Tlogin.

The formal description of service process is as following:

1）First time the client send the key(kc) to domain server in T. The domain server response with the error disconnection message(e).

2）If the same client continues to send requests, the domain server will split the adderss of register server into several parts and send it with error message to customer.

3） After client decrypt the error message and get the address of register server, it should login into the register server within the cycle time of Tr.

$T_r = T_s + calu(P_r)$

$calu(P_r) = calu(P_{r1}.P_{r2}.P_{r3}.P_{r4}) = P_{r1} + P_{r2} + P_{r3} + P_{r4}$

4） After client login into the register server, the register server would send the adderss of function server to client. And then it would login into the function server T_t.

$T_t = T_r + calu(P_t)$

$calu(P_t) = calu(P_{t1}.P_{t2}.P_{t3}.P_{t4}) = P_{t1} + P_{t2} + P_{t3} + P_{t4}$

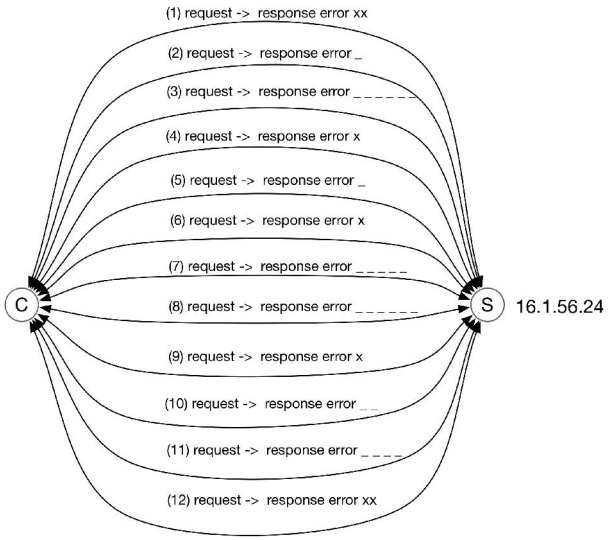

Figure 2. The Architecture of SPSS

IPSBSP(IP Split to Blank Space Protocol)算法描述如下：

IPSBSP Algorithm

1st Connect :

The first time client C connect to Domain S, S return the error information and select a register server(R_s) randomly; S insert the client C's ip and R_s's ip(P_r) into connect history database.

2nd Connect to 22 times Connect:

When the client C connect to domain S the second time, S take out the P_r and split it into several items. Then it construct the array errorList as following:

$P_r = R_aR_bR_cR_d \,.\, R_eR_fR_gR_h \,.\, R_iR_jR_kR_m \,.\, R_nR_oR_pR_q$

$errorList = [**, R_a, R_b, R_c, R_d, *, R_e, R_f, R_g, R_h, *, R_i, R_j, R_k, R_m, *, R_n, R_o, R_p, R_q, **]$

$errorList[0] = [**]$

$errorList[1] = [\underbrace{\_\_\_\ldots\_}_{R_a}]$

$errorList[2] = [\underbrace{\_\_\_\ldots\_}_{R_b}]$

$errorList[3] = [\underbrace{\_\_\_\ldots\_}_{R_c}]$

$errorList[4] = [\underbrace{\_\_\_\ldots\_}_{R_d}]$

$errorList[5] = [*]$

.....

$errorList[20] = [\underbrace{\_\_\_\ldots\_}_{R_q}]$

$errorList[21] = [**]$

S reply the client the error information with the errorList[i]. Until the client get the errorList[21], it will extract the register server's ip address.

III. DYNAMIC KEY ALGORITHM

In order to guarantee the security of the service, after client complete P times of service invoke, it should re-choose the function server and re-calculate the login key.

When the server calculate the new function server with RSA(route select algorithm), it would send the adderss to client. Then the client re-calculate the login key(Kn) by using the time of login into function server(T_r) and current key(Kc) and login into the new function server.

Kn= LoginKey (Tr, Kc);

When the client update function server for n times, the domain sever will take the identity authentication. The client should send the login history of n times to domain server to complete the dynamic authentication.

A service schedule time table is as following:

Table 1. The Service Schedule of SPSS System

1 Request Session	Time of first request to domain S	T_s
	IP of register server IP	P_r
2 Register Session	Time of login into register server	T_r
	IP of function server	P_t
3. Service Session	Time of login into function server 1	T_{t1}
	IP of new function server 1	P_{n1}
	Time of login into function server 2	T_{t2}
	IP of new function server 2	P_{n2}
	.....	
	Time of login into function server n	T_{tn}
	IP of new function server n	P_{nn}
4. re-authentication	IP of register server IP	P_r

In order to improve the efficiency of service, system provides two RSA algorithms.

A. *Nearest Choose Algorithm*

The precondition of the algorithm should satisfies the following conditions:

1. The speed of the client connection is basically the same.;
2. Function server location is determined.;

When the first time of re-choose function server, it would be selected in function server set randomly. After the registration finished, the transfer time of data package would be recorded as T1. The second times it could calculate the T2. According to the intersection of the two circles(S1 and S2), the position of the client has two possible(C1 and C2). The third times, we choose the nearest point(S3) to C1 in the functional server collection. And send the request to C1 and C2 at the same time. Then we calculate the transfer time T(S3-C1)and T(S3-C2). If T(S3-C1) is less than T(S3-C2), the position is C1,otherwise it is C2. All the following times, it choose the most short distance function server from the client.

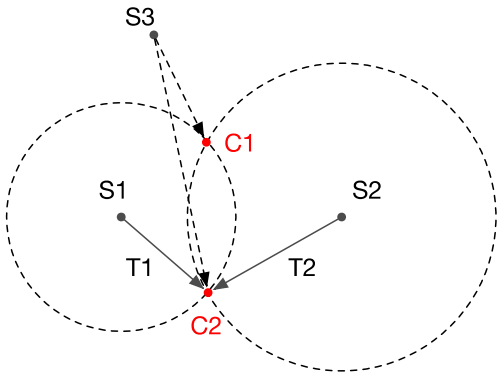

Figure 3. Nearest Choose Algorithm

Nearest Choose Algorithm

```
{ Switch(times)
   case 1: //the first time connect to function server
      R1=T1 * V;
      break;
   case 2: //the second time connect to function server
      R2=T2 * V;
      C(C1,C2)= CircularIntersection(R1,R2,S1,S2) ;
      S3 = SelectNearestDistance(C1);
      break;
  case 3: //the third time connect to function server
      R3 = T3 * V;
      R4 = distance(S3,C1)
     if (R3<R4)
        C = C1;
     else
        C = C2;
     break;
  default: //subsequent connection to function server
      SelectNearnestDistance(C);
}
SelectNearnestDistance (C)
{
   Foreach s ∈ S do {
      dist = sqrt((C.x-s.x) ^2+(C.y-s.y) ^2);
      if (dist<Min) { Nearnest = s; Min=dist; }
   }
   return Nearnest;
}
```

B. *HighPerformance Choose Algorithm*

If the distance between the client and the server is not far away, and the speed of the network is basically the same, the response speed of the functional server is determined at this time.

High Performance Choose Algorithm

```
SelectHighPerformance (C)
{
   Foreach s ∈ S do {
      serviceTime = requestTime - responseTime;
      if (serviceTime<Min) { HpNode = s; Min= serviceTime; }
   }
   return HpNode;
}
```

IV. EXPERIMENT AND RESULT

To test the performance of SPSS system, we construct a platform with Netlogo[9] which using the ECC algorithm to simulate the encrypted transmission environment in wireless sensor network.

NetLogo is a multi-agent programmable modeling environment with java language. The researcher could set the conditions and variables to make experiment for researching the complex system over time.

Experiment1. the performance of Multi-hop Encryption Protocol.

Three groups are selected to invoke the SPSS service and other three groups with the traditional cloud service. We analyze the efficiency of them. The main cost of SPSS system is the decryption of register server address, which is about 82.7%.

Table 2. The Service Schedule of SPSS System

	SPSS System (G1)	Original Cloudy System(G4)
Send request to Domain	675	0
Login into register server	73	0
Login into function server	68	72
Invoke cloudy service	121	117

The main cost of SPSS system is that the client should disconnect at least 12 times for get the address of the register server address which are to synchronous send. In order to improve the performance, we asynchronous send the request at once in the time of the initialization. But when it receive the responses, we decrypt them in order. The re-testing datum is as following in Table 3.

The cost of its decryption phase is reduced to 44.01%

Table 3. The Service Schedule of SPSS System

	SPSS System (G1)	Original Cloudy System(G4)
Send request to Domain	125	0
Login into register server	84	0
Login into function server	75	85
Invoke cloudy service	138	132

Experiment2. the performance of re-choose functional server.

We choose six groups to test the performance of two RSA algorithms, three with nearest-choose choose algorithm (NCCA), three with high-performance choose algorithm (HPCA). The re-choose functional server for each group is tested for ten minutes. The result is as following in Figure4.

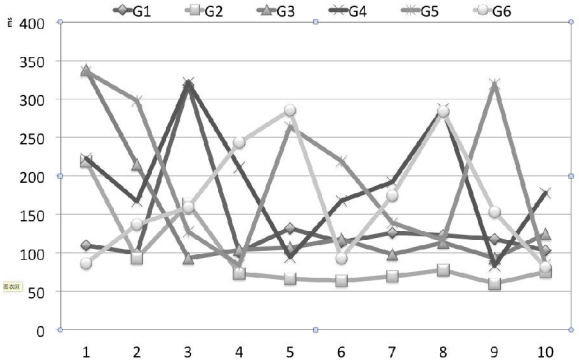

Figure 4. Nearest Choose Algorithm

The stability of the NCCA algorithm is better, for the main cost is the first 3 times to determine the client's position, but the following re-choose of the functional server gain the high efficiency. The stability of HPCA is poor, because of its efficiency is determined by the service efficiency. Therefore, the NCCA algorithm is suitable for the cloud framework in which any pair of nodes has a far distance, while the HPCA is more suitable for small range of service, such as in a LAN.

V. CONCLUSIONS AND FUTURE WORK

The paper announces a security protocol of scheduled service based on cloud computing. It improves two algorithms for dynamic key change. The system can be applied to the examination of the university. The future work will focus on trusted collaboration system for synchronous examination [7].

ACKNOWLEDGMENT

The authors thank the support from project of software development of wireless base station monitoring system based on P2P security and dynamic key(S330017-2014-000328) for zhejiang communications industry services company.

REFERENCES

[1] Stefan Brands and David Chaum, Distance-bounding protocols (extended abstract), In Theory and Application of Cryptographic Techniques, pages 344-359, 1993.

[2] Morten Tranberg Hansen, Aarhus, Denmark, Asynchronous Group Key Distribution on top of the CC2420 Security Mechanisms for Sensor Networks, Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland, 13-20, 2009.

[3] Florian Kerschbaum, Alessandro Sorniotti, RFID-based supply chain partner authentication and key agreement, Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland,41-50, 2009.

[4] Petr Svenda, Lukas Sekanina, Vaclav Matyas, Evolutionary design of secrecy amplification protocols for wireless sensor networks, Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland, 225-236, 2009.

[5] Christopher Ferguson, Qijun Gu, Hongchi Shi,Self-healing control flow protection in sensor applications, Conference On Wireless Network Security, Zurich, Switzerland , 213-224:2009.

[6] Li Xiao-Yong,Gui Xiao-Lin, Congitive Model of Dynamic Trust Forecasting, Journal of Software, Vol.21, No.1,January 2010,pp163-176.

[7] Jerry T. Chiang,Jason J. Haas,Yih-Chun Hu, Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration, Conference On Wireless Network Security archive, Proceedings of the second ACM conference on Wireless network security table of contents, Zurich, Switzerland , 2009, 181-192.

0080