Security Protection Scheme of Brain-Like System Based on Cloud Computing Platform

Haoyu Wei and Nanfeng Xiao *

School of Computer Science and Engineering, South China University of Technology, Guangzhou, China
Email: 422289391@qq.com; xiaonf@scut.edu.cn

Abstract. The functions of human being’s brains are very difficult to simulation by computers, therefore many scientists are focusing on research of brain-like system (or robotic brain) based on cloud computing platform, which can simulate the human being’s hearing, vision, thinking and action. However, due to the security incidents of the internet occur frequently, the robotic brain based on the cloud computing platform may be seriously harm by the security incidents. Therefore, this paper designs and implements of the overall security solution of the robotic brain based on cloud platform. The cloud platform intranet is divided into the intranet trusted zone and the DMZ zone, and strict filtering strategies are set in the zone, and firewalls and firewalls are set up in the DMZ zone and the external network zone. Monitor incoming network traffic at the network interface, and deal with abnormal traffic. At the same time, it audits security events in the intranet, conducts the statistical analysis on content security, server security, and application control, and blocks suspicious attacking IP. A series of safety measures are adopted to ensure the safety of the internal network of the robotic brain based on cloud platform.

Keywords. Cloud computing, robotic brain, cloud security.

1. Introduction

In recent years, with the rapid development of cloud computing [1], it is generally believed that the future development directions of AI are computational intelligence, perceptual intelligence and cognitive intelligence, and the key technologies that AI really needs to break through are to let computers realize these intelligence, such as self-thinking and self-learning [2], and making the computers be robotic brains which are similar to the human being’s brains [3]. At present, the brain-like system (robotic brain) research based on the cloud computing has become a hot topic in the AI fields, as shown in figure 1, because the cloud computing can provide a series of effective mechanisms and algorithms for the data acquisition and the data processing, which can make the intelligent robots and their robotic brains and their learning capabilities have been being further developed.

However, the internet-based cloud computing platform is prone to the dangerous situations, such as technology being leaked, services being eavesdropped, and computing platforms being attacked, which are threaten to the security of the robotic brains [4, 5]. In order to effectively solve the security threats, this paper designs a security protection scheme for the robotic brains based on the cloud computing platform, which will be of great significance for AI and the distributed intelligence based on the cloud computing.
2. Cloud Computing Platform Security Analysis

As a powerful support and protection barrier for the cloud computing, the cloud computing security inevitably faces multiple security threats and security problems [6-9], which includes user data security, identity authentication, virtualization, mobile terminal security, and so on. Recently, many famous cloud security companies have proposed some cloud computing security solutions, and also have provided many cloud computing platforms and their security products (e.g., Alibaba Cloud, Tencent Cloud, Huawei Cloud, and so on). In order to ensure the security of the robotic brain and the cloud computing platform, this paper proposes a reason-able protection scheme for the robotic brain, which includes: (1) the intranet security division of a robotic brain; (2) internal network host security of the cloud computing plat-form; (3) virtual firewall deployment and its configuration scheme; (4) the intranet audit and intrusion tracking. The key security technologies of the proposed protection scheme based on the cloud computing platform are firewall, isolation area (or Demilitarized Zone, or DMZ), intrusion detection technology, and so on, which will be described as follow.

3. Design of the Security Protection Scheme

3.1. Internal Network Security Division

3.1.1. The Intranet Security Division. In order to maintain the intranet security of the robotic brain, it is necessary to identify the potential vulnerabilities as soon as possible, and divide securely the intranet of the robotic brain. And according to the requirements of the proposed protection scheme in this paper, the entire network is divided into an intranet trusted zone, a DMZ zone, and an external zone. Figure 2 shows the intranet division of the robotic brain, and figure 3 gives the network topology map.
In figure 2, the intranet trusted zone mainly includes the host and the servers (intranet core zone) required by the robotic brain for its vision, auditory, thinking and actions, which includes the essential devices and zones such as the application servers, storage zone, and security management zone. The DMZ zone stores the servers and the interfaces such as HTTP, FTP, WEB, DNS, and SSH for the external services. A firewall is set in the intranet trusted zone and the DMZ zone to ensure that the core network services are securely and credibly carried out. The network located outside the intranet trusted area and the DMZ area is the outer network zone. The firewall is set in the interval of the DMZ zone and the external network, and the very strict communication rules are set so as to prevent the excessive detection of the external traffic on the cloud computing platform to achieve a certain degree of the security isolation.

![Network topology of the robotic brain.](image)

3.1.2. The Intranet Configuration. Environmental construction. According to the intranet division, a virtual DMZ environment is built, which is based on VM Workstation and Ubuntun, and install Gns3, Dynamips, and Qemu on Ubuntun. The relative mirror is selected as follows:

- Pix: pix803.bin;
- Internal 1 & Internal 2: c3725-advsecurityk9-mz.124-25d.bin;
- External Router& DMZ Router: c2691-jk9s-mz.123-17.bin.

And a virtual network is allocated for the experiments in the paper, which is shown in tables 1 and 2, respectively.

Configure the firewall: (1) assign IP to the firewall interface. (2) turn on the firewall pix and configure the firewall security features. (3) at the same time, enable the inter-interface routing and use the route aggregation, and allow the intranet access to the DMZ zone.

Configure the DMZ zone: the DMZ router interface information is configured as shown in table 3, which configures the DMZ routing.

Configure the external zone: the external router inter-face information is configured as shown in table 4, and the external router is configured as shown in figure 4.

| Network | Area name     | Subnet IP  | Subnet mask |
|---------|---------------|------------|-------------|
| Vment8  | Internet      | 192.168.146.0 | 255.255.255.0 |
| Vment10 | DMZ           | 192.168.130.0 | 255.255.255.0 |
| Vment11 | Internal Server | 172.16.10.0    | 255.255.255.0 |
| Vment12 | Vision        | 172.16.20.0   | 255.255.255.0 |
| Vment13 | Audition      | 172.16.30.0   | 255.255.255.0 |
| Vment14 | Mind          | 172.16.40.0   | 255.255.255.0 |
| Vment15 | Execution     | 172.16.50.0   | 255.255.255.0 |
Table 2. Firewall interface allocation.

| Ports | Connection       | IP           |
|-------|------------------|--------------|
| e0    | Internal1-f2/0   | 192.168.0.2/30 |
| e1    | Internal1-f1/0   | 192.168.1.2/24 |
| e2    | DMZ Router-f0/1  | 192.168.2.2/24 |
| e3    | External Router-f0/0 | 192.168.3.2/24 |

Table 3. DMZ router interface.

| Ports | Connection | IP           |
|-------|------------|--------------|
| f0/0  | Vmnet10    | 192.168.130.5/24 |
| f0/1  | Pix-e2     | 192.168.4.2/30 |

Table 4. External router interface.

| Ports | Connection | IP           |
|-------|------------|--------------|
| f0/0  | Pix-e3     | 192.168.0.9/30 |
| f0/1  | Vmnet8     | 192.168.146.5/24 |

Figure 4. External router interface configuration.

3.2. Internal Network Host Security

3.2.1. Security Configuration of Intranet Network Devices.

The internal network security is also largely dependent on the configuration of the internal network device. The configuration of the internal network router and the switch is described as follow: (1) log in to the internal1 console, configure the network interface f0/0, and set its working type to “Full Duplex”, as shown in figure 5. (2) encrypt the plain text information on the router and give the router the test.net domain name address, then generate a 1024-bit RSA key pair and set SSH login mode only, as shown in figure 6. (3) then configure the other network interfaces as shown in figure 7, and the network topology is shown in figure 3, and the rest of the interfaces are configured in the same way. Table 5 shows the internal1 interface. (4) configure an ACL (Access Control List) to prevent the unauthorized users from accessing the device, the following is the configuration of f0/0 (Internal_Server). (5) configure the internal 2 in the same way. Table 6 shows the interface configuration of the internal 2. It should be noted that there are ports that are not used in the internal 2 and need to be strictly closed by internal 2 (Config) # interface 1/0; internal 2 (Config)# shutdown.
Figure 5. Internal1 router F0/0 interface configuration.

```conf
azure(config)#enable secret Cisco1
azure(config)#service password-encryption
azure(config)#ip domain-name test.net
azure(config)#crypto key generate rsa
The name for the keys will be: azure.test.net
Use the size of the key modulus in the range of 384 to 2048 for your General Purpose keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
Generating 1024 bit RSA keys, keys will be non-exportable...[Ok]
```

Figure 6. Internal1 router service security configuration.

```conf
azure(config)#interface fastEthernet0/0
azure(config-if)#description tointernal
azure(config-if)#no shutdown
azure(config-if)#ip address 172.16.10.5 255.255.255.0
deluxe
deluxe
azure(config-if)#exit
```

Figure 7. Configuration of the other interface.

```conf
azure(config)#interface fastEthernet0/1
azure(config-if)#description tointernal
azure(config-if)#no shutdown
azure(config-if)#ip address 172.16.10.6 255.255.255.0
azure(config-if)#deduplex
```
3.2.2. Host Personal Security. There are many aspects for the intranet host security. Firstly, the problems of the intranet host key management and the key distribution needs to be solved. A strong and effective password is required. At the same time, the pass-words of the hosts in each zone of the intranet should not be the same, therefore, the rotation system can be adopted, for example, on the intranet: (1) host port. For the host port, a cautious strategy should be adopted to deploy the host firewall according to the principle of the least privilege, and disable the service unrelated to the host service [10]. (2) system update. The intranet individual host systems need to be updated and backed up in time, especially for the real-time major vulnerability protection updates that can often be prevented at the critical moments.

4. Virtual Firewall Deployment and Configuration

4.1. Deploying a Virtual Firewall [11]

Alibaba Cloud deployment. Alibaba Cloud provides the tenants with Virtual Private Cloud (VPC) services that can establish their own virtual network services. The tenants can build the networks and environments according to their needs. The tenants can divide the private IP network segment and deploy the service to the virtual switch as needed. At the same time, the users can configure the routing rules of the virtual routers and implement the security control for the access control. The flexible public IP address of the Alibaba Cloud is the public network IP address that the users can apply for according to their own needs. After applying, the users can bind the corresponding cloud products to the IP for real-time access. The deployment steps are specified as follow: (1) create a personal VPC. Log in to the Alibaba Cloud console and select a proprietary network VPC, which is shown in figure 8, respectively. (2) create a proprietary network. Select the geographic and the available zones, fill in the information as needed, and create a proprietary network and virtual switch.

Create an ECS (Elastic Compute Service) instance. Select “Switch” under “Private Network VPC”, enter the switch just created by the users, and click the “Add” button under “ECS Instance” to enter the ECS instance interface. Setting the parameters: (1) region: select the same region as the created VPC. (2) vCPU: select “2vCPU” or “4vCPU” according to the user needs. (3) memory: select “2 GiB” or “4GiB” according to the user needs. Set the mirror after selecting the appropriate instance: (1) “Mirror Market”→“Shen-xin-fu virtualize the next generation firewall”; (2) Storage: select the default value of 40GB, and do not add a data disk. (3) Network: the users must select “Private Network”, and select the network created by the users earlier. (4) Security group: if there is no security group, the users can create a new security group and configure the related rules (open HTTP443 port). (5) System configuration: select “Custom Pass-word” in “Login Credentials” and set the login password. The password requirements include the uppercase letters, the lowercase letters and the numbers. Try not to use

| Table 5. Internal1 interface connection situation. |
|--------------------------------------------------|
| Port | Connection | IP         |
| f0/0 | SW1-2      | 172.16.10.5/24 |
| f0/1 | SW2-2      | 172.16.20.5/24 |
| f1/0 | SW3-2      | 172.16.30.5/24 |
| f2/0 | Pix-e0     | 192.168.0.6/30 |

| Table 6. Internal2 interface connection status. |
|--------------------------------------------------|
| Port | Connection | IP         |
| f0/0 | SW5-2      | 172.16.50.5/24 |
| f0/1 | SW4-2      | 172.16.40.5/24 |
| f1/0 | Pix-e1     | 192.168.0.7/24 |
the special symbols to avoid login to the firewall. Add the additional configurations or instructions as needed to pay for the order.

![Diagram of Proprietary network and Switchboard](image)

**Figure 8.** Creating a VPC and virtual switch.

Apply for an elastic IP. In the “Management Console”, select “Resilient Public IP” under the “Network” column, select “Apply Flexible Public IP” or “Specify IP Address Application” according to the user’s needs, select the same area as the VPC environment and choose the payment method, and the flexible IP number. Bind the ECS instance after the application is successful. After the binding is successful, log in to the public IP address of the application. The login user name is admin and the password is the custom password set when the ECS instance is created, as shown in figure 9.

![Diagram of Login credentials](image)

**Figure 9.** Customizing the root password.

### 4.2. Configuring a Security Policy [12]
Configure SNAT policy: configure the appropriate SNAT policy in the convinced virtual next-generation firewall to allow the intranet users to access the internet: (1) in the “Navigation Menu”, find the “Object Definition” column, select “Network Object”, and add “IP Group Object”, add the IP required for the experiments. (2) select “Address Translation”, add “Source Address Translation” in the “Firewall”, then specify the source area: manage; source network object: intranet; destination area: manage; destination network object: all; protocol: all of the source address translation: specify IP (IP address of eth0 interface); (3) select the application control policy in “content security”. The source network object, source area, destination network object, and destination area are the same as those in (2). Select to open the HTTP, FTP, DNS, and SSL applications.
Configure the DNAT strategy: (1) select “Address Translation” and add “Destination Address Translation” in the “Firewall”. Source area: manage; destination IP: specify IP (IP address of eth0 interface); protocol type: TCP, port: 80 (open 80 port web service); destination address translation: specify IP (providing intranet IP of web service). (2) configure the application control policy, which is the same as the configuration mentioned before, and here will not be described again.

4.3. Intranet Audit and Intrusion Tracking [13]

4.3.1. Basic Concepts of Intrusion Detection. The intranet of the robotic brain needs to configure the intrusion detection system as the second defense line behind the firewall, so as to prevent, track, locate, and block the source IP of the intruder or the suspected behavior, record the corresponding behavior and inject the log. In addition, the built-in the data center, and send the email alerts, notify the network administrators of the dangerous signals and analyze the relevant data to determine the intrusion cause, so as to find the ways to disintegrate the intrusion, and maintain the system, reflect and summarize. For IPS (Intrusion Prevention System), the reasonable characteristics and the rules are equally important. The qualified IPS can reduce the processing packet delay while efficiently analyzing the data packet, ensuring low false alarm rate and false negative rate, reducing the impact on the network delay of the protected system, and reducing the user’s bad experience.

On the other hand, the IPS vulnerability intrusion feature identification library must be updated in time, and the latest rules are applied to the basic filter, and the data packets are checked by verbatim, so as to more accurately locate the attack, and identify its behavior and category. Behavior auditing of the incoming traffic and the user operations facilitates tracking of the possible intrusions. By finding and blocking the intruder’s springboard IP and repairing the system vulnerabilities in time, the intruder risks using the other springboards to re-invade can be reduced, as shown in figure 10.

4.3.2. Intrusion Detection Configuration. Firstly upgrade the IPS library to meet the latest protection requirements. In the navigation menu, choose “System Maintenance”, click “Library Upgrade” in “System Update”, and select the IPS vulnerability identification library for “Update Now”. If the new version has an intractable problem, the users can select “Rewind” to restore the system to the previous library version; when configure IPS, in the navigation menu, choose IPS and click “Add” in the upper left corner to add an IPS protection policy. For the SNAT policy, the source area and the network objects are selected as the intranet users, and the destination domain and the network objects are external network objects. For the possible attacks such as “Trojans”, the file vulner-abilities, the system vulnerabilities, the malicious programs, etc., they are blocked and alarmed, and recorded in the corresponding logs in order to the network administrators to analyze. For the DNAT (destination network address), the source area and the source network objects are the external network access the users, and the destination domain and the network objects are the intranet trusted IPs (intrusion prevention system), so that the intranet servers are protected from the common attacks such as mail, DNS, remote connections, and file transfers. At the same time, it can effectively defend against the key detection and the brute force and the monitor, identify, reject, block IP and record it in the related logs, as respectively shown in figures 10-12.
Figure 10. The DNAT application control policy.

Figure 11. Setting the alarm event and notifying the administrator.

Figure 12. Managing the log.

5. Conclusion
This paper only focuses on the macro deployment security protection scheme. Based on the Ubuntu and the gns3, the experimental firewall and the router mirror are found in the appropriate channels. The deployment and the construction of the intranet partition environment are started, and the DMZ-based intranet is built. Deploy the security policies and the access policies on the routers and the firewalls, encrypt the plain text passwords, and enable the static routes to improve the confidentiality and the information content integrity. Configure a reasonable ACL (Access Control List) as the network boundary to monitor the network traffic entering and leaving the intranet. Protect the internal network security. On the internal network host security and the IPS deployment attack and the defense
experiments, the original scheme is to install and deploy the virtualized mountain cloud grid, but it is also difficult to get the installation package and the authorization, and finally changed to the experiments on the deep convincing firewall and obtained the experimental results. In addition, regarding the hidden dangers of the virtual machine migration, the virtual machine protection isolation, etc., the internal network has not yet proposed the related solutions or the measures to be improved.

Acknowledgment
The research in this paper has been funded by the Fundamental and Applied Fundamental Research Fund of Guangdong Province (No. 2015A030308018), and the author expresses deep honest thanks.

References
[1] Zhang X 2018 Brain-like intelligence guides the future of AI Nature **40** (5) 343-348.
[2] Human Machines and Cognitive Labs Brain Science and AI Are Still Difficult to Integrate http://www.sohu.com/a/280362768_297710.
[3] Jiang C J and Wang J L 2019 Intelligence comes from people and expands into work-Thoughts on the development of artificial intelligence China Engineering Science **20** (6) 93-100.
[4] Miao Y T 2017 Research on China’s Cyberspace Security Strategy from the Perspective of Overall National Security Concept (Hunan University).
[5] Ye H P and Chen J 2018 Cloud Computing Security Protection Technology (Beijing People’s Posts and Telecommunications Press).
[6] Wen C Z and Qin W L 2018 Cloud computing technology security prevention and control strategy Electronic Technology and Software Engineering **22** 187.
[7] Yang L 2018 Information security and protection in cloud computing environment Information Recording Materials **19** (11) 71-72.
[8] He J 2019 The main security threats and trends in cloud computing Computers and Networks (2) 52.
[9] Zhang S H 2018 The first priority—Analytics of cloud security construction Computer and Network **18** 58.
[10] Hou J F 2019 Analysis of the security status and solutions of cloud computing platform Tianjin Vocational College Joint Journal **21** (2) 109-110.
[11] Mao Y 2018 Research on network security status and defense strategy in the era of cloud computing Computer Programming Skills and Maintenance **7** 166-168.
[12] Xue S 2017 a network border protection design based on DMZ principle Network Security Technology and Application **4** 53-54.
[13] Liu J 2012 The creation method of DMZ area under different network security requirements Financial Technology Times **8** 72.