Communication Security Design of Brain-Like System Based on Cloud Computing Platform

Gang Deng 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. This paper mainly studies the communication security problems of brain-like system (or robotic brain) based on cloud computing platform, and designs a more convenient and safer communication mechanism for the robotic brain, which includes password algorithm design, digital signature design before login, data exchange design during login process, and security protection design against network attacks. Only the legitimate users can communicate with the robotic brain to ensure that the control authority of the robotic brain is not illegally stolen. In the authentication process, the key agreement must be carried out first, the user name and password of the legitimate user must be encrypted and sent, and the encryption algorithm must be guaranteed to be unable to be deciphered under the existing technical conditions. For the important communication data, the encrypted transmission is required, the encryption key is determined through negotiation, the encryption algorithm must be safe and reliable, and the encryption and decryption speed must be guaranteed. This process requires ensuring that communication data is not stolen illegitimately, and the data can be verified to avoid tampering and illegal data insertion. The users may control the robotic brain to work, and ensure its safety during the communication process.

Keywords. Cloud computing; robotic brain; communication security.

1. Introduction
Although the existing intelligent robots have certain mobility and many special functions, most of them become furnishings because they lack of robotic brains. Therefore, in recent years, many brain-like system (robotic brain) research institutions have been set up, which hopes to acquire techniques and methods similar to human being’s brains, such as thinking, learning, execution, and can be used by the robotic brains, as shown in figure 1. The robotic brains can control the intelligent robots to help human beings to do work [1, 2]. Therefore, this paper mainly studied the communication security problems of the robotic brain based on the cloud computing platform, the main work is the login security design, which includes the password algorithm design, the digital signature design before login, the data exchange design during login process, and the security protection design against the attacks, so as provide a more convenient and a safer communication mechanism for the robotic brain based on the cloud computing platform.

2. Robotic Brain Communication Security Design
The communication security problems of the robotic brain based on the cloud computing platform mainly consist of virtual firewall configuration structure, password and login security, data storage security, communication content security, data transmission security, and so on.
2.1. Password Algorithm Design [3, 4]

2.1.1. Certification Security. After considering various secure encryption schemes to ensure the login security, MD5 (Message-Digest) algorithm is chosen finally to encrypt the password when logging in, as shown in figure 2. The advantages of the MD5 algorithm are: (1) fixedness: regardless of the number of data byte input, the MD5 value calculated from this data is composed of 32-bit hexadecimal strings. (2) convenience: the input characters are calculated by the hash function, and each data has a specific MD5 value. (3) consistency: even if a byte is changed, the calculated MD5 value will be very different, which improves security. (4) security: if only know the data and the MD5 value, it is difficult to use the exhaustive method to decipher the password, the probability of finding the same original data with the same MD5 value is very low. Since the MD5 value of the same string password is immutable, it is not safe, therefore it is necessary to add a salt value based on the MD5 value, the security can be guaranteed, the corresponding DES (Data Encryption Standard) algorithm is also designed and adopted, for the encryption and decryption shown in figure 3.

By the DES algorithm, only the legitimate users can communicate with the robotic brains to ensure that the control rights of the robotic brains are not illegally stolen.

![Figure 1. Robotic brain based on cloud computing platform.](image)

(a) Span brain functions based on the cloud computing [1]  
(b) Robotic brain components based on cloud computing [2]

![Figure 2. The MD5 algorithm flow chart.](image)
2.1.2. Communication Security. Firstly, the login security design must ensure the communication safety of the robotic brains, which include: (1) authentication security. In the authentication process, the key negotiation is firstly performed. The legitimate user’s username and the password must be encrypted and sent. The encryption algorithm must be guaranteed to be undeciphered under the existing technical conditions. The authentication process also needs to consider how to prohibit the third parties from replaying, hijacking, and other attacks. (2) communication security. For the important communication data, the encrypted transmission is required. The encryption key is determined through the negotiation, and the encryption algorithm is safe and reliable, and the encryption speed and decryption speed are guaranteed. This process requires that the communication data is not illegally stolen, the data can be verified, and the tampering and the illegal data insertion are avoided.

The encryption algorithms are very common in the network communication: (1) the asymmetric encryption. The used encryption method is asymmetric, the encryption uses one key, and the decryption uses another key, which are different and have no direct connection. The generated two keys are named as public key and private key respectively, and the private key is managed by itself, and the public key is publicly available. (2) the symmetric encryption. The encryption method used is that the same key is used for the encryption and the decryption, and the sender of the information encrypts the data by using the key, and ensures that the key is not leaked during the communication process, and the information receiver uses the key to decrypt the content. The symmetric encryption algorithm is characterized by a relatively high encryption speed and is suitable for the encryption with a relatively large amount of data. As long as someone gets the key, it can exchange information with it, therefore the security is not high enough.

For the critical communication data, this paper uses an asymmetric encryption algorithm for encryption, because the security is a top priority. The asymmetric encryption algorithm is shown in figure 4: (1) Party B becomes a unique pair of keys (public key, private key) and propagates the public key, but the private key can not be published. (2) Party A receiving the public key, encrypts the information to be encrypted with the key (public key) and sends it to Party B. (3) Party B decrypts the encrypted information with another key (private key) stored by it. Party B can only use his secret key (private key) to decrypt the information encrypted with the corresponding public key. Suppose a third party obtains the transmitted cipher text by other means during the transmission process, although the public key is public, the third party can not decrypt it. The cipher text can only be decrypted by the private key, and the private key is sent by Party B. In the interaction process, once Party B wants to reply to the encrypted information of Party A, Party B needs to obtain the public key of Party A to encrypt the information, and then decrypt the information through the private key.
2.2. Cloud Security Design [5, 6]

2.2.1. Using HTTPDNS to Prevent DNS Hijacking. To ensure the normal information interaction between the client application and the server, HTTPDNS resolution service is used, and HTTPS is more secure than HTTP. The traditional DNS resolution services are vulnerable to the DNS hijacking. By HTTPDNS resolution service, the APP can communicate with the server directly through the IP address instead of communicating with the server through the domain name to ensure the communication security. HTTPS resolution service is shown in figure 5.

2.2.2. Data Transmission Security. HTTPS channel is a hypertext transfer protocol derived from security, which means that it is an upgraded version of HTTP. HTTPS actually uses Netscape’s Secure Full Sockets level (SSL) as a sub-layer of HTTP application level. It is a URI scheme with the same syntax as http system, used for the secure HTTP data transfer.
2.2.3. Using URL Signature. Without a URL signature, anyone can request a server after receiving the request data. After the URL is signed, the server verifies the request data, processes the legitimate request, and discards the illegal request. With the method, the time between the client and the server must be kept in sync to ensure the request uniqueness.

2.2.4. Encryption Using Protocol. If the data is transmitted in the plain text, there is a risk of the data being stolen during the transmission; therefore, the transmitted data must be encrypted. The general need for the encrypted data transmission occurs in the user’s data that the user must log in to view. In this paper, the user’s private data signing key must be dynamic to ensure the data security. The signing key is usually returned to the client after the authenticated user logs in. Both the server and the client retain this key for signing the data and then agree to the encryption mode used to encrypt the plain text data. The adopted AES (Advanced Encryption Standard) encryption algorithm is shown in figure 6.

![Figure 6](image_url)

**Figure 6.** The AES (Advanced Encryption Standard) encryption algorithm.

3. Cloud Security Protection and Testing

3.1. Binding Using MAC and IP Addresses [7, 8]

Binding technology for MAC (Media Access Control Address) and IP addresses, is designed to ensure that only certain users can use the software on the right client [9], the unauthorized hosts and the users can not log in to the client, which improves the security to some extent. The information of the authorized host is stored in the server database, and when the user attempts to log in, the program
automatically retrieves the MAC and the IP address. The following is the call function for the retrieved IP:

```java
String clientIP= InetAddress.getLocalHost().getHostAddress();
```

After obtaining the IP address by calling the function, the command program of the MAC address corresponding the host can be obtained in the Java program according to the obtained IP address, and the string data and the input stream information at the end of the MAC address are obtained from the command program. The complete MAC address of the corresponding host can be obtained from the input stream sequence:

```java
Process PP = Runtime.getRuntime().exec("nbtstat-a"+clientIP);
InputStreamReader ir = new InputStreamReader (PP.getInputStream());
```

### 3.2. Prevent SQL Injection Attacks

The SQL injection is a common means of the network attack, the harm caused by the SQL injection is huge. Because of its particularity, it can obtain the administrator rights to a certain extent. The harm to the database is particularly serious. The SQL injection attack is simply adding some special characters to the web form to achieve the effect of spoofing the server. To prevent this problem, filter out some characters such as single quotes "". If want to enhance it, then filter out some traversal functions, such as declare, exec and so on.

In order to prevent the SQL injection attacks, a two-dimensional or multi-dimensional verification mechanism can be established, add a rule for retrieving the characters and the parameters input by the user based on the original verification, and the user can not directly embed the SQL statement. The parameterized SQL, in order to further improve the security and the execution efficiency and the maintainability of the SQL statements, all of the SQL query statements use the login verification and the stored procedures in the program. Taking the stored procedure set in Oracle 11g as an example, the Java login code calls the stored procedure to determine which it is a legal black budget based on the success score.

```sql
CREATE OR REPLACE PROCEDURE checkUser
(no IN TBEMP.eid%TYPE, name IN TBEMP.ename%TYPE, success outnumber)
AS
BEGIN
    SELECT COUNT(*) INTO success FROM DEPT WHERE eid = no AND ename = name;
END;
```

### 3.3. Anti-Exhaustive Attack [9, 10]

In some previous cyber-attacks, the exhaustive attack is very common, and it is also a violent deciphering method, that is, constantly trying to log in until deciphering. Although this kind of the attack is currently rare, the basic protection has been made. Usually the guess numbers can be limited. When the number of the input errors reaches the upper limit, the log in cannot be realized. The password complexity, the character alphanumeric case, etc. are all taken into account, and the number of the password bits is maximized. Use verification codes to prevent unlawful violent deciphering or exhaustive deciphering, the login rules can also be created. For example, only the machines that specify IP can log in, and only the specified pages can log in. It can be also set a maximum number of the verification, limit the number of the login per IP to 5 times per day, and block the login port service for that IP. In order to prevent the Trojan from recording the password entered by the keyboard, the system can use the soft keyboard technology to improve the safety factor.

### 4. Communication Experiments [11, 12]

For the mixed encryption DES (Digital Encryption Standard) and the RSA (Rivest-Shamir-Adleman), the experimental results are shown respectively in figures 7 and 8, and denote that the mixed encryption DES and RSA are feasible.

This section mainly lists some major cyber-attacks. The corresponding countermeasures are taken to carry out the strict security protection. For example, the common SQL injection attacks, the
practical and the efficient counter-measures are used to minimize the security risks. The method of the MAC and the IP address binding to further improve the security are innovated, and also tested the feasibility of the hybrid encryption DES and RSA.

```java
public class DESandRSATest {

    /**
     * To do DES and RSA hybrid encryption, firstly do DES encryption, and encode the DES encrypted content by base64, and then do RSA encryption for the DES encrypted content by base64.
     */
    @Test
    public void test1() throws InvalidKeySpecException, NoSuchAlgorithmException {
        String deskey = "password"; //DES encryption key
        String content = "Smells good, warning!"; //Content
        System.out.println("Original encrypted content: ", content);

        //DES encrypt
        byte[] encryptbyte = DESUtil.desEncrypt(content, deskey); //Encrypt the content and return as byte array
        System.out.println("DES encrypted content : "+Base64.encodeBase64String(encryptbyte));

        //RSA encrypt
        String rsacontent = RSAUtil.publicEncrypt(content, publickey);
        System.out.println("RSA encrypted content: "+rsacontent);

        //Get the private key
        String prikey = "MIIG6DAQEBALh+gkMhY69dU4BEAFMICA18ggg1hBgEARAA68dU4qER2zjyw9IzwoGw24np56e8mtrgh6680tndtdu//get the private key
        String rsatext = RSAUtil.privateDecrypt(rsacontent, prikey);
        System.out.println("RSA decrypted content: "+rsatext);
    }
}
```

**Figure 7.** Experiment demo.

```
"C:\Program Files\Java\jdk1.8\0.0.11\bin\java.exe" ...
Original encrypted content: Smells good, warning!
DES encrypted content: ZxFJkbo09do0BpyUV1qO03w==
RSA encrypted content: dcSyV40ILyP0G5_WP1TBLB+FMiu8MfSty42
RSA decryption content: ZxFJkbo09do0BpyUV1qO03w==
DES decryption content: Smells good, warning!
Process finished with exit code 0
```

**Figure 8.** Experimental results.

5. Conclusions
The major innovations of this paper are as following: (1) uses the MD5 algorithm with the salt value, which is more secure and the operation rate is guaranteed. (2) the method of the binding MAC address and IP address is used to ensure security. This approach is designed to ensure that only certain users can use the software on the right client. The unauthorized hosts and the users cannot log in to the client,
which improves security to some extent. (3) the combination of the DES and the RSA makes their advantages and disadvantages complement each other, that is, the DES encryption speed is fast. However, there are still many problems to be solved, this paper does not explore deeply the communication security problems in the ports, XSS, weak passwords, etc., which will be studied in future.

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] Youku Technology https://v.youku.com/v_show/id_XNDg1MTQ0MDg4.html?refer=seo_operation.liuxiao.liux_00003307_3000_z2iuq2_19042900.
[2] Xiao N F 2016 Robotic Brain (Beijing China Science Press).
[3] Ye H P and Chen J 2018 Cloud Computing Security Protection Technology (Beijing People’s Posts and Telecommunications Press).
[4] Xiao Z, Hong Y and Qian W 2009 The information security guarantee system of US federal government procurement and the inspiration to China Journal of Beijing Electronic Technology Institute 17 (3) 17-22.
[5] Shen C X 2010 Constructing an information security system for active defense and comprehensive prevention Financial Electronics 12-18.
[6] Yan G G 2007 Legal security comparison of military information security between China and the United States Information Security and Communication Confidentiality (7) 106-108.
[7] Yang S L 2005 Security system for information security Library Forum 2005 25 (2) 49-51.
[8] Zhang J H, Wang W and Hou L 2012 Research of information security guarantee system Construction Computer Security (8) 72-75.
[9] Jin C H and Sun Y 2004 Research on linear redundancy of S-box in the AES S box Acta Electronica Sinica 32 (4) 639-641.
[10] Feng D G, Zhang M and Xu Z 2011 Research on cloud computing security Journal of Software 22 (1) 71-83.
[11] Liang X M, Sheng H Y and Zhou X 2006 Research on RSA algorithm system Network & Computer Security (12) 26-28.
[12] Wang Z H 2012 Design and implementation of a secure login subsystem Science Technology and Engineering 12 (22) 5624-5628.