Cybernetics Protector

Ashutosh Mishra
B.E. (Computer)
Dept. of Computer Engg.
Sinhgad Academy of Engineering,
Pune-48

Pratik Chandwani
B.E. (Computer)
Dept. of Computer Engg.
Sinhgad Academy of Engineering,
Pune-48

Mustafa Bakrolwala
B.E. (Computer)
Dept. of Computer Engg.
Sinhgad Academy of Engineering,
Pune-48

Abhijeet Bhor
B.E. (Computer)
Dept. of Computer Engg.
Sinhgad Academy of Engineering,
Pune-48

Prof.Gandhali Kulkarni
M. E. (CSE-IT)
Asstt.Professor
Dept. of Computer Engg.
Sinhgad Academy of Engineering,
Pune-48

Abstract—**the purpose of this paper is to present a website for Secret Intelligence Agency. The agency has always used undercover agents to solve complex cases and dismantle criminal organizations. The paper presents a solution so that Secret Intelligence Agencies and their agents can communicate and exchangethe evidences in a secured way. The paper presents Cybernetics Protector developed using the J2EE technologies.**

Keywords—**Secret Intelligence Agency, Security, Face Recognition, Digital Signature.**

I. Introduction

The Secret Intelligence Agency is the nation's first line of defence. It accomplishes what others cannot accomplish and go where others cannot go. It carries out the mission by collecting information that reveals the plans, intentions and capabilities of the adversaries and provides the basis for decision and action.The Cybernetics Protector is software which allows a security agency to handle various confidential missions in a secured way. The Cybernetics Protector software is concerned with the security of the country and thus proper care has to be taken that confidential data from within the database is not leaked out.

Every country requires a Secret Agency who undertakes cases which are a threat to the national security. These agencies operate with the help of undercover agents who help solve these cases. Since these cases deal with the nations' security, the communication and data transfer between the agents and higher authorities need to be protected. Hence developing such a system is necessary to help these agencies operate in a secret and secured way.The system will be used by a set of five different users. These users are Defence Ministry, Chief, Agents, employees and Citizens of the country.

II. SYSTEM FUNCTIONALITY[4]

Figure 1 explains overall functionality of the system along with different set of users involved.

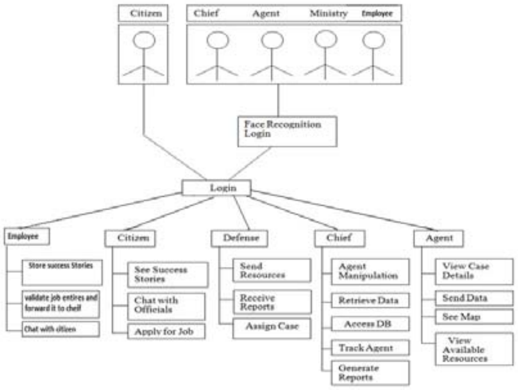


Figure 1 Cybernetics Protector Users

- **The Defense Ministry-**The Defense Ministry assigns cases to the Secret Agency and allocates resources toit. It should be able to receive reports regarding the cases.
- **The Security Chief-**The Chief of the Secret Agency has the highest powers. He can administer the agents, assign cases and resources. Also he has right to view the database.

Proc. of the International Conference on Pervasive Computing and Communication (PCC)
Editor In Chief Dr. R. K. Singh.

ISBN: 978-981-07-2579-2

- **The Agent-**The undercover agent can send the evidence and data collected in an encrypted fashion so that the data cannot be intercepted.
- **Citizen-**A citizen has the lowest access rights. A citizen can only view the success stories of the agency and chat with the officials.

The functions of these different users shown in Figure 1 are as listed here,

1. Agent Manipulation

This feature is provided to the Chief of Security. The Chief will be able to Add/Delete/Edit Agent Records.

2. Agent Appointment

This feature is provided to the Chief of Security. The chief will appoint an agent for the case.

3. Secure sending and retrieval of data

This feature is provided to the Chief of Security, Agent and the Defense Ministry. This feature basically enhances the security of the software.

4. Access of Data Logs

This feature is provided to the Chief of Security. This feature enables him to analyze the data logs.

5. View Case Details

This feature is provided to the Agent. The agent will receive the entire case details from the Chief of Security.

6. View Resources

The chief and agents can view the resources available.

7. Report Management

This feature is provided to the Chief of Security, Agent and the Defense Ministry. The Chief will use this feature to generate reports and send them to the Defense Ministry. The agents can use this feature to send the reports to the Chief. The Defense Ministry will be able to receive the reports.

8. View Map

This feature is provided to the Agent. The agent can view the dynamic map of any place in the world. This feature will help the agent for further planning.

9. Send Resources to Secret Agency

This feature is provided to the Defense Ministry. The Defense Ministry is responsible for any resources that are to be made available to the agents.

10. Assign Case to Agency

This feature is provided to the Defense Ministry. The defense ministry will create a new case and the case details along with the mission objectives to be sent to agency.

11. View Success Stories

This feature is provided to the Citizen. The citizen has the least powers. The citizen can view the details of completed missions which are posted by the agency.

12. Provide Tips and Feedback

This feature is provided to the Citizen. The citizen can provide tips and feedback regarding any article that is posted by the agency.

13. Apply for Job

This feature is provided to the Citizen. The citizen can inquire about the different job profiles available at with the agency. Also he can inquire about the various qualifications required for different job profiles.

III.BACKGROUND

The Cybernetics Protector software is concerned with the security of the country and thus proper care has to be taken that confidential data from within the database is not leaked out. The main focus of the system is on security and thus the following sets of features are used to provide high security.

- Encryption and Decryption
- Digital Signature
- Face Recognition Login

A. Encryption and Decryption[2]

This system is based on the 3 pillars of information security- Confidentiality, Integrity and Availability. The digital signature used here protects the integrity and authenticity of a message. However other techniques are still required to provide confidentiality of the message being sent. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text).

In many contexts, the word encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again (i.e. to make it unencrypted). For this project uses inbuilt package **'javax.crypto'**

To provide higher integrity and confidentiality project uses both the digital signature and encryption mechanisms. The document is digitally signed by the sender as well as the document is encrypted.

B. Digital Signature[1]

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.

Any data/document which is sent through the system will require the sender to digitally sign the data before sending. The concept works in two stages, Signing and Verification as illustrated in Figure 2(a) and 2(b) respectively.

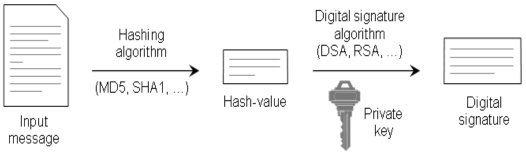


Figure 2(a) Signing

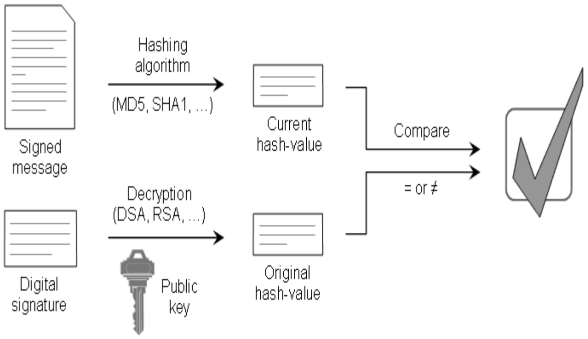


Figure 2(b) Verification

java.security Package: Java provides an in built package with the classes and interfaces for the security framework.

1. **Generate private and public keys:**TheKeyPairGenerator class is used to generate pairs of public and private keys. Key pair generators are constructed using the getInstance factory methods. These are static methods that return instances of a given class.A Key pair generator for a particular algorithm creates a public/private key pair that can be used with this algorithm.
2. **Sign the data:** A digital signature is created (or verified) using an instance of the Signature class.

```
              Signature dsa =
Signature.getInstance("SHA1withDSA","SUN
                    ");
```

DSA is a Digital Signature Algorithm while SHA1 is a Secure Hash Algorithm which is the message digest algorithm.

3. **Verify the Signature:** Onceall of the data is supplied to the Signature object, one can verify the digital signature of that data and report the result. Suppose that the alleged signature was read into a byte array called sigToVerify.

```
          boolean verifies =
        sig.verify(sigToVerify);

System.out.println("signature verifies: "
             +  verifies);
```

The `verifies` value will be true if the alleged signature (sigToVerify) is the actual signature of the specified data file generated by the private key corresponding to the public key

C. Face Recognition Login[3][4][5]

The Cybernetics Protector software provides a very secured logging in process with the help of face recognition along with password protection. . The system requires the Chief, Agent, Defence Ministry and the Employees to log into the system using face recognition system.

The project usesOpenCV library for face recognition.OpenCV, Intel's free, open-source computer-vision library can greatly simplify computer-vision programming. It includes advanced capabilities like face detection, face tracking, face recognition, Kalman filtering, and a variety of artificial-intelligence (AI) methods in ready-to-use form.

This functionality contains,

- Capture image
- Detect face and convert it into useful format
- Create database
- Recognize face

1. Capture image:

Project uses theinbuilt functions from PHP to initialize the web camera and capture the images. The user images are captured at client side.

a. webcam.set_hook(hook_name,user_function);

webcam is a top level global namespace.This allows one to set a user callback function that will be fired for various events in the system. Here are all the events one can hook:

onLoad - Fires when the Flash movie is loaded on the page. This is useful for knowing when the movie is ready to receive scripting calls.

onComplete - Fires when the JPEG upload is complete. Your function will be passed the raw output from the API script that received the file upload, as the first argument.

b. webcam.set_api_url(URL);

This allows one to set the URL to server-side script that will receive the JPEG uploads from the Flash movie. Beware of cross-domain restrictions in Flash.

c. webcam.snap();

This instructs the Flash movie to take a snapshot and upload the JPEG to the server. Make sure you set the URL to your API script using webcam.set_api_url(), and have a callback function ready to receive the results from the server, using webcam.set_hook().

d. webcam.set_swf_url(URL);

This allows you to set the URL to the location of the “webcam.swf”flash movie on your server. It is recommended to keep this file in the same directory as your HTML page, but if that is not possible, set the path using this function. Beware of cross-domain restrictions in Flash. The default is the current directory that your HTML page lives in.

2. Detect the face and convert it to useful format:

This step is to detect the faces from the image and crop the face in required size and format. To do this, project uses inbuilt “haar” function from openCv library. This function detects face from the image and gives rectangle’s coordinates as the output. Using these coordinates face is cropped and converted to grayscale image. Thereafter this image may be stored in the database or can be used for face recognition.

3. Create database:

While registering any new employees or agents face database is updated with his photos. The facesare stored in database with filename as [id_*cnt*], where *cnt*is 0, 1, .n. A sample face is as shown below in Figure 3.

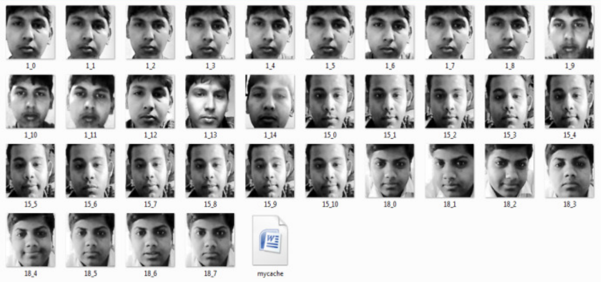


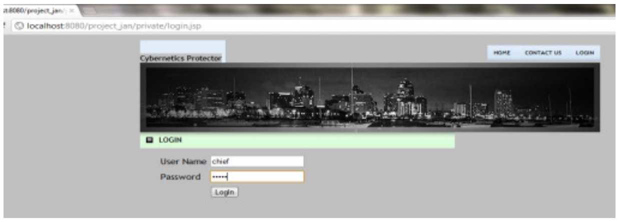
Figure 3: Face Database

4. Recognize face:

Here the face from second step is taken as input and compared with the face database. Cache file is created from all images and this file is compared with input face image. If the face is found to be matching, its filename is returned. The id from this filename is compared with user id who is logging in. If both the ids match then the user getsan access to the site.

The following snapshots of the project screens explain how face recognition is implemented and used by different authorities of the Intelligence system.

Figure 4 is a login screen of the project which redirects the user to face recognition module.


localhost:8080/project_jan/private/login.jsp

Cybernetics Protector

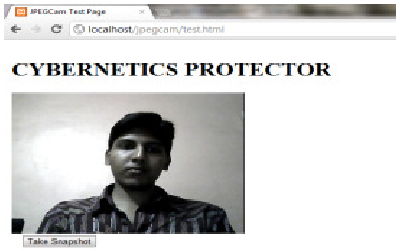
LOGIN

User Name chief

Password •••••

Figure 4: Login

Once the userid and password is provided the face recognition module captures the user face and tries to match it with the face database. Figure 5 shows the face capturing.

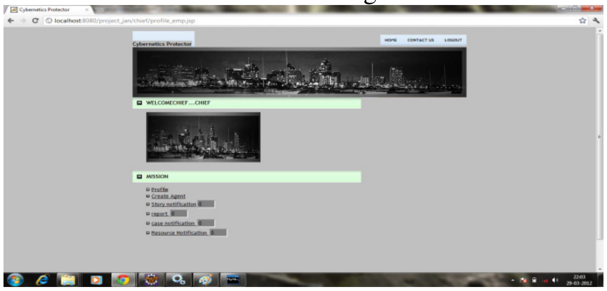

JPEGCam Test Page

localhost/jpegcam/test.html

CYBERNETICS PROTECTOR

Figure 5: Face detection

The face may get denied by the system and hence unauthenticated user will not be able to access the system. If the face is recognised, the user id from login screen and the one from recognised face’s filename is checked. If these user ids match, user gets a login to the system. Figure 6 shows the user profile, an agent/ chief or defense sees after successful login.


Cybernetics Protector

localhost:8080/project_jan/chief/profile_emp.jsp

Cybernetics Protector

WELCOMECHIEF....CHIEF

MISSION

- Profile
- Create Agent
- Story notification 0
- report 0
- case notification 0
- Resource Notification 0

22:03
29-03-2012

Figure 6: User Profile

IV. CONCLUSION

This project thus allows secret agencies to manage secret cases in a secured and confidential way. The secured login system which uses face recognition login provides a high level of security. Digital Signatures and encryption used will help to prevent unauthorized access to data. Thus this project achieves information security by following the 3 principles of ‘Confidentiality’, ‘Integrity’ and ‘Authenticity’.

REFERENCES

[1] “Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications”, *Harn, L. JianRen*

[2] “Cryptography and Network Security”, Fourth Edition

[3] http://ubaa.net/shared/processing/opencv/

[4] http://www.ibm.com/in/university/greatmind/tgmc.html

[5] code.google.com/p/jpegcam/wiki/APIDocs